Isolate your Internet?

Kavé Salamatian,
professor of computer science at Savoie-Mont Blanc University

Abstract:
This update on the questions of sovereignty and control over the Internet borrows a cyberstratégic approach to the question: "Can you isolate your Internet?" As this approach shows, governments could take control of their national network, but this would have a heavy cost. It would require not only strong political determination but also the adaptation of the regulatory and economic environments of the digital realm. The cost of taking control could soon exceed the hoped-for benefits and even turn out to be counterproductive. Thought about this question calls for a global, strategic, long-term vision, since the position adopted can have an impact that reaches much farther than imagined.

The Internet is inescapable in our contemporary world. This major vector of the digital revolution is deeply altering societies. Ever more services and organizations "of vital importance" are "on" the Internet. The Internet is a cyberspace where we increasingly project our lives socially and economically. As a consequence, it and the networks that make it up figure among a state's strategic equipment.[1]

While states want to expand the scope of their sovereignty to this network of networks, this is not easy to do. In recent years, we have observed several instances of a total shutdown of the Internet within a country for obviously frivolous reasons, such as the prevention of cheating during secondary school examinations. However the reasons given for most shutdowns are related to national security or the protection of the population during a local or national rebellion. An interesting study, which has raised questions about the effectiveness of such measures, has shown that large-scale shutdowns fuel violence instead of reducing it.[2] This is evidence that shutdowns of the Internet come with economic, social and political costs for the country that are hardly offset with any direct benefit. As these cases have demonstrated, a country can be isolated from the Internet, but this sudden isolation frequently wreaks the opposite effect of what was expected. Over the past few years, the question of state sovereignty over the Internet has cropped up, again. This sovereignty implies the capability of actions on the network at the scale of a country.

The cyberstrategic approach adopted herein seeks to examine the scope of state control over (the part of) the Internet within its borders. This helps us describe several ways that states have tried to exercise sovereignty over the Internet.

By paraphrasing the classical definition of strategy, cyberstrategy can be defined as the "art of positioning, directing and governing one's cyberforces in cyberspace for the purpose of attaining cyberobjectives". With regard to the question of isolating the Internet, this definition implies specifying these "cyberobjectives", listing the "cyberforces" that face each other, and delimiting the field for maneuvers 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 2021.

[2] ROUSSELOT F. (2019) "Shutting down social media does not reduce violence, but rather fuels it", 29 April, *The Conversation*, available at https://theconversation.com/shutting-down-social-media-does-not-reduce-violence-but-rather-fuels-it-115960.

Cyberobjectives

For nation-states, the Internet is a strategic component. Thanks to digital technology, a wide range of services has been placed “on line” that used to be managed “off line”. Connectivity to the Internet has thus become a necessity. It is even vital for a growing number of business and state services. Given globalization however, the scope of connectivity is not just national. International exchanges have considerable importance for organizations of vital importance and economic agents. Counterbalancing the importance of international connectivity are regulatory and geopolitical considerations. A first cyberobjective is to guarantee the domestic connectivity of services of vital importance and of the national economy. When deemed desirable, it can be extended to international connectivity within the bounds set by regulatory and geopolitical considerations.

A second point to ponder: the Internet responds to needs in communication that, though not vital, are important for social and political reasons. Freedom of speech and the fluidity of exchanges affect citizens’ confidence in their government and economy. Connectivity is, of course, double-edged since it also enables malevolent persons (domestic or foreign) to undermine this confidence in government. A second cyberobjective is to balance the social, political and economic benefits of the free circulation of information with the risks that this freedom brings in terms of a loss of confidence in, or of control over, the information circulating on line.

A final point has to do with cybersecurity. Over the past few years, government-related forces in one state have made cyberattacks against vital infrastructures in other states. Examples of this are: the Stuxnet virus that targeted the Iranian nuclear program and the cyberattacks that, blamed on Russia, targeted Estonia in 2007, Georgia in 2009 and 2020, and Ukraine in 2017 and 2018. States are also worried about attacks by cybercriminals, mafiosi or even terrorist groups. These fears are to be borne in mind when setting cyberobjectives.

By balancing contradictory requirements, setting cyberobjectives is a political action in the highest sense. Deciding whether to shut down the Internet in a country or to exercise sovereignty (in one way or another) over a country carries very heavy political implications. It is an indicator of the cyberstrategy adopted by the state in question.

Cyberforces

Setting cyberobjectives serves to identify cyberforces, such as “organizations of vital importance”, regulators, security forces, economic agents and citizens. To these let us add network operators, Internet service-providers and high tech firms as well as universities and establishments in education and research (industrial and academic).

Network operators provide connectivity to the Internet, the field where other cyberforces will conduct maneuvers. Nation-states often have a “historical” public operator, who used to have monopoly over telecommunications within the country. This setup, which still exists in many lands, has a drawback: high prices due to the lack of competition and a diminished capacity for investments — in a context where Internet service-providers are busy and capital hungry. The role of network operators is to install an expensive infrastructure that has to be amortized fast to keep pace with rapid changes in technology.

The historical setup is being replaced with a competition-driven model. However a competitive marketplace is to be kept under the oversight of regulatory authorities (who exercise variable powers, purely economic or broader). Allowing foreign service-providers into the game is a sensitive question. Foreigners are needed because they put up the much needed capital and also bring the offer of international connectivity. However their presence raises questions about the competent jurisdiction in cases of litigation and about security and the position to be adopted in the state’s strategy. For these reasons, some countries have forbid foreign players, sometimes by forcing them to be “hosted” by, or form partnerships with, local players.

Whereas some states separate the Internet's economic aspects from its security implications, others have placed security at the center of their decision-making. Some states consider the Internet to be a "whole", a space of information encompassing the technical infrastructure, the services deployed thereon and the information circulating there. For them, as in the case of China, a central authority sets the rules and has to manage this whole space. The Cyberspace Authority of China (CAC) is in charge of all dimensions of cyberspace and directly under the president of China. Other states have organized the Internet in compartments — the infrastructure, contents, cybersecurity, state security — that are regulated independently of each other. France has adopted this approach: ARCEP oversees telecommunications; ANSSI, the security of information systems; and the DGSI, state security, in particular for matters having to do with terrorism and espionage.

Networks usually arise out of a process of "emergence" — an undirected process of microscopic interactions between relatively independent parties that has concrete macroscopic results. A network takes shape out of individual, microscopic interactions between players who decide to invest in order to connect with each other, but this usually takes place under a regulatory framework that limits the space of possible actions. When there are no regulations, the parties involved tend to form a "small-world network", where the average distance between nodes is short and cliques of nodes are tightly interconnected.[3] When the decision is to be made to interconnect two nodes, the prisoner's dilemma crops up: the players cannot easily assess the costs and benefits of cooperating (a reliable connection at a high bit rate) or of defections (disconnection or a lesser quality of services due to overused resources). As a consequence, players minimize connection costs while protecting themselves from defections by making more connections. These structures are resilient owing to their build.

However the existence of regulations might force players toward more fragilely designed structures. For example, forcing network operators to go through a single gateway for international connections simplifies traffic control but increases the network's vulnerability to any denial-of-service attack that targets this gateway. Decisions about regulations for networks are complicated, and "butterfly effects" frequently occur — when the application of a "harmless" local decision sets off unexpected, large-scale effects. This "Streisand effect" refers to the situation when the removal of a content deemed offensive sparks an even wider distribution of the content whereas its distribution would have been very limited had censorship not occurred. The decision to isolate a network might seem evident with a short-sighted view of requirements, but it might turn out to cost more than the risk that motivated the decision.

Cloud- and IXP-providers (at Internet exchange points) play a key role in the resilience of networks by offering alternative routes when an outage occurs or attacks block the major routes. Many of them are affiliated with network service-providers, but some are independent groups or user associations. Their existence depends on the market's relative openness, in particular toward foreign investors. However foreign investments might run counter to regulatory requirements. This tension exists in Africa, where the Internet has been "densified" thanks to the many communities of IXP-providers formed in recent years. However most of them rely on aid from the Chinese government, which has offered them Huawei equipment "for free".

Isolating the Internet inside a country makes sense only if there are enough domestic services and contents. This condition is tied to the emergence of a digital economy within the country, but this economy depends on connectivity and a fluid circulation of information. In other words, the determination to control the Internet can be an obstacle to the formation of an active economic ecosystem based on a domestic network.

[3] FALOUTSOS M., FALOUTSOS P. & FALOUTSOS C. (1999) "On power-law relationships of the Internet topology", *Computer Communication Review*, 29(4), pp. 251-262; DOI: https://doi.org/10.1145/316194.316229.

The field for maneuvers in cyberspace

Let us return to our initial question. Can a country's Internet be isolated? Can the field of action of cyberforces be limited without inflicting unbearable damage? A malicious actor would ask the reverse question: "Can I inflict maximal damage by reducing this field of action through cyberattacks?" Although there are many ways to act on connectivity, we can establish a global typology of structures for exercising control.

In countries that have retained a regulatory framework shaped by a public utility monopoly, international connectivity is usually centralized at one or more clearly identified gateways. In his case, shutting down the domestic network is relatively simple: disconnect these gateways. Given the lack of diversity within these countries however, cutting off international connections means that all activities in the country's digital economy will grind to a halt. Furthermore, the concentration of connectivity at a limited number of gateways jeopardizes the network, since attacks by malicious parties on these gateways can knock out the network.

In countries with a more diverse digital ecosystem, cutting off the Internet is more complicated. It requires a "kill switch", which groups at a central point the control of all communication networks. Creating this central point is not easy since all actors, national or international, in the digital ecosystem will have to cooperate. In several states (*e.g.*, China and Iran), legal texts or even the constitution require that the domestic network's backbone belong to the government and be, therefore, fully under its control. These requirements assume that the state has the capacity for making investments and the agility for coping with the growth of traffic on this domestic backbone.

Would it be possible to firmly control connectivity while allowing a thriving ecosystem to develop that would form the grounds for a local, prosperous digital economy? This conundrum is of concern not just to many totalitarian states but also to some Western countries. China figures among the countries that have set up a strict regulatory framework that restricts the activities of foreigners. Since the advent of the Internet in 1987, the Chinese state has separated its Internet into three parts: the domestic network, the foreign network, and the gateways or buffers between them. The Internet is fully under state control, and its backbone has to belong to the state. Contents are filtered at the entrance by China's Great Firewall (GFW). Surveillance is ubiquitous. Foreigners may not set up operations directly on the Chinese network, but they may do so in a limited number of buffer zones (located in Hong Kong and at several points in China). Even when these buffer zones are geographically located in China, they are outside since they are located on the other side of the GFW. The state has designed this setup from the very start of the country's Internet. The Chinese network's architecture did not result from an "emergence" via independent actors, as happened in most other countries. The result is, indeed, by design. The interconnection of the Chinese Internet with the outside world takes place via official controllers at most of the gateways, in particular the dozen points where international cables (under sea or on land) arrive in the country.

In parallel, the Chinese government's protectionist policies (backed by the GFW) support the development of a national digital economy. These policies forbid Facebook or Twitter from having access to the Chinese Internet and considerably slow down Google's operations. They offer incentives for developing digital firms (such as Lenovo, the world leader for manufacturing computers, or Huawei, which ranks second as a builder of routers and first as a manufacturer of smartphones). They have presided over the cession of state firms to private businesses. These policies, which fit into an ambitious strategy for training computer engineers, have oriented major investments in research (academic and private). China could, if it wanted to, disconnect itself from the global Internet. Since the very start, it has designed an architecture for separating the domestic network from the outside world, developed a thriving digital economy and devised a cyberstrategy centralized in the CAC (which, as pointed out, is directly under the authority of the president's office). For economic and strategic reasons however, China has preferred remaining a part of the global Internet.

What about the countries that did not, from the start, set up a system with this sort of architecture and regulatory constraints? To isolate their domestic network, they would have to overhaul the existing architecture, which has usually emerged out of a process. This reconstruction would come at a high price, since interventions would have to be made on a network already in operation. Several countries are trying to do this. I might mention Russia. Since an act of law promulgated at the end of 2019, it is trying to redesign Runet so that it can be disconnected from the global Internet. However the political willpower is not on par with the immensity of the task. The Russian network grew well during the 1990s but sporadically thereafter, a story well told by Kevin Limonier.[4] The outcome is a very well developed network architecture that is very hard to control, even less so given the country's surface area. In ate 2019, the Russian state conducted a full-scale experiment with disconnection in order to draw up a list of the services that depend on international connectivity. To conclude, even though Russia clearly wants to redesign its network, the road ahead is still very long.

One country, Iran, has managed to redesign its network so as to control it fully, improve its granularity and develop a diverse ecosystem of connectivity with a high level of resilience. As in many other countries, the Internet came to Iran via universities and research organizations. The Institute for Studies in Theoretical Physics and Mathematics in Tehran was the precursor in 1994. It is still the domain name registry of *.ir*. As the Iranian Internet underwent fast growth, the regime increasingly felt threatened by it. Following the Green Movement in 2009, the government launched a vast censorship plan. The Stuxnet virus, imputed to the United States, served as the main argument for redesigning the domestic network and making it resilient to attacks and, too, easier to control. It took about ten years to set up the new network. It is now in operation under a "centralized authority of cyberspace", which groups all decision-making about its architecture.[5]

The Iranian case still stands out as an exception. It would not have been possible without international and then American sanctions, which kept other international players out of Iran (with the notable exception of Rostelecom, which, via the Europe-Persia Express Gateway profited from Iran's strategic geographical position).[6] The sanctions made it much harder for a digital economy with international connections to emerge in Iran. Iranian cybernauts have been forced to fall back on local solutions despite their intense wariness of them. In other words, the redesign of the domestic network in Iran was made possible by the joint action of the government's determination to control the network and the sanctions (in particular the American ones) which allowed for no other alternative. The country was caught in this vice.

Conclusion

This article has taken stock of the question of sovereignty and control over the Internet. An approach from cyberstratégy has been adopted to answer the question of whether the Internet can be isolated. As shown, a state can take over its domestic network; but this comes at a cost and requires both a strong political determination and adaptations (of the regulatory environment and the digital economy). The cost of this takeover might easily overshoot the expected benefits, and prove to be counterproductive. This question must be seen from a strategic, global, long-term vantage point, since the position adopted can wreak effects that reach much farther than the set of conditions that prevailed initially when the position was staked out.

[4] LIMONIER K. (2018) *Ru.net: géopolitique du cyberespace russophone* (Paris: L'Inventaire).

[5] For the details, see: SALAMATIAN L., DOUZET F., LIMONIER K. & SALAMATIAN K. (2019) "The geopolitics behind the routes data travels: A case study of Iran", 19 November, available at https://arxiv.org/abs/1911.0773.

[6] https://www.vodafone.com/business/carrier-services/connectivity/submarine-terrestrial-cable/EPEG