Digital sovereignty and national security

Claire Landais,
SGDSN,
&
Julien Barnu,
advisor in industry and digital technology

Abstract:
Our digital sovereignty — our capacity for remaining the master of our choices and values in a digitized society — has three complementary aspects. First of all, preserve the traditional elements of sovereignty during an era when digital technology tends to undermine state monopolies: what might be called "sovereignty during the digital era". Secondly, develop in cyberspace an autonomous capacity for making evaluations, decisions and launching actions: "sovereignty in digital space". Thirdly, control our networks, electronic communications and data, which could be described as "sovereignty over digital tools".

Our digital sovereignty — our capacity for remaining the master of our choices and values in a digitized society — has three complementary aspects. First of all, preserve the traditional powers of sovereignty during a new era when digital technology undermines powers that used to be exercised by nation-states alone; this might be called "sovereignty during the digital era". Secondly, develop in cyberspace an autonomous capacity for undertaking evaluations, making decisions and launching actions: "sovereignty in digital space". Thirdly, control our networks, electronic communications and data, in other words, a "sovereignty over digital tools".[1]

Sovereignty in the digital era

New forms of information and communications technology (ICT) have gradually enabled private organizations to rival nation-states, by assuming powers that have historically been state monopolies. This partly irreversible trend should lead governments to decide the powers of sovereignty they want to keep and those that they might delegate to the private sector, if need be within a regulatory framework. Let us make a nonexhaustive list of a few powers of this sort.

IDENTIFICATION OF PERSONS. The social networks are now providing identification on the Web, the leader being Facebook Connect. The services they offer are widely used — at present by private websites and for uses that are not "sensitive". For want of a response by state authorities, these services might, within a few years, become the current means of identification in cyberspace.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in February 2020.

However Europe and France have reacted. These actions involve:

- setting up a French legal framework for digital identifications delivered by the private sector. The Digital Republic Act of 2016 foresees that only those systems of digital identification that meet the conditions set by ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) can be presumed reliable.[2]
- developing a sovereign digital identification system under the AliceM program of the French Ministry of the Interior, while waiting for the rollout of the digital identification procedure on which an interministerial task force is working;
- setting up a platform (France Connect) designed and operated by an interministerial department on digital technology. This should allow for federating various providers, private and public, of identifications for online access to public or third-party services.
- establishing a joint legal framework in the European Union (in particular the EU's so-called "eIDAS" Regulation), which provides for the recognition of identifications between member states and the interoperability of national digital identification systems.[3]

ATTACK AND DEFEND. To cope with constantly growing cyberthreats, some organizations, mainly in the United States, are challenging the state's monopoly on the legitimate use of force and advocating an offensive doctrine for responding to attacks, which would authorize private organizations to launch ripostes ("hack back"). This is founded on a moot interpretation of the right of legitimate defense. The risk of that some countries legalize hack-back practices is quite real, as well as the risk of their international diffusion.

Allowing private parties to conduct offensive actions will worsen instability in cyberspace, since uncontrolled ripostes risk targeting innocent third parties or wreaking collateral damage. Given this, France has chosen to continue forbidding this practice and actively work for an international ban on it, whence the "Paris Call for Trust and Security in Cyberspace", published by the minister of Foreign and European Affairs on 12 November 2018 at the Paris Peace Forum and advocated by the president of the French Republic during his speech at the Forum on Internet Governance at UNESCO.[4] This was an occasion for reasserting a state monopoly on the legitimate use of force. This call is now being discussed in various forums, in particular the OECD and UN.

DOMESTIC SECURITY. The effectiveness of our intelligence and of the services that undertake legal investigations depends on forms of digital technology that are in short supply on the national and European markets. As a consequence, we depend on foreign offers to, for example, process big data. State authorities must work with industry to come up with national or European solutions. In pursuit of this objective, the Council on Innovation decided in April 2019 to issue a competitive challenge on the question of applying artificial intelligence to cybersecurity: "*How to automate cybersecurity to make our systems robustly resilient in the face of cyberthreats?*" The purpose of this challenge is to come up with innovations to the benefit of firms for detecting sophisticated breaches in information systems and automatically correcting flaws.

Other trends of this sort might be mentioned, such as the cryptocurrencies that are undermining the state's monopoly over issuing money. However this question falls outside the competence of the SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale, an interministerial organ under the Prime Minister's Office).

[2] Act n°2016-1321 of 7 October 2016 for a "digital republic" available at https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746.

[3] EU Regulation No. 910/2014 of 23 July 2014 on "electronic identification and trust services for electronic transactions in the Internal market" available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[4] Available via https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf.

Sovereignty in cyberspace

The second facet of our digital sovereignty is to maintain the capacity of the state and, in a way, of our firms and citizens to have an autonomy for evaluating, deciding and acting in cyberspace. As for the state, France has chosen to have the means for maintaining an autonomy of decision-making in matters of defense and security in cyberspace. Reaching this objective depends on three factors.

First of all, THE SOVEREIGN CAPACITY FOR DETECTING CYBERATTACKS against the state and critical infrastructures. ANSSI has developed its own detection systems for monitoring public administrations; and industrialized solutions have been worked out for building confidence to the benefit of French firms. In April 2019, ANSSI certified two French manufacturers' detection probes. In addition, the program act for the armed forces for the period 2019-2025 has considerably bolstered our national capacity for detection. It allows ICT operators to set up means of detection in their networks and ANSSI to deploy a probe on the network of Web hosting services infected by hackers. These provisions are now being put into practice.

Secondly, THE SOVEREIGN CAPACITY FOR ATTRIBUTING CYBERATTACKS. The choice to develop and maintain this capacity signals a major commitment. The ability to determine a cyberattack's origin will soon be a power in the hands of a very small number of countries, namely those that will have made the strategic choice to develop it.

Finally, A NATIONAL DOCTRINE OF DISSUASION AND REACTION based on:

- a national method for assessing a cyberattack's severity that takes account of our legal standards (the penal code, code of defense, the EU's General Data Protection Regulation, etc.). In response to a call from the *Revue stratégique de cyberdefense*, all parties active in cyberdefense have drafted a paradigm for ranking cyberattacks.[5]
- a national doctrine for responding to cyberattacks. This doctrine ensues from the principle that any response is a political decision to be formulated on a case by case basis in the light of international law. The response might involve a public declaration about the attack's origin, the adoption of countermeasures or even (insofar as it cannot be excluded that a cyberattack might reach the threshold of an armed attack) the recourse to legitimate defense under Article 51 of the Charter of the United Nations.
- offensive capacities for coping with the risks of armed attacks by having military options for a response in cyberspace (and other environments). Cyberweapons are now a full-fledged part of the operational capacities of armed forces, and a doctrine determines the conditions for using them in military operations on the theater of foreign operations in compliance with international law.
- the international promotion of France's view that: *a)* international law applies in cyberspace; and *b)* a public declaration about the origin of an attack is a political decision, a matter of sovereignty that a structure based on alliances, such as NATO, cannot make.

For our firms, the goal is to maintain a capacity for innovation in a context of hegemony (the American ICT giants); but this question lies outside the SGDSN's competence.

As for citizens, their autonomy to make evaluations and decisions is related to the sincerity of the democratic debate about the manipulation of news and information by foreign powers. Though preponderant in the fight against such manipulations, the state's role (regulation, incentives, international cooperation, etc.) must be sustained by relays in "civil society". Its key objective should be to reinforce our democracy's "antibodies" through the quality of public debates, the accountability of platforms for their operations, education in using the social networks, and pluralism.

[5] Review published by the SGDSN. See http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/.

Sovereignty over digital tools

Digital sovereignty also involves our capacity for protecting telecommunication networks and the data that pass on them against espionage and sabotage.

In matters related to the security and resilience of networks, legislative measures over the past several years have provided for a control of the core equipment in networks. Given the growing importance of mobile networks and, in the near future, of 5G and the new uses stemming from it, the legal framework has had to be modified. Accordingly, Act n°2019-810 adopted on 1 August 2019 requires that ICT operators "of vital importance" obtain in advance an authorization from the Prime Minister's Office for using certain types of equipment in mobile networks.

Control over our networks also entails protecting the undersea telecommunication cables essential to our economy. Besides reinforcing protection, the government is carrying out an ambitious policy to make France attractive for the laying of cables. By multiplying the number of submarine cables that arrive at land stations in France, flows of international telecommunications will be more resilient.

To protect the communications and data of the state, firms and citizens, the issues are so varied that France's objectives should be discussed by sphere of activity:

- For CLASSIFIED data and communications, we should require that they be protected against targeted attacks from highly skilled enemy forces. This implies national control over certain forms of technology — at the top of the list, encryption. In this domain, France has a trusted industry capable of providing high-level, certified security equipment for protecting exchanges of data classified as "top secret". Maintaining a national industry on the cutting edge in this field is an absolute priority.
- For SENSITIVE data and communications, we should set the requirements to which the digital technology used by the state and critical operators will be subject. Trying to satisfy all needs with purely national solutions is not realistic. Without actually excluding foreign suppliers, this objective means that France should have an industry of trusted technology that can make elementary security bricks and design complex systems by integrating foreign bricks.
- For the economy more broadly (specifically for the cybersecurity to be provided to firms that are not of vital importance) and for citizens (to protect their uses of digital technology), the state must preserve its capacity for influencing the decisions that firms and citizens make about electronic technology. To do this, it must point out quality solutions but without imposing them. For this purpose, ANSSI will gradually generalize its certification procedures in order to foster the adoption of the best solutions. These procedures will become even more pertinent for economic reasons as they are expanded on the European scale, as allowed under the EU cybersecurity regulation that the European Parliament adopted on 12 March 2019.[6]

This three-pronged approach also holds for questions related to the cloud. For its classified data, the state will exclusively use its own cloud. For other sorts of public data and for firms, the classification of clouds by ANSSI will be helpful when making a choice among the offers (not necessarily from national suppliers) that provide sufficient guarantees against technical risks (*e.g.*, attacks on computers) and legal risks (*e.g.*, the pressure to hand data over to foreign authorities).

[6] See https://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html.
& https://eur-lex.europa.eu/eli/reg/2019/881/oj.