Problematizing digital sovereignty, constructing Europe: Warfare, regulation and enemization through digital devices

Marie Alauzen

PROBLEMATIZING DIGITAL SOVEREIGNTY, CONSTRUCTING EUROPE

Warfare, regulation and enemization through digital devices

Marie Alauzen

marie.alauzen@univ-eiffel.fr

Abstract

The chapter examines the constitutional order that emerged in Europe through the quest for digital sovereignty. Drawing on policy documents and an ethnographic investigation of a French diplomatic unit, I explore two problematizations of digital sovereignty. The first, which originates with NATO and the East StratComm task force, is grounded on the assumption of an emerging threat and the constitution of Russia as a common enemy. The idea that Europe must take part in an information war is based on the supposition that a technological arrangement can be stabilized. Along with this, and in reaction to it, the EU has built a problematization of digital regulation processes. A moral economy has been embedded in a regulatory framework, with the understanding that digital service platforms have also become enemy figures. The elicitation of these problematizations introduces a critical perspective on digital sovereignty as a way to define Europe through technologies and knowledge that suppose a common enemy. I call this "constitutionalism through the enemy".

Keywords (6)

constitutionalism; digital regulation; digital sovereignty; disinformation; enemization; information warfare

Discerning Disinformation, Constructing Sovereignty in Europe

Crediting the Disinformation Issue

In January 2022, France published its priorities and program for the Presidency of the Council of the European Union (EU) for the next six months. After the fight against covid-19, the second most important guideline for "a more sovereign Europe" was defined as "Strengthening European Democracy" (PCEU, 2021, p. 8). In this context, strengthening democracy did not mean a greater degree of citizen participation in European affairs, an additional quality of deliberation, or more transparency and factual assessment of election processes. It consisted of two measures: improving the legislative framework before the next European elections, and countering "hybrid threats". First, the French Presidency was intent on amending the regulation on the status and funding of political parties, regulating online political advertising, and amending the Electoral Act; and second, it was committed to reinforcing the EU's prevention and response capacity against cyberattacks affecting the EU and its Member States, and tackling the day-to-day disinformation eroding public confidence. In other words, this motto of a "more sovereign Europe" and "European democracy" defined the tenets of a Europeness that would restore what is often called "digital sovereignty" by securing the electoral process, investing in cyber-defense, and guaranteeing the democratic viability of the arenas in which public debate can take place.

To situate this political prioritization, we should bear in mind that in May 2017, two days before the final round of the French presidential elections in which the centrist candidate, Emmanuel Macron stood against and the far-right Marine Le Pen, e-mails related to Macron's campaign were leaked. In these emails, memos, notes and mundane party reservations were conflated with false documents to produce evidence of tax evasion and election fraud. This pirate operation started with an early disinformation campaign consisting of rumors, fake news, and even forged documents; a hack targeting the computers of Macron's campaign staff; and, finally, a leak consisting of 15 gigabytes of stolen data, including 21,075 e-mails posted on a file-sharing site and spread through social media and Wikileaks (Jeangène-Vilmer, 2019). The national cybersecurity agency, as well as the US intelligence committee, journalists and cybersecurity experts, qualified this leak as an "election interference" that might be related to a hacking group with ties to Russian military intelligence. Since these leaks, Macron, who represents the French

citizenry not only through the national electoral system, but also through his practices and his rhetoric, and who repeatedly depicts himself as a European, has been personally committed to tackling the "disinformation issue". Disinformation is a flexible term often used to refer to the dissemination of false or biased news for hostile political purposes. It is thus empirically connected to the vocabulary of interference, intentional manipulation, fake news, fact-checking, and debunking, and its implications in terms of technological investments. Macron has publicly repeated that an issue of this nature deserves more credit, arguing for "more European engagement", and considers, without being more explicit, that media fact-checking should not be the only collective answer.

While neither the spreading of fake information in the public space nor foreign electoral intervention is new (Bloch, 2013; Darton, 1984), digital platforms and the correlative risk of information manipulation has made it easier and more large-scale. The year before the Macron Leaks, in 2016, the Dutch referendum on the Association Agreement between Ukraine and the EU, the United Kingdom's referendum on membership of the EU, and the US presidential election had already raised similar democratic concerns. It was, moreover, not only a matter of regulation of digital platforms that put this information into circulation and framed the public space. In most of these cases, Russia stood accused of interfering in internal affairs, destabilizing the political situation and manipulating public opinion through digital devices to discredit and divide its "enemies". In military doctrine, this interpretation of actions relating to information is referred to as "hybrid threats". Hybrid activities are characterized by an alteration of the demarcation between "war" and "peace", and a blurring of the boundary between "internal security" and "external security" – as the framing of terrorism and counterterrorism over the past thirty years has illustrated (Linhardt and Moreau de Bellaing, 2019).

This chapter scrutinizes the particular way in which Europe is instantiated through the disinformation issue and formulation of a collective answer to a problem thus defined. I address the emerging understanding of disinformation by making a broader argument about the significance of digital sovereignty as a novel principle of government, and exploring the issue of Europe and European subjects enacted by digital devices. My guiding question is then: how has digital sovereignty become a category of government defining Europe? How is it practically constituted as a distinct kind of political object, able

to enact a political subject? I argue that, even before the French Presidency of the Council of the EU and the 2022 Russian war on Ukraine, it had become a compelling marker of a type of "European constitutionalism". Following Jasanoff's conceptualization of constitutionalism that offers an extension for the empirical description of the arenas in which the realizations including the more technical one are highly political (2003), European constitutionalism defines an arrangement of knowledge that shapes the relations between political institutions and citizens, and specifies a European identity for both. This transformative horizon of "digital sovereignty" for Europe has been legible in policymakers' increasing concern with hybrid threats and disinformation as a means to maintain Europe's capacity to act and to protect citizens in all digital technologies. The claim has contributed to the imaginary of Europe as a coherent political entity, based on what Linhardt and Moreau de Bellaing call "enemization" (2019), that is, the collective validation of a reasoning that proceeds through the construction of a central enemy. In keeping with the theme of this volume on Europe-making by digital innovation, I argue that the quest for digital sovereignty has resulted in different "problematizations" of Europe. Problematization is a central concept in STS as it defines a problem worthy of collective examination and treatment (Laurent, 2017), and here the two problematizations share the delineation of an enemy for Europe.

It is not simply a matter of constructing a "European difference" by shaping Europe's image in relation to that of the US, as in the case bio-regulation, with the precautionary principle (Dratwa, 2012), and harmonization (Laurent, 2022). It produces a Europe not in a competitive relationship or by asserting values like trust and transparency, but by means of a Schmittian characterization of the public enemy (*hostis*) (Schmitt, 1996). By connecting the shared reasoning to these two problematizations of Europe, I introduce a critical perspective on digital sovereignty, which I label "constitutionalism through the enemy" to draw attention to a radical shift in the representation of Europe.

Unfolding European Constitutionalism

If our perception of it is not to be reified, Europe, like any conceptual entity – science, nature, culture or the state – must constantly be rediscovered. STS scholars thus consider the "co-production" of the social and natural order, that is, the gradual construction of

wider technical or geographic and social realities resulting from the circulation of people and things that deploy knowledges and stabilize devices (Jasanoff, 2004; Latour, 1993; Shapin and Schaffer, 1985). Accounts of processes of constitutional ordering of realities have portrayed Europe as a "multiply imagined community", which challenges efforts to form stable shared visions, including visions of truth, justice or peace (Jasanoff, 2005). The examination of these visions requires that we carefully examine constitutive trials, experiments, ordinary tribulations and what Barry calls "technological zones" (2001). Technological zones do not coincide with national territories nor any taken-for-granted institutions, but with infrastructures, norms, and standards, fostering spaces for the circulation and implementation of technologies. The concept captures in a particularly accurate way the socio-political institution of Europe and Europeness in the contemporary period, and has led to a depiction of the political subject in interaction with technology and territory.

Following this line of thought, STS scholars have firstly addressed Europe's engagement with bioscientific research and innovation and its capacity to build supranational imaginaries in contexts of uncertainty. For instance, analyzing the difficulty of the EU to impose its political will on biological organisms, Lezaun focuses on the role that traceability has played to deepen consumer confidence in biotechnology and improve responsibility by means of testing techniques, spatialization of detection work, and other tools designed to fix things in specific places that define Europe (2006). By examines the formulation, in parliamentary deliberations, of the precautionary principle as critical in governing the life sciences and technologies, Dratwa shows the constitutional role that "precaution" plays in shaping Europe: both a biopolitics, a means of legitimating regulation of life, and a supranational institution binding member states (2012). In both cases, "Europe" has been formed with socio-material arrangements of biotechnology in the mutual constitution of actants. Laurent claims that this kind of EU policymaking based on objects (more than human subjects) defines the constitutional strength of Europe (using European institutions) by giving shape to desirable futures through the entry of objects in democracy (2022).

Alongside the dreams of harmonization by regulating biotechnological objects, the government of digital technologies has opened up alternative perspectives about Europe, Europeness, and Europeans as data subjects. Many probes focus on data and the tensions

raised by the EU emphasis on privacy rights. They show that in digital infrastructures the European data subject has arisen as a category of individual actors able to give their consent (Starkbaum and Felt, 2019), and that this has bred frictions with pseudonymization or anonymization of large data sets and re-identification procedures (Shabani and Marelli, 2019). These works point to the formation of the individualistic European digital subject (McFall, 2020). They also invite us to multiply investigation sites, to grasp the outlines of the technological zones built by information infrastructures, and to collect the situated meanings of Europeness, European objects and European subjects.

The approach undertaken here can be read as a continuation of ongoing debates on European constitutionalism by digital technologies, and more specifically those that exacerbate socio-technical ambiguities and political tensions. In the way that I analyze digital sovereignty, political and technological orders of Europe are seen not as static, but rather as "reimagined, or reperformed in the projection, production, implementation and uptake of socio-technical imaginaries" (Jasanoff and Kim, 2009: p.124). From this perspective, I identify two problematizations of digital sovereignty that have emerged from policy documents and administrative interviews and have established Europe, Europeness and European subjects through the trials and tribulations of diplomatic activity. The first problematization indicates that the defense of Europe's digital sovereignty was spawned by the North Atlantic Treaty Organization (NATO)'s characterization of hybrid threats, and then by its association with European Union bodies, which gave substance to a European arrangement to combat disinformation. This problematization presents Europe as a network of anxious states and expertise, more or less prone to naming Russia as a common "enemy". European subjects are above all the journalists and the military, because they are the ones who define Europeness in the defense against disinformation and who materialize the will to preserve digital sovereignty. The second problematization of digital sovereignty that I analyze focuses on the issue of EU regulation of digital platforms. Alongside and in reaction to bellicose problematization, the EU has also built a problematization of digital regulation processes that establishes digital service consumers as data subjects. A moral economy has been embedded in new regulatory frameworks, according to which digital service platforms have also become enemy figures presenting a risk to Europe's influence. The Digital Services package encompasses a set of rules applicable to the whole EU, intended to

design a technological zone where digital sovereignty is preserved through digital services consumer protection. In conclusion, I suggest a critical perspective by discussing the theoretical and political implications of digital sovereignty for Europe as "constitutionalism through the enemy".

Study and Methods

The article draws on two main data sources, documentary and ethnographic: I collected documentary material produced between 2015 and early 2022, describing anti-disinformation initiatives in Europe; and, in July 2020, I joined the team of the French Ambassador for Digital Affairs at the French Ministry for Europe and Foreign Affairs, where I began participant observation. The policy documents on disinformation that I collected were produced by a range of national, European and non-governmental institutions, and reported the production of administrative knowledge and the orchestration of priorities. Sponsored participation also afforded me the opportunity to observe the French ambassador's team and to gain access to a tacit dimension of the French understanding of disinformation in Europe. I attended dozens of videoconferences and meetings. I also conducted 19 interviews with four project members and their colleagues in government administrations. The body of data from these observations (July 2020 to July 2021) consists of approximately 20 days of field notes and transcripts, and full transcriptions of interviews.

The data allowed me to examine political, technical and judicial operations entangled with the quest for Europe's digital sovereignty. From an empirical entry point, they complete the international relations accounts that have shaped analytical frameworks and expertise on disinformation, hybrid threats, platform regulation and digital sovereignty, but have not considered the local production of their concepts and the practical achievement of the phenomenon in institutional practice. While this documentary and ethnographic analysis makes up an empirical approach to the shaping of Europe by digital devices, it is situated in a French Ministry, and therefore cannot be removed from a French understanding of Europe (ideally, one would have observed the European institutions involved in action). The results are therefore limited by a relatively short time of access to the people involved.

Problematizing Digital Sovereignty in Warfare

In the following section, I turn to the practical examination of the notion of "hybrid threats" which has marked a change in the way of considering the promotion of war and peace, and has problematized the diffusion of information through and at the borders of Europe. The circulation of a NATO policy has contributed to the debate of several EU bodies on the "disinformation" caused by a common enemy, Russia, that imperils the sovereignty of Europe. These reflections have materialized in the attempt to demarcate a boundary between internal and external disinformation and to network national and European administrations.

Engaging Europe with Hybrid Threats

In a statement in 2015, NATO introduced into its official communication the notion of "hybrid threats" that had been circulating in international political arenas and among scholars, along with other conceptualizations on warfare issues: new, irregular or asymmetrical wars (NATO, 2015). On the official website, the term is defined as follows:

Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilize and undermine societies (NATO, 2018).

The blurring of the lines between war and peace preceded the appearance of the term, since scholars call displacements due to contemporary warfare "neither war nor peace"[1]. In particular, non-military aggression such as terrorist attacks by networks disregarding national borders have contributed to the complexity of understanding what war and peace actually are. In reaction to and in anticipation of the phenomenon, the military and legal doctrines of counterterrorism have tended to undermine the division between "internal security" and "external security", "military action" and "police action". War studies, that have informed doctrines with concepts and expertise, have particularized and situated

[1] For a sociological stance on war studies disputation, see: Linhardt and Moreau de Bellaing, 2013.

those dynamics of knowledge into the aesthetic of postmodern conflicts (e.g. Mälksoon, 2018) which, in turn, guides strategic investments and operations.

According to western military experts (Lasconjarias and Larsen, 2015; Lopling, 2018), NATO's definition cited above was a reaction to the release of Russia's 2014 military doctrine of "non-linear warfare" – itself presented as a reaction to the threat that NATO would represent for Russia – and the growth of political tensions since the invasion of Georgia in 2008 and the annexation of Crimea and Donbas in 2014. Although war studies usually consider the NATO definition of hybrid threats insufficient to address the phenomenon, it does provide three elements to grasp the problem that has arisen for the Euro-Atlantic Alliance in this context. First, hybrid threats tend to defy the framework that western states have historically imposed, by undermining the lines between the rules of war and peace, criminal and enemy, activists, terrorists, mercenaries and regular combatants. In that perspective, war and peace are no longer opposed but rather paired into institutional arrangements, thus disrupting the normalcy established through concepts like nation-state, sovereignty, borders, and so on. Second, the target of hybrid threats is not the state – for example through a strategic infrastructure or a battalion of regular forces –, but society as a whole. By challenge the nature of reality and suggesting a "real" reality hidden beneath the official one, they open up the possibility of contradicting the framing offered by the state (see the political technology of non-occupation by "little green men" in Crimea and Donbas, Yurchak, 2014). Third, the determinants and spatiotemporal delineations of hybrid activities remain largely implicit, but are distinguished by an ongoing possibility of the revival of war, reshaping collective arrangements even in the absence of attacks. In this sense, the term "hybrid threats" has brought together different actions and knowledge, from media disinformation campaigns to terrorist activities. In doing so, it has introduced an additional element to the military doctrine of NATO that has gradually extended debates on war and (in)security in Europe beyond military spheres.

The analysis of this strategic and security situation has been entrusted to the European Center of Excellence for Countering Hybrid Threats (CoE Hybrid), an institution created in October 2017 in Helsinki. The CoE trains civil servants from NATO members and partner countries and provides them with expertise drawing on case studies and retro-engineering. NATO's civil-military intelligence and security division has also dedicated a

new branch to hybrid threats analysis. NATO allies putting in battle order around this category have encouraged not only a fresh look at practices around influence, but also a rethinking of the national legal and institutional arrangements in terms of strategic communication, military cooperation, crisis response and cyber defense. In other words, the eruption of the terminology of "hybrid threats" has given rise to reflexive operations on the merits, the democratic response or the recharacterization of the common enemy of Europe that materialized in institutions and technologies. In this way, Europe is understood as a Euro-Atlantic assemblage of ready-for-war states concerned about the Russian military agenda, while European subjects are passive targets protected by reactive military forces.

Some of the political staff and civil servants concerned have, however, been destabilized by the success of the notion "hybrid threats". This is not just a disagreement over the terms of the definition of war; hybrid threats have appeared to them as an Anglo American politization line, aimed more or less skillfully at performing an anti-Russian coalition in Europe.

It is an understatement to say that when our diplomats saw the notion of "hybrid threats" coming up, and then the creation of an institution dedicated to this subject [CoE Hybrid], they took a dim view of it. Not only the French, but many chancelleries and military headquarters were very skeptical (Interview with a French Diplomat, August 2020).

Even though some diplomats are suspicious about the evolution of NATO's military doctrine, and certain war studies experts claim there is not much new in hybrid threats, which are simply a reflection of the evolving nature of modern war (Lasconjarias and Larsen, 2015; Lopling, 2018), their misgivings have not prevented the emergence of a growing space for debate. Since 2015, an increasing number of experts and civil servants have been discussing concerns about information and measures that were previously considered ideologically suspect – mostly because they were seen as overtly "anti-Russian". Another French diplomat summarized thus the new starting point for the debates: "[Everything] starts from the moment when you can influence elections; votes are the basis of the legitimacy of the state in international relations" (Interview, July 2020).

The EU's Concern about Disinformation

As early as 2016, the European Commission (EC), the European Parliament (EP) and the Council of the European Union (CEU) issued a joint communication echoing NATO's concerns about hybrid threats in Europe (EC, EP, and CEU, 2016). Without mentioning explicit states or non-state actors, like NATO does with the Russian Federation and the pro-Russian groups, they examined the feasibility of applying the solidarity clause of the Lisbon Treaty (in case of a wide-ranging and serious attack) and proposed closer cooperation between the European Union and the NATO countries (see also: NATO and EC, 2016).

In 2018, after intense discussions, some EU member states' fears about Russian "disinformation activities" took precedence over the hybrid threats issue in EC public communication (EC, 2018a). Disinformation was defined as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm" (EC, 2018a, p. 2). The notion of hybrid threats was used to qualify aggressive acts, but outside the EU – especially in Ukraine –; it was not central to the EU's internal affairs and remained attributed to NATO. With this semantic split between internal and external affairs, the EU's institutional answer was, however, the creation of the Hybrid Fusion Cell, established within the Intelligence and Situation Centre of the European External Action Service. Hybrid threats were thus considered as foreign affairs, and were *de facto* left to the initiative of NATO and the member states. The EU's take-up of the disinformation issue, supported by another influential task force, was nevertheless grounded in NATO's preoccupation with preparation for a new war.

Since March 2015, disinformation has been handled by the 16 members of the External Action Service's East StratComm task force, gradually expanded to include teams from the western Balkans and the southern part of the Union. Initially focused on the pro-Kremlin media, this group monitors the European public space (including that of EU Member States and partnerships) with the aim of alerting people to the state of the "Russian threat" and producing a counter-discourse for the population. This involves the online detection, analysis and exposure of disinformation campaigns on the euvsdisinfo.eu website. Thought of as external action, the initiative specifically aims at civil society and democratic institutions in the Eastern Partnership of the EU (Armenia, Azerbaijan,

Belarus, Georgia, Republic of Moldova and Ukraine), but also focuses on member states' public space (see Figure 1, for the Czech Republic). In addition to a large European public space analysis, the East StratComm task force has established a rapid alert system that has set legible contact points for monitoring in public administrations, and supports independent media in the Eastern Partnership through training and funding. In EU public communication, all of these activities have increasingly mobilized the notion of "Europe's digital sovereignty" in an explicit but often vague way – alongside "democracy" and "security" –, and have pointed to Russia as a main culprit of disinformation activities.

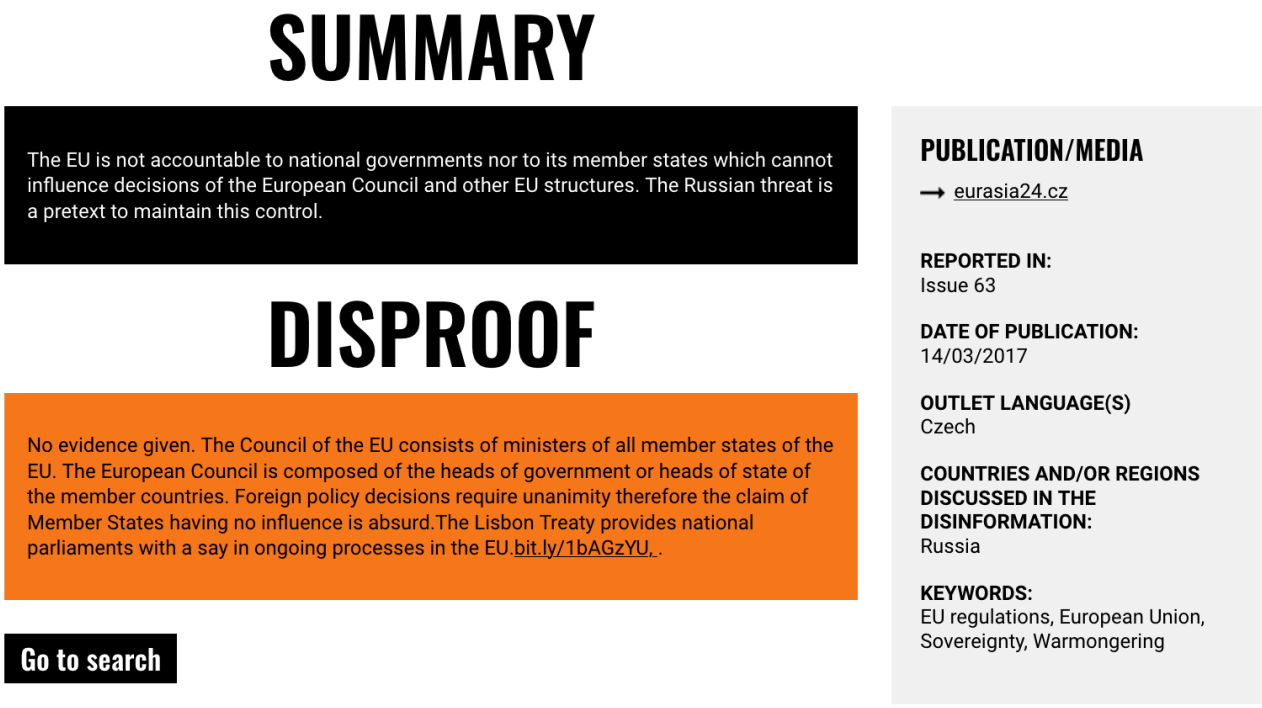

Figure 1 Example of disinformation detected on a Czech website, analyzed with regard to European treaties and published on euvsdisinfo. The case shows both the strategic position of sovereignty and the political dimension of disinformation, which cannot be reduced to the assessment of erroneous, falsified or manipulated facts or facts that resemble opinion.
Available at: https://euvsdisinfo.eu/report/the-eu-is-not-accountable-to-national-governments-nor-to (accessed, 08/10/2022).

In December 2018, following a report by a group of experts (EU experts, 2018), two communications (EC, 2018a, 2018b), and a code of best practices (EC, 2018c), and grounded on NATO's concept of "hybrid threats" in military affairs, Europe adopted an action plan against disinformation (EC et al., 2018). This gave the above-mentioned

expert group's work a wider impact and more financial means. The representatives of the member states saw the document as an opportunity to test the coherence of "Europe" behind the figure of the whistleblower warning about Russia, and to clearly see the differing degrees of hostility appear among the member states and institutions concerned. A dispute on the performativity of keeping out "the enemy of Europe" thus appeared in diplomatic arenas. The Baltic States, Poland and the UK led the enemization movement. They mobilized recent history by rereading Brexit as an event fueled – if not provoked – by Russian trolls, and associated it with the Soviet propaganda and infiltration that had targeted public opinion during the Cold War. While they were encouraged to point to Russia as Europe's common enemy, member states like Germany, France and Italy were reluctant to attribute attacks to Russia, and drew attention to other adversaries (China, ISIS, North Korea, etc.). "We have received numerous requests in Europe (especially from the British and the Baltic states) and we have seized the opportunity to present a more nuanced position towards Russia", commented a French diplomat (Interview, August 2020). They also promoted a broader perspective on the digital sovereignty issue, including regulation of digital platforms and the promotion of European technologies above those of the US and China. I will come back to this in the second part.

The Europeans Against Disinformation program has permeated the policies of the Union and has steadily strengthened since 2018. The most edifying public accomplishment is the Commission's Action Plan for European Democracy, adopted in December 2020 (EC, 2020). The plan shows a shift from traditional concerns such as the promotion of public participation, to the protection of elections (defending electoral infrastructures or preventing hacking and disclosure) and the fight against online hate speech. Countering disinformation has a dedicated chapter in the action plan, in which it is noteworthy that China has discreetly joined Russia on the list of states that have launched "influence operations and targeted disinformation campaigns on covid-19 aimed at undermining democratic debate, exacerbating social polarization and improving its own image" (EC, 2020, p. 19).

Public documents produced by the European institutions between 2015 and 2020 show the spread of NATO's problematization of warfare in Europe through the issue of hybrid threats. Originally associated with Russia, hybrid threats were then reformulated in EU expert arenas around the issue of "tackling disinformation in and at the borders of the

EU" and "preserving digital sovereignty", which has shaped European political and technical infrastructure beyond institutional boundaries. No solid legal categories and standards have emerged from this infrastructure. It is a military-oriented doctrine, a network-building between member states, and an agreement on a figure of the enemy: the Russian Federation and its allies, be they trolls, hackers or pro-Kremlin media content spread in the public spaces of the EU and the Eastern partnership countries. As a result, a technological zone (Barry, 2001) connecting early warning services, intelligence gathering, and continuous analysis of the public space has been stabilized. It is governed by a specific temporality: anticipation of an attack that implies reactivity both of the armed forces and civil society. In this configuration, military forces, fact-checkers and independent journalists constitute both the main figures of European subjects and the front line. The success of this problematization has decreased the legitimacy of alternative ways of defining "Europe" (e.g. a Europe including Russia, as the Council of Europe did until the 2022 invasion of Ukraine), so that European categories, tools and values have to some extent been rethought in light of this warlike orientation.

Demarcation in Network Building

Networking Europeans concerned by disinformation replicates the Rapid Alert System for Food and Feed (RASFF), created in 1979 as a key tool to react swiftly when risks to public health are detected in the food chain. Such Rapid Alert System activity contributes to an "infrastructural Europeanism" (Schipper and Schot, 2011). Yet, as Marres argues, unlike food that can be removed from stores, "We can't have our facts back" (2018). Although the system can flag disinformation "from external sources" (see Figure 1 for the countries and/or regions discussed with regard to disinformation), it is unable to remove content from the web or to stop its circulation online and offline. So, what is the purpose of the system? In socio-political imaginaries spawned by process modeling and public communication, monitoring appears to be at the head of the operational chain countering disinformation. In France, the chain has been formalized in four military-inspired operations: monitor, detect, characterize, and respond. Monitoring, a sovereign activity consisting of surveillance of the public space in all its complexity, is claimed to have become indispensable to the continuity of democratic life guaranteed by the state. It relies on huge technological investments in digital tools, to spot attacks in real time, to sound

the alarm, and thus to preserve public debate as much as possible from purposeful damage.

Political staff and senior civil servants value disinformation monitoring, especially on social media, as it can provide immediate feedback on public action and on political and institutional communication. It allows them to answer certain questions asked by political analysts, including whether a social movement such as the Yellow Vests, Anti-Masks or Extinction Rebellion has been propelled, encouraged or amplified "from the outside", and thus to change the consideration of the claims. The uses that I observed in France during my fieldwork testify that monitoring the public space completes popularity ratings of polling firms. A social network analyst commented that ministerial cabinets have in recent years become "addicted to social network analysis of disinformation" and that "even some ministers themselves spend 20 minutes a day reading these memos" (Interview, September 2020).

Paradoxically, while the tasks involved are considered highly technical, this monitoring is discredited and low-paid, to the extent that the agents performing it are sometimes thought to be almost replaceable by machines. Yet they are also deemed to "perform digital sovereignty"[2]. The observation of interviews and meetings suggest both frustration among those who are constantly learning new tools and read in several languages, and a series of misunderstandings about the content and expectations of their job. In routine work, monitoring is never exclusively oriented towards disinformation; it also highlights trends in topics, for governments (the reception of a reform announcement, for example). "We don't dismantle [criminal] networks, we don't program stuff [cyberweapons], it's speech extracted from the public space!" (Interview with a foreign affairs monitor, November 2020). Like her, I posit that with disinformation monitoring there is recurrent confusion between intelligence gathering and thematic analysis of the public space.

In spite of the investments in monitoring, the European Rapid Alert System has not been triggered. It has been used only as a professional network to share national experience, and "infrastructural Europeanism" seems to be very fragile. The difficulty that has arisen since 2019, since the creation of the network and the publishing of the

[2] On these mechanisms of silence and visibility in computer-supported cooperative work, see: Star and Strauss, 1999.

action, has been to define, in everyday practice, what disinformation is or is not, and therefore what a threat is or is not. First, the labeling – called identification – supposes a clear demarcation between internal and external threats. Yet, establishing the evidence that a piece of information was externally provoked is arduous and requires technical investigation. Some member state representatives and experts have introduced doubts about the methodology used, in particular on the euvsdisinfo website. They argue for a strict separation between, on the one hand, threat hunting, critical infrastructure protection, and responding to incidents, and, on the other, attribution that is considered in cyber security literature not only as one of the most intractable problems for computer scientists, but above all as a political act ("what states make of it", according to Rid and Buchanan, 2015). From a technical point of view, robust outcome depends on attributive evidence in metadata, which can easily be manipulated. For example, it can be rewritten with the Cyrillic alphabet or aligned with the Moscow time zone to point to the most famous culprit. It also implies analyzing the replicated nature of the phenomenon (i.e. identifying bots and action plans), and locating the origin of the attacks (e.g. with traffic analysis). Second, the effort to build an unambiguous demarcation is inscribed in detection and warning systems, but these systems are evolving fast. Moreover, despite heavy investments in machine learning tools, the construction of consistent demarcations takes time and its stabilization leaves the attacker the time and means to revise their methods. For instance, beyond the success stories brandished the day after the presidential election, the investigation on the Macron Leaks mentioned above required considerable means and nearly two years of investigation (Jeangène-Vilmer, 2019). Simply put, the results have fed European case studies but came too late to be valuable feedback for cyber defense. Disinformation practices are, furthermore, becoming increasingly sophisticated. Third, cooperation between European intelligence services in the CoE Hybrid and Fusion Cell has not been straightforward, and publicizing the analysis revealing a damaged infrastructure and an attacker is not perceived by all as strategic. The nuanced and multi-layer Macron Leaks analysis reports forensic clues that French representatives are reluctant to release. Although Russia was publicly held responsible in 2017, the defender's forensics found that not all perpetrators are traceable to the Russian Federation. American far-right movements were deeply involved, but as the United States is a

privileged ally of France through NATO, it is not subject to the same enemization as is Russia.

Aside from the problematization of Europe and its digital sovereignty through warfare, another problematization of European constitution is emerging at the same time and, to a certain extent, in reaction to large platforms and digital market regulation.

Problematizing Digital Sovereignty into Tech Regulation

In this section, we see the birth of a second problematization of digital sovereignty in Europe, involving the vision of a technological zone where large digital platforms designed in the US and China are regulated. It may seem paradoxical that the construction of Europe as a technological zone for protecting consumers of digital services, employs the notion of digital sovereignty inherited from the modern state framework. It is therefore necessary to explain why and how platforms are presented as an issue requiring both collective investigation by European public administrations, and the building of a regulatory framework protecting digital service consumers. The process presents obvious differences compared to the construction of Europe through the enemization of Russia, but it also has similarities in the reasoning and its inscription in tools of government.

How Large Platform Services Became a Common Enemy

Studying the co-production of digital technologies and Europe, Mager noticed the spread of martial metaphors like "war", "fight" or "battle" in the media to describe the complex negotiation of the EU data legislation (2017). The European identity in data protection was constructed in opposition to "the other", a coherent political entity represented by Silicon Valley companies that have heavily invested in lobbying strategies, with the support of the US government. The martial metamorphosis that fueled the General Data Protection Regulation (EU GDPR, 2016) has shaped the European socio-technical imaginary in digital regulation. After the GDPR came into force in 2018, the process of making an enemy – if not an adversary – out of large digital platforms continued and crystallized. This phenomenon must be understood in a relational perspective: in reaction to the enemization of Russia and the problematization of Europe by disinformation, and in the wake of the GDPR, some of the EU stakeholders have drawn

attention to the political role that platforms play in digital issues. I will focus again on the French case, to understand how platform regulation was put on the EU's agenda. This initiative was certainly not the only one, because its felicity required diplomatic action and congruence with other actors' efforts.

In the mid-2010s, the French Ministry of Education was alarmed by Facebook/Meta's explicit investment in education. For instance, Get Digital! is a project launched in September 2020 to provide, "digital citizenship and wellbeing at school and at home". The firm thus provides ready-to-use lessons and tools to educate young (Facebook) users to protect their confidential information and to stay safe while surfing the Internet (Figure 2). The caring initiative can be read as a way to introduce Facebook to a generation that is more receptive to other social media like TikTok, Twitch or SnapChat. Moreover, without being explicit in its business model, filter bubbles and the kind of liberal citizenship underpinning tips and activities, its lessons aim at encouraging users to share information (thus performing themselves as digital services consumers).

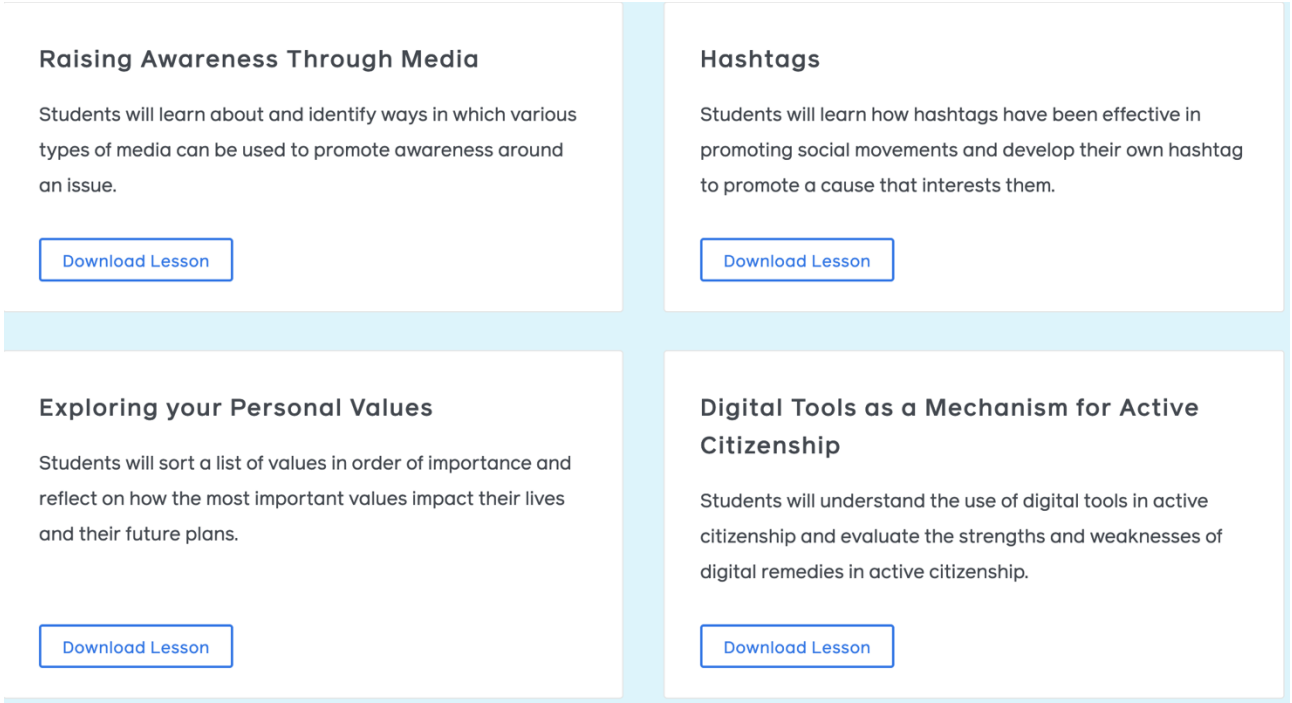

Figure 2 The digital empowerment lessons offered to teachers convey a liberal citizenship project, in which students' political lives involve the use of digital interfaces.

Source: https://www.facebook.com/fbgetdigital/educators/empowerment Accessed: 12/10/2022.

The French Ministry's Education and Media Liaison Center (*Centre de liaison de l'enseignement et des médias d'information*, hereinafter referred as the CLEMI) is involved in

training teachers to help them foster pupils' "critical thinking". It already provides privacy training (not just for personal data), and for that purpose prepares memos to analyze large platforms' educational doctrines. While the CLEMI alerts the European Commission on the influence of foreign high-tech companies, it is unwilling to define Facebook or other platforms as a central enemy, and promotes a critical perspective on all information content. In the aftermath of the 2015 terrorist attacks, the institution had already pointed out the French government's lack of critical perspective on Islamist deradicalization. It considered that scrambling together the categories of deradicalization and countering disinformation proceeded from the same harmful logic of "arming teachers", "general mobilization", "republican response", and "standing up for oneself".

Mobilization is not schools' responsibility! We do not educate against, we educate on, it's quite different, in particular because it puts students back at the center of learning [. . .] We've been very suspicious of the phenomenon of fake news since 2016 because we feared that it would be an entry point to the idea of "arming teachers", of "fighting back", like for deradicalization. (Interview with the CLEMI general delegate, November 2020.)

The CLEMI problematization of digital platform politics found allies among diplomats who were alarmed by the univocal enemization of Russia in European affairs. First, French diplomats were concerned about the invisibilization of other potential enemies, in particular China, whose aggressive diplomatic activities were evidenced in the creation of an international broadcaster, China Media Group, and by the denunciation of the Pasteur Institute during the pandemic. Second, they felt that focusing on state actors would overshadow the fact that platforms make money from disinformation circulating on social media, and that while they have become one of the public sphere's central infrastructures, their moderation policies are not subject to public debate. A senior official of the French Ministry of Culture commented: "[w]e are in a regime of generalized private censorship that no longer questions, at least among the defenders of freedoms in Northern Europe. Today, given the place taken by platforms in the public debate, we consider that this is no longer acceptable" (Interview, August 2020). As a result, since 2018, both French diplomats and Ministry of Education officials have produced case studies and analyses based on doctrine, and tried to raise awareness among their European partners about the need to regulate the platforms. In this attempt, some diplomats acknowledge that the

message has been simplified, to the extent that the focus on critical thinking has been narrowed down to the issue of platform politics.

First of all, it's not easy to push for criticism of one's own communication, and it's even more difficult if it comes from Europe. But we also realize that for some countries, doing "strategic communication" and "counter-propaganda" – like the Baltic States, or the United Kingdom, which is very good at it – is vital, so we're not going to make them move. On the other hand, we are gradually becoming aware that we have a common problem with the platforms. (Interview with a diplomat, December 2020)

The Moral Economy of Regulation Framework: from National Trials to Infodemia

In France, the General Directorate of Media and Cultural Industries of the Ministry of Culture supports the media and defends freedom of expression and of the press by drafting laws, managing aid, monitoring activities, certification, and so on. It has long been interested in the issues raised by moderation and the taxing of platforms, and in 2020 it created a delegation for the regulation of digital platforms. This delegation is dedicated to the economic aspects of these platforms: it produces knowledge on the evolving business models of the platforms, and reports on the effects of the digital transition on the media's and cultural industries' economic models. The delegation considers that the public sphere as it was framed by classical print media has been transformed by digitalization, and that the repercussions thereof on the political process has been neglected by public policy[3]. Unlike the CLEMI, the delegation does not initiate policy in France, but actively feeds the European Commission with memos demonstrating that the regulation of digital platforms is required to restore and maintain a stable democratic public sphere.

Moreover, since 2018, the High Council for Broadcasting (*Conseil supérieur de l'audiovisuel*, hereinafter referred as the CSA) has regulated large digital platforms through the "duty to cooperate". First implemented in 2020 in the context of the covid-19 pandemic, this duty consists not of interfering in social media content, but of imposing a series of obligations on platforms to provide means, on which they report annually by

[3] For a systemic expression of this pessimistic view, see Habermas, 2022.

answering a questionnaire. The method for producing local knowledge on platforms can be analyzed as a problem of truth production, or "veridiction", comparable to the stress tests used by the European Central Bank in 2014 when assessing the solidity of banks (Violle, 2017). The answers from the questionnaire are analyzed by the CSA, which then produces recommendations for the following years (Figure 3). Answers and analyses are then published on the institution's website (CSA, 2020). In 2020, this mode of regulation – summed up as the "naming and shaming" doctrine – has been shown to have a certain degree of diplomatic efficiency. After an initial attitude of irresponsibility and arrogance vis-à-vis political institutions, the CSA has noted "with satisfaction" some evolution in the platforms' posture: they have responded for the first time to rather heavy demands, answered additional questions, and provided documents on their internal processes. This does not mean that the CSA has not noted many points requiring improvement, particularly concerning the lack of information provided on human and financial means, and on the intelligibility of the algorithms used. The CSA's role of initiating cooperation has been portrayed to the European Platform of Regulatory Authorities (EPRA) and to the European Commission[4] as a "prototype of future European regulation" (EPRA, 2019). In other words, from the Ministry of Culture to the CSA, it is obvious that the problem of platforms' regulation has to be reformulated to be resolved "at the European level", that is, within the European Union, in order to empower consumers who are targeted by platforms' business models.

[4] EPRA is a network of broadcasting regulators set up in 1995. Members exchange information, cases and best practices on media regulation. 55 regulatory authorities from 47 countries, including EU member states, EU candidates, and EU Eastern partners are members of EPRA.

The CSA makes the following recommendations:

1. It requests operators, in future, to provide it with **details of their procedures for detecting and processing accounts** responsible for the large-scale propagation of false information.
2. It would like to obtain information on **advertising revenue**, even where minimal, generated by accounts that are responsible, or potentially responsible, for the large-scale propagation of false information and that have not been detected and deactivated since their creation.
3. In the interests of user awareness and transparency, the CSA encourages operators to **develop user information** on the measures for controlling such accounts.

Figure 3 "Combatting accounts disseminating false information on a massive scale", the three recommendations following the questionnaire analysis by the CSA. Source: Combatting the dissemination of false information on online platforms: an evaluation of the application and effectiveness of the measures implemented by operators in 2019, English summary, p. 10.

The Covid-19 epidemic has recomposed the modalities of cooperation with platforms. The development of what the World Health Organization had named "infodemia" showed that there could be a risk to public order when certain information was propagated, even when there was no intention or external manipulation. This undermined the idea that every piece of misinformation was an attack, or at least that there was a malicious speaker behind it. Moreover, infodemia encouraged some platforms to take measures to promote institutional information, to increase cooperation with national agencies, and to approach other state institutions to raise awareness among legislators (in the UK and Germany, but also more widely). The political dimension of the platforms' activity has become much more explicit: users have seen the design evolving in a few weeks (e.g. with the highlighting of "certified information"), and public authorities have been canvased (e.g. to encourage young people to vote before the election). In return, they are progressively equipping themselves to decipher the game these emerging geopolitical actors from the United States and China (and subject to their law) play. For instance, since 2021, the French Ambassador for Digital Affairs has designed and maintained for European negotiation purposes an Open Terms Archives, a web service to trace the changes in platforms' privacy terms (Figure 3). It has contributed to building

a more informed diplomacy by objectifying platforms' political action: in the example below dedicated to Alibaba, the tool highlights the addition of an exception "in the event of a national or a regional spread of epidemics or pandemic" during the months following the spread of covid-19.

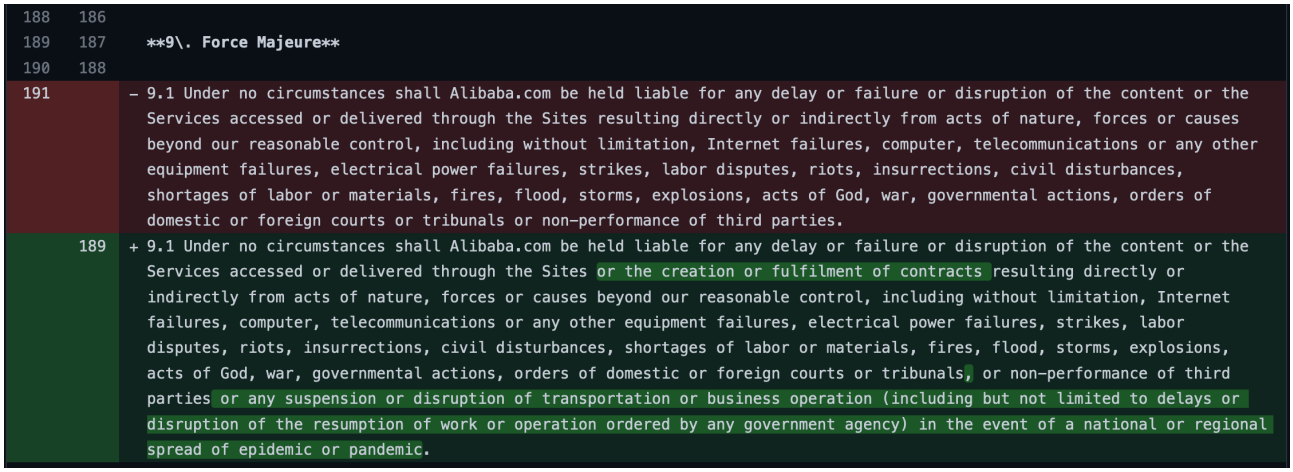

Figure 4. One of the OpenTermsArchives case studies: in June 2020, Alibaba added an exception to the fulfillment of contracts "in the event of a national or a regional spread of epidemics or pandemic".

Source: https://github.com/ambanum/CGUs-data/commit/37503cb23 (accessed: 12/10/2022).

The Waiting Horizon for Digital Services Regulation

The Digital Services Act is an EU Commission initiative stabilized in December 2020 to reform the rules governing digital service providers used by European citizens (2020). This reform is wide-ranging and multifaceted, and involves the creation of obligations for digital service operators: transparent reporting; requirements for conditions of service relating to fundamental rights; cooperation with national authorities; designation of a contact point and, where appropriate, a legal representative; quality of user information; verification of identification information of access providers; and so on. In some respects, the duty of platforms to cooperate with the CSA has successfully been a test for European regulation, as the legislation on digital services ratifies the shift from the logic of results to that of means. The focus of the controversy is thus shifting from publishers to content hosts in a gradualist approach, leading to a distinction between intermediary services, hosts, platforms and large platforms. The latter will be subject to additional obligations: cooperation in the event of a crisis (regardless the contract they write); adherence to a code of conduct; data sharing with authorities and researchers; transparency of

recommendation systems; external risk audits and publicity; risk management obligations; and appointment of a compliance officer.

The text outlines a European understanding of "freedom of information", which involves both the removal of terrorist and violent extremist content online (a consensus practice since the United States joined the Christchurch Call in 2021), and the sorting out of content that is functional and dysfunctional for public debate. It also acknowledges the complexity of moderation, caught up in a metamorphosis of the political genre of outrage, with users increasingly willing to report content and victims more likely to seek redress in this public space. Legal categories that emerge in the Digital Services Act are categories of competition law, tax law, personal data law, mixed with notions of public law (such as the duty to cooperate, public order, etc.).

The designation of platforms as "enemies" started as a political rhetoric, used to perform a socio-political imaginary reactivating GDPR pride that has encouraged new steps in digital consumer protection and opened up perspectives on European public order. The text has thus stabilized a problematization of digital sovereignty involving foreign platforms as enemies of Europe, on which strict rules must be imposed. We will have to wait for the implementation to understand the effects of the Digital Services Package. As it stands, it seems this is not as far-reaching a process of enemization as the one mentioned in the case of Russia, against which the possibility of a new war is envisaged – especially since the 2022 attack on Ukraine. However, since the GPDR was instated it has remained a line of reasoning that has become stronger and more widespread, and that encourages the merging of economic law with public law. It would be necessary here to continue the sociological investigation within the application of the Digital Services Package obligations, to grasp what this hybridization has in common or not with that of the civilian and military law categories mentioned by Linhardt and Moreau de Bellaing (Linhardt and Moreau de Bellaing, 2013; 2020).

Discussion: Digital Sovereignty as Venom? Constitutionalism through the Enemy

Following in the footsteps of STS scholars, I have explored the effects of certain digital sovereignty-related notions on European technologies and political entities, which has enabled the reconfiguring of what is known and imagined as "Europe", and how it is

governed when reclaiming "digital sovereignty". I have examined two problematizations of digital sovereignty in Europe and its shaping of two (un)desirable futures, warfare and regulation, which define different European subjects and objects. On the one hand, anxious States, concerned with protecting populations from the Russian enemy, making independent journalists, fact-checkers and soldiers active subjects of an informational war; and, on the other hand, consumers with individual rights who must be protected from a common enemy by establishing a technological zone, namely that of the large digital platforms. As these platforms are themselves emanations of other states (the US and China), their regulation from the outside is a particularly sensitive issue.

In the construction of Europe, the two problematizations of digital sovereignty share a common feature: the production of both an action and a collective identity in a process of enemization, understood as a reasoning that increasingly proceeds through the construction of a central enemy (Linhardt and Moreau de Bellaing, 2019). Linhardt and Moreau de Bellaing's analysis of what they call the "enemization process" is based on the hybridization of modern legal categories. They found that in legal doctrine, external categories – like "adversary", from military terminology – have merged with internal ones – such as "ordinary criminal" – and have shifted socio-political practices. Concretely, the hybridization of modern legal categories has opened up the possibility of killing through military intervention rather than bringing to justice a person who is defined as an enemy, not as a criminal. The process they describe regarding the concept of enemy in criminal law doctrine was driven by the rhetoric of a drastic transformation of war by terrorism, that would require distinctive legal instruments and devices (extraterritorial law, extralegal kidnapping, indefinite detention without trial in the Guantanamo Bay detention camp, etc.). The authors consider that such undermining of the delimitation of modern categories has weakened democracy.

The process of enemization described in this chapter is not entirely comparable to the definition of enemy in criminal law doctrine, because in both cases the category of enemy continues to refer to an external entity: a state (and its mercenaries), and some big corporations (and the states behind them). There is no enemy within something defined as Europe (which is why Russia was suspended from the Council of Europe in 2022 for example). However, in both cases, I argue that it is a way of making Europe by digital arrangements and through an inimical mode of reasoning that assumes a central and

common enemy. This socio-technical process that points a finger either at Russia or, to a lesser extent, at large digital platforms, testifies to a certain way of co-producing Europe and digital technologies. It is not only the matter of building the "European difference" vis-à-vis the United States (Dratwa, 2012; Laurent, 2019; Lezaun, 2006). This European constitutionalism seems different from those that transcend national orders and reinvent democratic enactments with multiplicity and the desire for common European futures. It produces Europe not in a competitive relationship and by asserting positive values, but by mobilizing a Schmittian characterization of the public enemy (*hostis*) (Schmitt, 1996). The Europe that is emerging from these two problematizations carries the possibility of a confrontation, which can be destructive. Undoubtedly, the categories of competition and harmonization by standards, which are part of a completely different European political order, are strong enough not to leave all the room to enemization. But constitutionalism through the enemy constitutes a radical shift in the way of knowing Europe, and thus a political tension that we can no longer afford to leave out of the debate.

Acknowledgments

This chapter stemmed from a research project on the cartography of the French state's fight against information manipulation, funded by the French Ambassador for Digital Affairs, during 2020–2021. I thank my research partners. The paper has benefited from helpful comments and criticisms by Pierre Alayrac and Blaise Wilfert-Portal, in the "Socio-history of European integration" seminar at the École Normale Supérieure (Paris Sciences et Lettres), where an early version of the chapter was presented in October 2021. I think Alexandre Violle for sharing his desire to describe the socio-technical making of Europe. I am grateful to Liz Libbrecht for helping me to clarify the language. I also gratefully acknowledge coordinators, reviewers and authors from *Project: Europe* for their excellent comments.

Declaration of Conflicting Interests

The author declares no potential conflicts of interest with respect to the research, authorship, and publication.

Funding

The research leading to this publication received funding from the French Ambassador for Digital Affairs, at the French Ministry for Europe and Foreign Affairs. Principal investigator: Marie Alauzen.

Bibliography

Barry, A. (2001). *Political machines: Governing a technological society*. A&C Black.

Bloch, M. (2013). "Reflections of a Historian on the False News of the War." *Michigan War Studies, 51*, translated from the French by James P. Holoka. Available at: https://www.miwsr.com/2013-051.aspx (accessed, 8/10/2022).

Christchurch Call (2019). Christchurch call to action to eliminate terrorist and violent extremist content online. Available at: https://www.christchurchcall.com/christchurch-call.pdf (accessed, 8/10/2022).

CSA, 2020. Combatting the dissemination of false information on online platforms: and evaluation of the application and effectiveness of the measures undertaken by operators in 2019. Available at: https://www.csa.fr/content/download/258905/771715/version/1/file/Combating%20the%20dissemination%20of%20false%20information%20on%20online%20platforms%20-%20An%20evaluation%20of%20the%20application%20and%20effectiveness%20of%20the%20measures%20implemented%20by%20operators%20in%202019.pdf (accessed, 8/10/2022).

Darnton, R. (1984). *The Great Cat Massacre and Other Episodes in French Cultural History*. New York: Basic Books.

EC (2018a). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of religions. Tackling online disinformation: a European Approach. COM/2018/236 final.

EC (2018b). State of the Union: European Commission proposes measures for securing free and fair European elections, Available at:
https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681
(accessed, 13/07/2021).

EC (2018c). Code of Practice on Disinformation, Available at:

https://ec.europa.eu/newsroom/dae/redirection/document/87534 (accessed, 13/07/2021).

EC (2020). Communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions on the European democracy action plan. Available at: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423 (accessed, 13/07/2021).

EC, EP and CEU (2016). Joint communication to the European Parliament and the Council. Joint Framework on countering hybrid threats a European Union response. JOIN/2016/018 final.

EC, *et al.* (2018). Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of religions. Action Plan against Disinformation. JOIN/2018/36 final.

EPRA (2019). Making social networks more accountable: towards a new French framework. Available at: https://www.epra.org/news_items/making-social-networks-more-accountable-a-new-csa-s-recommendation-and-a-facebook-mission-report-to-create-a-french-framework (accessed, 13/07/2021).

EU DSA (2020). Proposal for a regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC, version of 15 December 2020 subject to ordinary procedure, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN (accessed, 13/07/2021).

EU E-commerce (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Single Market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0031

EU Experts Group (2018). Tackling disinformation online: Expert Group advocates for more transparency among online platforms. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_18_1746/IP_18_1746_EN.pdf (accessed, 13/07/2021).

EU GDPR (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (text with EEA relevance), http://data.europa.eu/eli/reg/2016/679/oj

Jasanoff S. (2005). *Designs on Nature: Science and Democracy in Europe and the United States.* Princeton, NJ: Princeton University Press.

Jasanoff S. and Kim S. H. (2009). Containing the atom: Socio-technical imaginaries and nuclear power in the United States and South Korea. *Minerva* 47(2): 119–146.

Jeangène-Vilmer, J. B. (2019). The "Macron Leaks" operation: a post-mortem. Report to the Atlantic Council. June. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/ (Accessed, 13/07/2021).

Jopling, L. (2018). *Countering Russia's hybrid threats: an update*. NATO Parliamentary Assembly.

Habermas, J. (2022). Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere. *Theory, Culture & Society*, *39*(4), 145–171. https://doi.org/10.1177/02632764221112341

Lasconjarias, G., and Larsen, J. A. (eds). (2015). *NATO's Response to Hybrid Threats*. NATO Defense College, Research Division.

Latour, B. (2004). Why has critique run out of steam? From matters of fact to matters of concern. *Critical Inquiry* 30(2): 225–248.

Laurent, B. (2017). *Democratic Experiments: Problematizing Nanotechnology and Democracy in Europe and the United States*. The MIT Press.

Laurent, B. (2022). *European Objects: The Troubled Dreams of Harmonization*. MIT Press.

Lezaun, J. (2006). Creating a new object of government: making genetically modified organisms traceable. *Social Studies of Science*, 36(4), 499–531.

Linhardt, D. and Moreau de Bellaing, C. (2013). Ni guerre, ni paix : Dislocations de l'ordre politique et décantonnements de la guerre. *Politix*, 104, 7-23. https://doi.org/10.3917/pox.104.0007

Linhardt, D., and Moreau de Bellaing, C. (2019). The "Enemization" of Criminal Law? An Inquiry into the Sociology of a Legal Doctrine and its Political and Moral Underpinnings. *International Political Sociology*, *13*(4), 447–463.

Marelli, L., and Testa, G. (2017). "Having a structuring effect on Europe": The innovative medicines initiative and the construction of the European health bioeconomy. In V. Pavone and J. Goven (eds), *Bioeconomies Life, Technology, and Capital in the 21st Century. Palgrave Macmillan*, Cham, pp. 73–101.

Marres, N. (2018). Why we can't have our facts back. *Engaging Science, Technology, and Society*, 4, 423–443.

Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. *European Security*, *27*(3), 374–392.

McFall, L. (2020). Individualising Solidarities. In: Van Hoyweghen, I., Pulignano, V., Meyers, G. (eds) *Shifting Solidarities*. Palgrave Macmillan.

NATO (2015). Statement by NATO Defence Ministers, 95, June 25. Available at: https://www.nato.int/cps/en/natohq/news_121133.htm?selectedLocale=en (accessed, 13/07/2021).

NATO (2018). NATO's response to hybrid threats. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm? (Accessed, 13/07/2021.)

NATO and ECEU, EC (2016). Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Available at: https://www.nato.int/cps/en/natohq/official_texts_138829.htm (accessed, 13/07/2021).

Rid, T., and Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38* (1–2), 4–37.

Schipper, F., and Schot, J. (2011). Infrastructural Europeanism, or the project of building Europe on infrastructures: an introduction. *History and Technology*, 27(3), 245–264.

Schmitt, C. (1996). *The Concept of the Political.* Chicago, IL: Chicago Press.

Star, S. L., and Strauss, A. (1999). Layers of silence, arenas of voice: The ecology of visible and invisible work. *Computer Supported Cooperative Work (CSCW)*, *8*(1), 9–30.

Violle, A. (2017). Banking supervision and the politics of verification: the 2014 stress test in the European Banking Union. *Economy and Society*, *46* (3–4), 432–451.

Yurchak, A. (2014). Little green men: Russia, Ukraine and post-Soviet sovereignty. *Anthropoliteia*. Available at: https://anthropoliteia.net/2014/03/31/little-green-men-russia-ukraine-and-post-soviet-sovereignty/ (Accessed, 13/07/2021).