Cyberthreats in the 21st century: From playing on borders to forming cybercriminal autonomous territories

Éric Freyssinet,
head of the national pole for fighting against cyberthreats, National Gendarmerie

Abstract:
Cybercriminals play on borders. Defenders, equipped with the same weapons, must learn to control their digital territory and be just as dexterous. They must cooperate to fight against cyberthreats. This means modernizing both models for managing "digital territories" and the legal framework.

Cybercriminality and territories

Information and communications technology (ICT) and even more the Internet have been designed to abolish borders and bring individuals, organizations and people together. Technological reality is quite different from reality in the realm of the law. This situation can be seen as a juxtaposition and interconnection of digital territories with local rules (FREYSSINET 2017) as well as territorial restrictions. In matters of digital security, each information system and sphere of personal information is to be protected from indiscretion and from the intrusions of cybercriminals or rogue states. In this digital realm, which is open by nature, this means re-erecting and guarding borders around the "territory" to be protected.[1]

Protecting a digital territory

To be capable of protecting a digital territory, it has to be precisely and exhaustively delimited. How to sketch this territory's perimeter? Any user of ICT, any firm or organization with a legacy of information to be kept safe and secure (and all of us now have such a legacy) must answer this question. Which data and information systems to protect? Where are they located?

Data can be placed in several categories: those we create, those we acquire, and those that, created or acquired by others, directly concern us. This last category is much harder to define or control. For individuals, it includes, for instance, the set of data about their activities and interactions with a social media platform that is in the platform's possession. For a firm, local authority or administration, this category comprises, for example, blueprints for buildings or the data gradually collected by a service-provider in the course of exchanges and transactions.

Various criteria can be used to classify data, among them: confidentiality or requirements about their availability or their preservation and integrity over time.

This approach via data helps us avoid the pitfall of focusing exclusively on information systems and equipment. We should be concerned not just with the security of the information systems we own but also with all systems that contain or process our data.

[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 January 2021.

A “digital territory” can thus be defined as the set of information systems that each of us owns or that contain or process data belonging to our legacy of information. This implies, by the way, that a significant portion of a person’s digital territory might be shared with other persons, each party having a different or complementary role (as owner, renter, manager or superintendent). A person’s digital territory is not just located in a place that he/she owns or rents. It also refers to other places, maybe in several countries.

The responsibilities of these various parties may be set by use, agreements, contracts or the law. The concept of the party “responsible for processing personal data” is set by law. The EU General Data Protection Regulation (GDPR) allows the data-processor to share responsibilities with a subcontractor. The law thus recognizes the complexity of defining a digital territory.

By stepping back a moment, we soon realize that the digital territory to be defended by a nation-state extends far beyond the country’s geographical borders, reaching out to wherever is located the digital territories of its citizens and firms. Accordingly, the French system of justice has the responsibility for protecting the data of citizens, whether the latter have accounts hosted in Roubaix or Silicon Valley.

Consequences for authorities in charge of the security of digital territories

For persons, firms and the heads of security of information systems, a contract often sets the conditions about overseeing the security of their digital territory. This solution is not scot free in a world where the market enables us to engage service-providers from different jurisdictions. It has a major consequence: we cannot possibly, when thinking about the law in relation to digital security, simply refer states to their geographical boundaries. Instead, we must devise legal tools that allow each state, national system of justice, head of digital security, to protect its digital territory, and exercise sovereignty while respecting the sovereign rights of other parties. This spirit guides current negotiations for a second protocol to the Council of Europe’s 2001 Convention on Cybercrime.[2] This protocol will, in particular, allow judicial authorities in one country to directly request information from an operator in any other country that has signed the convention.

Sometimes however, everyday affairs are simpler than this. Day after day throughout the world, computer security incident response teams (CSIRTs) exchange data about incidents and try to find solutions by directly cooperating with each other. Although these exchanges do not take place under any legal framework, they do respond to a legitimate need and are undertaken under a code of ethics for building trust (EthicsfiRST 2019).

How cybercriminals play on the borders of digital territories

Cybercriminals make light of borders. In fact however, borders, whether between countries or between digital territories, represent both boundaries that criminals have to overcome and allies from which they can obtain protection. Indeed, geographic and political borders are an advantage for these criminals, since they slow down cooperation between cybersecurity teams, hamper investigations, and make it harder to track criminals and their financial transactions. On the other hand however, borders are obstacles for cybercriminals, as for anyone else.

Let us take the case of criminals specialized in “phishing”. Their goal is to collect as many banking details or account identifications for online services as possible. They typically launch their actions from a country where the same language is spoken as by their potential victims. In a nearby country, they then take control of a website where they install their phishing kit while making it invisible to the website’s owner. They then send out messages via e-mail or texting to bait victims. This baiting is often done with the help of a subcontractor who, specialized in spamming, manages a botnet of involuntary client machines that are spread all over our planet while the server in

[2] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

command is located in another country through which e-mail can be rerouted. Once these criminals have collected their victims' data, they look for a black market to sell the data. They do not know where this market is located, since they contact it through the Tor protocol, which they have chosen in order to remain anonymous.[3] They will be paid in a cryptocurrency (often bitcoins), which they will keep or else convert on line into a local currency.

As we see, the main purpose for building this cybercriminal ecosystem is for the criminals to "cover their tracks" from whoever is trying to detect their activities or identify them (FREYSSINET 2013). This comes at a cost: these criminals often have to "trust" unknown parties, pay fees to middlemen and even sometimes risk losing the data they have collected with so much (dishonest) effort.

Cybercriminality during the pandemic

On account of sheltering in place during the coronavirus pandemic in March and April 2020, the reduction in physical mobility severely hampered "usual" criminal activities, such as burglaries and drug trafficking. Not as much can be said about cybercriminality, which increased significantly. In the first quarter 2020, the French gendarmerie recorded an increase of 22% of cases of cybercriminality detected or reported compared with the same period during 2019. The number of cases of ransomware soared (+134%).[4] This trend has continued throughout the year, unstymied by the pandemic.

Two trends were observed during what has been called the "confinement" in French: a massive shift in the themes that cybercriminals used to pitch their in tune with health-related themes; and their relentless efforts to take advantage of points of vulnerabilities in the health sector (while some establishments were relatively disorganized owing to telecommuting). In March 2020, attacks spiked on the Remote Desktop Protocol, which was being used to connect corporate servers to home computers (GALOV 2020). In many cases, RDP had often been configured in haste without paying sufficient attention to security rules. Many of these attacks, everywhere around the world, offered masks for sale by fictive companies. To take a typical example: a French criminal adapted his scam to include surgical masks, hydrogel and coronavirus tests.[5] This episode proves, were proof needed, that cybercriminality makes game of the restrictions stemming from geographical borders.

Are cybercriminals forming autonomous territories?

An emerging trend is the possibility (or ambition) that digital delinquents have to gradually create their own autonomous territories in cyberspace. They try to impose their own rules in the stead of national laws in the country where their clients or users are located. For example, delinquents who manage online retail platforms impose their own rules about access, taxes, fees, comportment and expulsions. Their power might even reach much farther than all this.

[3] Tor, the "onion router", is a protocol for routing a message via at least three intermediate servers so as to mask the addresses of the servers and, too, of those who consult them. This feature is increasingly integrated in Web browsers (*e.g.*, Brave). The websites accessible via Tor have been misnamed the "dark web".

[4] Ransomware encrypts a victim's data while blocking access to them. To obtain the password for unlocking and decrypting the data, the victim is asked to pay a ransom (often in a cryptocurrency).

[5] A criminal identified by the DGCCRF and OCLAESP: https://www.lemonde.fr/societe/article/2020/04/20/coronavirus-une-arnaque-au-materiel-de-protection-a-plus-d-un-million-d-euros_6037114_3224.html

The major driving force in this trend are cryptocurrencies (such as bitcoin, which was launched in 2009). These virtual assets can be traded for legal tender, and thus function like money. Despite their apparent decentralization, their administration is often centralized since a limited number of persons control the procedures for creating the cryptocurrency. We might imagine taking control of these cryptoassets or creating them, even though this would mean recognizing them as a medium of exchange.

A second driving force is the specific nature of what I have called digital territories: they make game of political and geographical borders. The law and technology have enabled the creation of a digital territory under the control of groups who move their business from website to website on the physical platforms of legitimate players in the digital economy or even on the information systems of cybercriminal organizations that flaunt themselves on line.

Leaving too much power take shape around this "virtual independence" carries a heavy risk: legitimate authorities might come under the influence, through corruption, of these strong forces in this parallel economy. Several actions are needed to counter this risk. Attempts by cybercriminals to form autonomous territories in digital space must be detected and broken up. Furthermore, new legal "weapons" must be designed but without hampering legitimate investments and innovations. It is, therefore, indispensable that laws be passed about cryptoassets, in particular about the transparency and accountability of the organizations that control them.

References

EthicsfiRST (2019) "Ethics for incident response and security teams", 5p., available via https://www.first.org/global/sigs/ethics/ethics-first-20191202.pdf.

FREYSSINET É. (2013) "Botnets. Illustration de nouvelles formes de criminalité organisée", *Revue du GRASCO*, 6, pp. 10-18.

FREYSSINET É. (2017) "Appréhension des cybermenaces en 2017. De la cybercriminalité à la cyberdéfense", *Revue Défense Nationale*, 2017/10, 805, pp. 82-86.

GALOV D. (2020) "Remote spring: the rise of RDP bruteforce attacks", 29 April, https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/.