INTERNET GOVERNANCE: NATIONAL SOVEREINGNTY, PRIVACY AND COMBATING CYBERCRIME UNDER THE PERSPECTIVE OF THE CYBERNETIC DEFENSE INDUSTRY

- Area: SET OF INTERNET GOVERNANCE PRINCIPLES
- Entitled by: Fabio Furtado Ramos
- Region: Brazil
- Organization: Axur
- Sector: Private Sector

- Keywords: NATIONAL SOVEREINGNTY, PRIVACY, CYBERCRIME, CYBERCRIME INDUSTRY

Abstract

Our lives have significantly changed in the past decades due to the advent of the Internet and the diffusion of the information technology. We cannot, however, forget that the information technology is not an end on its own, but a way for the development of the society, so that the human beings can reach their maximum potential and for the society to reassure the values of democracy and preserving of individual rights. Something with such characteristics cannot belong to anyone; neither can be controlled or monitored to meet the motivations of a group, whichever those motivations may be. The nature of the internet and base of its conception is to be free and even anarchic - term that suggests an environment not subordinated to the State or any other form of power.With that in mind, national sovereingnty, privacy and combating cybercrimes need to be discussed in an open and frak way so that we can keep its best principles along with the necessary changes to combat emerging threats.

Document

INTERNET GOVERNANCE: NATIONAL SOVEREIGNTY, PRIVACY AND COMBATING CYBERCRIME UNDER THE PERSPECTIVE OF THE CYBERNETIC DEFENSE INDUSTRY

Fabio F. Ramos - framos@axur.com - Fabricio Pessôa - fabricio.pessoa@axur.com

Context

Our lives have significantly changed in the past decades and, if we can relate the catalyzing event of all that change, it certainly is the advent of the Internet and the diffusion of the information technology. We might not be able to actually measure the impact of the information technology in our daily lives yet – not now, while we are sunk in it.

We cannot, however, forget that the information technology is not an end on its own, but instead, it is a way. A way for the development of the society, so that the human beings can reach their maximum potential. It is a way for the society to reassure the values of democracy and preserving of individual rights.

The Internet is the main result of the evolution of information technology. It is a conquest from the plural society. It is the organized global society, source of information, inspiration and consequent evolution from the oral tradition. It is also a source of explicit knowledge for the creation of the true global and has become a primary foundation for the creation and affirmation of the individual and the society.

Something with such characteristics cannot belong to anyone; neither can be controlled or monitored to meet the motivations of a group, whichever those motivations may be. The nature of the internet and the base of its conception is to be free and even anarchic - term that suggests an environment not subordinated to the State or any other form of power, making the monopoly by force inapplicable.

The internet is the network of the networks, interconnecting commercial, academic, governmental and domestic networks. When the American Department for Defense, through its agency DARPA, idealized an alternative for the delivering of information, considering the possibility having communication knots eventually affected by enemy

missiles, it was actually conceiving a communication network that was independent and able to operate without direct control of anyone. This is the real spirit of the internet.

Introduction

In June 2013, the surprising revelations of the at the time NSA technician Edward Snowden showed the world that the national sovereignty and the individual freedom were at risk. The debate about the role of the internet in the relationship between people, companies and the government is a highly relevant topic considering the abuse that has been committed by governments that feel themselves owners, if not of the whole internet, at least of part of it.

The first thing that needs to be clear for the understanding of the position of the institutions that deal with cybernetic defense and security is that their guidelines should be oriented by the main role of both defense and security: protecting the information society, a society that has massively migrated from the physical to the digital and connected world. The role of the Defense and all agents who work to make sure the laws are being respected is to make the internet a safe place.

When the perspective of security and defense are being debated, two are the main points that cause higher inflection: (i) about the impact of the anonymity for the internet as it is now and (ii) about the capacity of a country of being affected by a direct intervention (attack) and/or an existent cybernetic dependence.

ABOUT THE PERSPECTIVE OF THE CYBERNETIC CRIMES AND ANONYMNITY

The cybernetic security and defense exist to protect the information society. It is common sense that the society is vulnerable to the so called cybernetic threats, thus the science of security becomes necessary to preserve the basic attributes of the information: confidentiality, integrity and availability. Disrespect to any of those attributes could generate harm in the micro scale: individuals' interests; and at the macro scale: affecting the critical infrastructure of the information systems of a determined country.

May we like it or not, we live with insecurity in this world since our ancestors were primates and it is so true that to analyze and to mitigate risks are innate attributes for all of us and we do it all the time even in an unconscious way.

In the science of security, mitigate the risk means to apply ways of control and, being aware that the world "control" is cause of discomfort to the ones that, like us, respect and fight for freedom, it is necessary to mention that control can be of a preventive, detective, corrective or compensatory nature.

When of the law enforcement, treating common crimes in a global perspective, the law enforcement agents search for evidences, something that unequivocally relates an action to an individual. In the "real world" this evidence could be obtained by the analysis of DNA found in the crime scene, for example. In the cyberspace, the only way of finding this important correlation, which might mean to acquit someone is through interpretation of audit trails.

There is a forensic principle that can also be applied to the digital world which is called Locard's Exchange Principle. This principle indicates that "every contact leaves a trace", meaning that every time two or more objects meet, there is an exchange of material.

By allowing the unrestrictive anonymity on the internet - which would happen if the metadata of individuals were not stored anymore – we would be switching off the lights of public parks. More than that, we would not only be switching off the lights, but also distributing masks.

Granting the rights of unrestrictive privacy, which could benefit some people, would also

create an environment with perfect conditions for all kinds of crime. Between privacy and anonymity, order and chaos, there is a balance that needs to be found.

We may not forget that the commercial internet is the internet of dot-com. This internet is the same one used by our children and our parents, is an internet where anonymity could generate a very significant impact in people's lives since, as people say "the internet is a permanent mural" that once written cannot be erased. Imagine the internet's capacity of destroying reputations simply because some people trust the internet as an unequivocal source of information, while calumnious data may be put there on purpose with the very objective of spreading false information about people, companies or government.

Imagine the hundreds of hidden services from the darknets emerging at the surface where criminals would find a safe environment for trading organs, human traffic, child pornography, illegal commerce of guns, drugs and assassins. Nowadays, the internet has become somehow dangerous for those criminals and they have migrated to the deepest layers of the web. We could be bringing them back.

But how could we guarantee the anonymity of the ones who want to express their ideas without the risk of being punished by whoever may be interested on those ideas not being revealed? There are already tools for that to be done. Cryptography is far beyond being a sophisticated technical resource to become a technology available to whoever wants to transmit data without having personal information being revealed. For having a mathematical base, cryptographic algorithms may be easily analyzed for verification of its reliability.

One of the alternatives to be discussed by the actors of the internet in the world is the role of the state agencies in which concerns surveillance and maintenance of audit trails (logs) and, mainly, in the confidential storage and control of its use. We do not believe the internet would be better and safer by not keeping records of the actions taking place at the cybernetic environment. In addition, it is necessary to define rights to the civilian agencies that serve as a spokesman of the minorities.

ABOUT THE PERSPECTIVE OF THE NATIONAL SOVEREIGNITY ON THE INTERNET.

It is visible that the critical services of the countries are more and more based on the internet, like bank and post services, mobile communication, electronic government and, not less relevant, applications related to the interests of individuals, Would the countries today have conditions of preserving such important critical infrastructure on their own or they depend on services that are under the guardianship of other States?

We all know the answer. There is an excessive concentration of power on the hands of a few States, while the majority of the other States operate as if they were “clients” of a service. This dependence happens in basic services of the Internet (e.g. DNS), data logistics (e.g. cables and satellites) and applications (e.g. e-mail services, social networks).

When conflicts arise, the internet is even more relevant. Affecting network communications can mean stopping basic services, generating chaos and unmeasurable financial losses. Such a relevant infrastructure needs to be considered as critical by the countries.

The term “information weapon” was created to classify some technological artifacts as “high impact” when operated against enemy installations. Differently from what happens with traditional warlike arsenal which may be difficult to access for the militias, the information weapons can be used by individuals without the need of much resources. The usual form of cybernetic attack is a person with technical competence and a computer connected to the internet. This simplification vulgarizes this kind of attacks.

On the other hand, the concentration of power related to the management of the internet infrastructure gives an expressive advantage to some States in cases of conflicts. This advantage has been built over the past decades, in a veiled way, with investments in technology and infrastructure.

The new conjuncture of power should consider the balance of the forces based on the power of the information weapons, be it for the militias or for the great world potencies.

This is the future of war which will happen at the so called “fifth frontier” – the cybernetic space.

Thinking about the cybernetic space as a war environment is a view that can be validated on some news affirming that some States count on “armies” of at least 50,000 cyber soldiers.

In this context, our proposition is that the new internet governance conjuncture – and resulting distribution of power – may allow a better balance and autonomy of the world potencies and the rest of the world. This is not a simple challenge, as it requires sensitive topics to be discussed in an open and frank way.

ABOUT THE NEED FOR INTEGRATION IN FIGHTING CYBERCRIME

Another topic that needs discussion is related to standards and procedures in fighting cybercrime. The lack of specific laws and regulated procedures, or even the different ways in dealing with them in different countries, makes it easy for cybercriminals to operate in a relative safe way, since they can, for example, steal data from someone in the other side of the world without even leaving their bedrooms. As the frontiers in the cybernetic world are way more open than in the physical world, criminals have changed their way of operating to take advantage of that.

More than an integration of the countries and their intelligence agencies against such crimes, it is very important that everybody involved in that fight exchange information and align their methods to make that fight more effective. It is not only responsibility of the governments and police to engage that battle, since it would be very difficult (not to say impossible) for them to search the whole web for those crimes. Private Cyber Security companies and Internet Service Providers (ISP) should also join that fight so that cybercrime can be combated in an effective way.

Since the methods of investigation of cybercrimes are different from the physical world, it is very important that each actor plays its role: the private cyber security companies

identifying the threats, ISPs removing them from wherever they are hosted and the government intelligence agencies and the police investigating the criminals. It is also important to highlight that different kinds of crimes need different kinds of treatment and this is something that also needs to be discussed. Online fraud, for example, is very different from unauthorized use/commerce of intellectual property and should be treated as such.