***Cyber-Defense theorization***

***By BA, Martin Rodriguez Ossés***

***The importance of Cyber defense concept***

What is cyber defense?

I call Cyber-Defence to the exercise and the precepts of the defense of a nation on critical infrastructure sectors that are part of a digital sovereignty and the rights of its citizens in cyberspace. But it is also the exercise of tools in cyberspace to attack and undermine foreign sovereignties.

When I refer to critical infrastructure sectors of a nation I echo what has been published by Jeimy Cano. These sectors are: a) electricity, b) production c) storage and supply of gas and oil, d) telecommunications, e) banking and finance, f) water supply, g) transport, h) emergency services and government operations.

In the context of the Cyber defense, specific policies and related strategies are applied in what it´s called Cybersecurity to counter several crimes as: Identity theft, electronic theft, abusive access to computer systems and loss of sensitive information in organizations:

Cyberspace is the interdependent network of information technology´s infrastructures, including Internet and other telecommunications networks, computer systems, embedded processors and critical industries controllers. This medium allows individuals and institutions to share and exchange information.

Who are the actors / agents?

In terms of Cyber-Defence the leading actor is the State but not necessarily the most relevant. All actions crossed by the concept are implemented by multiple actors such as: a) individuals, b) collective groups (Anonymous, Lulzsec), c) private companies (owning part of the national infrastructure, computer security companies), d) governments, e) Transnational

Governmental organizations (European Union, for example) f) organized crime, g) terrorist organizations, h) private military companies.

The importance of Cyber-Defence concept

The new irruption modes in cyberspace world lead to new perspectives on power resources; on how to address the concept of defense but, above all things, on the concept of balance of power.

The use of new technologies highlights new capabilities, new resources at the reach of peripheral countries that compromise the balance of power and the international system itself.

The scope of the concept of threat (Balance Threat Stephen Waltz, 1985) is especially altered if we consider that material capabilities are overwhelmed in cyberspace and that resources of cyber defense´s danger lies in the anonymity of them.

Why care so much about cyberspace?

Because it is embracing all known space, exponentially multiplying its users. Generating an almost unstoppable demand for new services and spaces for placing advertising products available to everyone. It is no longer just a place where information flourishes. It is a market, a business. A place without boundaries where companies can showcase products, find customers but also a place where we can freely publish our opinion, bringing new voices and highlighting elements that, in mainstream media, are forbidden.

Cyberspace has no limits. What it does have limits, is access to it. That's why countries with a strong power of coercion over their communities are unwilling to allow access to spaces where margins for maneuver are so high.

***Cyber-Defense and Environmental Theories***

I refer to environmental theories when I allude to those studies in which geography, demography, resources distribution and technological development are protagonist agents and actors for the study of international relationships.

Cyberspace, its use and manipulation had set new guidelines to understand the edges of geopolitics. Had done wedge over land and sea superiority precepts, and compromised conceptualization over space domination (and time) as we knew it.

Cyberspace is a new frontier, one without physical limitations. Without mountains, valleys, rivers, oceans, without weathers, no winters, no summers. There are not intangibles agents as known that can determinate, affect or influence political and/or military decisions. There are no factors that forge national character. Thus, leaves behind former conceptions about geopolitics, since Aristotle (1) to XX century authors as Harold and Margaret Sprout (2).

It does have coincidences regarding the term frontier with the work of Frederick Jackson Turner (3): frontier push to west was a force that configured north American intellect and provided energy and inventive. In terms of cyberspace, individuals need constantly not just push frontier but chase it because, first, they have to update their knowledge to establish a new intellectual distance. That virtual frontier is always moving. In terms of cyberspace also exists to frontiers: one established to contain, the other established to conquer. The first is developed in the pursuit of defense of resources. The second is developed to combat those defenses.

In tune with these features, other authors that theorized about the concept of frontier are Friederich Ratzel (4) and Spykman (5). The first made famous the concept of lebensraum (vital space); the second theorized about dynamics frontiers.

Lebensraum indicated that State strained to extend it territorial frontiers; thus, frontiers are in constant movement. Dynamic frontiers claims that these zones are consider demarcations of zones in which expansions had temporary ceased.

Other peculiarity of cyber-defense with environmental theories is the one that link Darwinist approaches (survival of the strongest) mainly in the theorization of Thomas Robert Malthus (6) who understood that population

growth was diametrically opposed to food existence. Within cyber-defense should be considered three factors: a)

On cyberspace there are no resources on extinction process; on the contrary, resources are generated second after second. b) There is no ethic or morality capable of contain the action and manipulation curses of those resources. c) There is no justice regarding these resources neither agents nor actors involved.

Malthus thoughts drove to think the State as an instance of imperialist expansion. As if it is a natural evolution of the utilitarianist drive over existent objects (in this case, not just food, but any material resource). There is something about that in cyber-defense. How not to think on the imperial figure when the ground where it develops has the extension that the very same actors want/wish/desire? There is an inner Darwinism on the cyberspace operative. What exists (knowledge, information) have to be occupied, comprehended, and apprehended. Conciliations and alliances are to occupy, compete, conflict. This is the case of groups such as Anonymous or Lulzsec. They are collective agents which actions (conflict with those they identify as enemies) legitimized by the cooperation of different individuals. But none of these individuals are legitimate by themselves. There is no Lulzsec or Anonymous as the sum of individuals but as a hole.

Another feature comes from Quincy Wright (7) studies when referred to demographic transformations. He considered that population growth produced a cultural interpenetration and with communication increase generated a technological distance that narrowed but also increase the friction between peoples. In cyber-defense it occurs a similar phenomenology: interpenetration happened in a natural way as information begins to lose a define tutelage (knowledge becomes public, more and more public); actors with access to that information increases and technological distance tend to 0 continuously. That boosts the frontier phenomena that I mentioned creating conflict.

In geopolitics, debate revolved around the function of environment, its capacities. If it's moldable or not; if it determinates or not. Cyberspace answers those questions. It is moldable because environment is the construction of information using information. That is why hide the paradox of its condition: mean and end are mixed. There is no agent's determination over structures and

there is no structures that determined agents. Information allows to create new structures when is needed and that new structure will have new actors and structure can do anything about it.

Several authors had theorized about restrictions that environment imposes in matter of political decisions, of strategies. Alfred Thayer Mahan (8), Sir Halford Mackinder (9) and Giulio Douhet (10) are three big references. Mahan theorized about naval power, Mackinder about ground power and Douhet about air power. All of them in defense code. *What* can be attacked depended on the *how*. In terms of cyber-defense the target is diffuse. Although targets in defense matters are always tangibles (infrastructure, units, bases, etc.) in terms of cyber-defense there is an obligated link to technological development. Not all the states have a digitalized infrastructure. And not all states have *their entire* infrastructure digitalized. It is diffuse because harm that can be done depends of such digitalization. So little harm can be done by a cyber-attack to an analog protocol. Is difficult to harm where there is no link to a computer. And many times, a direct action of a man in situ is needed to perform a connection to the target.

Restrictions of the environment are given by the same cyber-defense with firewalls, and complex software to detect and contain infections or by the man himself: watch. That is why it is a very complex situation the one that international system is involved. Humankind progress can attempts to its own safety.

Cyberspace behave as a subsystem. With distinguishable boundaries of its operative environment. It's a data network that allows a self-adjusting process thru information flow. As all systems, it has inputs and outputs; outputs can return as inputs in a feedback behavior.

Now, I want to refer to Andrew M. Scott´s (11) definition of interaction in the international system and how this has an almost exactly counterpart in cyberspace. *"Thousands of agents introduce actions at the same time on the stage, those actions deviate, add and combined each other in several ways… is an unguided summation process. Individual agent's behavior is deliberated, but the process as a hole doesn't know any goal and is not under any general direction. A process which is in part under control, doesn´t stop just because the control element is no longer suitable; but it continues working and produces*

*results, some of what are deliberated"*. This indicates that problems, inputs, are multiplying faster than solutions actually can be found, overloading the system. Which is almost an exact definition of cyberspace. And the true reflection is the imperious need to add structural requirements in such subsystem.

As I referred previously, challenges are multiplying and move the "frontier".

***Realism Theory and Power in Cyber-defense***

Realism considers that human nature, not being innately good or perfectible, hardly can suffer alterations making the international system unable to escape this determinism.

Because of this foundational lecture of realism, the study of Power is vital. Only with the proper power distribution, there is a chance to diminishing the existing asymmetries in the international system.

Thereby, Balance of Power displaces idealist criteria as international law and the exercise of international organizations. On these two rest the perfectible lecture of the human being.

On realistic terms, Power is measure both on quantitative and qualitative levels. Is a multidimensional concept that doesn't close itself in military variables but includes as well technological, demographic, environmental, and geographical issues also coating the importance on governmental forms, leadership capacities, strategy and ideology.

*Realistics* also have a clear point of view towards moral principles and its applications. They believe that these cannot by apply to specific political actions because the State, main actor of the system, is inserted on an anarchic structure where must only reply on behalf of it national supreme interest: survival (12) (13). In these terms, Cyberdefense, as mode of attacking, finds perfect shelter in realism theory; considering that the scope where the State must execute its policies, is even more anarchic that the known international system; freeing this way of any ethical questioning.

Many authors had theorized about Power. An author that I find interesting to link with Cyberdefense is Charles P. Kindleberger (14), who defines Power as a “force capable of being used effectible”. His definition speaks of a dynamic nature of Power and includes a vision both of means and goals. A force that even without use exists; and on the effectiveness of its use reside its entity.

Kindleberger distinguishes 3 elements: prestige, influence and domain. *Prestige* is the respect that one feels to that power. *Influence* is the capacity to affect other’s decisions. *Domain* is the condition in which an actor A affects a significant number of decisions of an actor B, without “B” affects “A” decisions.

Taking just the thought structure of Kindleberger (he is an economist, taking it literally would be a mistake) help us to interpreted that equation examining a logic of Power in Cyberdefense. Force can be replaced by Information. Its effective use means comprehension, this is, the achievement of Knowledge.

The power of a nation in terms of Cyberdefense would be given by the knowledge gain. But this forces us to think that exists a new lecture of the logic of power, because without an effective use of knowledge cannot be consider as power (always on Kindleberger terms). This means that Power on Cyberdefense needs a double initial mechanism with two sequential forces: first Information, then Knowledge.

Now, the three elements of Power that follows also respond to logic of more than one instance: if prestige is respect felt by that power, we should ask: is it respect acquired by its use (necessarily effective)? Is it respect acquired by knowing the simple disposition of power of an actor (once effective)? Is it respect understood as a possible menace becoming a fear?

Prestige in Cyberdefense could be theorized in these 3 facets. A respect acquired by its effective use (Russia over Estonia); respect acquired by the knowledge of disposition (United States); a respect understood as fear: any

country with Cyberdefense structure that is understood as a regional or hegemonic competitor (United States, Russia, China).

The Influence is the capacity to affect others decisions. This, existing the domain, is understood as the capacity of making think other actor twice in a determinate situation before knowledge, fear or suspicious of an unknown or feared outcome. Influence in Cyberdefense is the most clear of the facets because all the actors involved in this new arms race have been forced to adjust their sketches being affected by the curse of actions of other actors (prestige).

However, Domain is the most unclear of the 3 elements to be identified. Though there is plenty evidence of Cyberdefense actions (cyber attacks), there is no domain feature expressed in the international system.

Let's take *stuxnet* virus for example, which was designed to affect Iranian nuclear installations (so far the most emblematic case). Did it discourage Iranian process in this field? No, it is just re designed Iranian times in its process to enrich uranium. But of course, we are just on the gestation of this new war methodology and would be risky to maintain that the domain will never concrete. In fact, it only makes us think if the lack of effectiveness on this matter will catalogue the whole scenario of lack of power or, at least, influence.

As well, there are authors that speak of a very important concept like interdependence. Such is the case of Klaus Knorr (15). Knorr theorizes about power and influence as coercion or absence of it. This compel us to think again of collective groups such as Anonymous and Lulzsec (that exert prestige and influence but not domain), and the paradoxical interdependence existed with other actors. They are interdependent, because those servers that allow holding information (therefore, its flow and manipulation) are patrimony of many actors that they want to attack. Without the existence of those servers Anonymous and Lulzsec cannot work.

Linked with the concept of influence I can't avoid mentioning the concept *perception* of power as it is defined by Michael P. Sullivan (16): the capacity of a state to project power (in any of its dimension) without the empiric need of use

it. That is, to practice a psychological control over other state's behavior because it is perceived as powerful. As Dougherty and Pfaltzgraff Jr. (17) well said, Power becomes the edge of diplomacy. But in terms of Cyberdefense there is not this dimension of power because it needs the action to legitimize itself. No State makes or stop making knowing of the existence of technological capacity and knowledge (always on Cyberdefense terms) of other state.

Bibliography

(1) Aristotle: "The Politics of Aristotle", trad: Ernest Barker (Oxford, Clarendon, 1961) pp. 289-311

(2) Harold y Margaret Sprout: "The Ecological Perspective of Human Affairs with Reference to International Politics" (Princeton, Princeton University Press, 1965), p.27

(3) Frederick Jackson Turner: "The Significance of The Frontier in American History" en Donald Sheehan, comp.: the Making of American History, Book II (Nueva York, Dryden, 1950), p. 200.

(4) Friederich Ratzel: "Anthropogeography" 2° ed. (Stuttgart, J. Engelhorn, 1899), part I, p.2; see Kirstof, op. cit., p 22.

(5) Nicholas J. Spykman y Abbie A. Rollins: "Geographic Objectives in Goreign Policy I", American Political Science Review, XXXIII (june de 1939), pp. 391-393.

(6) Thomas Robert Malthus: "An Essay on the principle of population"

(7) Quincy Wright: "A Study of War" (Chicago and London, The University of Chicago Press 1965) page 1144.

(8) Alfred Thayer Mahan: "The Influence of Seapower Upon History 1600-1783" (Boston, Little, brown, 1897), esp. pp. 281-329

(9) Sir Halford Mackinder: "The Geographical Pivot o f History", Geographical Journal, XXIII (april of 1904), p. 434

(10) Giulio Douhet: "The Command of the air", trad.: Dino Ferrari (Nueva York, Coward-McCann, 1942), pp. 10-11

(11) Andrew M. Scott: "The Logic of International Interaction", International Studies Quarterly, 21, N° 3 (septiembre de 1977)

(12) George F. Kennan: "Morality and Foreign Policy", Foreign Affairs (Invierno de 1985-1986), p. 206

(13) Robert E. Osgood: “Ideals and Self-Interest in America’s Foreign Relations” (Chicago University Press, 1953), p. 22

(14) Charles P. Kindleberger: “Power and Money: The Politics of International Economics and the Economics of International Politics” (Nueva York, Basic Books, 1970), pp 56, 65.

(15) Klaus Knorr: “The Power of Nations: The Political Economy of International Relations” (Nueva York, Basic Books, 1975), p.3

(16) Michael P. Sullivan: “International Relations: Theories and Evidence” (Englewood Cliffs, N.J. Prentice-Hall, 1967), p. 193

(17) James E. Dougherty y Robert L. Pfaltzgraff Jr. “Contending theories of International Relations” (New York, HarperCollins College Publishers, 1990), p 97.