UNKNOWN DIMENSION

Cyber space is a new setting with its own characteristics, which are challenging and dynamic, and require an adaptation of existing protocols in order to operate successfully. The young Cyber Defense Joint Command will be a reference in order to carry out the necessary tasks.

KEY WORDS: CYBER SECURITY / NATIONAL EXECUTIVE POWER / MINISTRY OF DEFENSE / MEASURES / TECHNOLOGY / STRATEGIES

By Julio Gerardo Lucero

CYBER SPACE AS A NEW OPERATIONAL SETTING

"A cyber attack will be considered a declaration of war", expressed the North Atlantic Treaty Organization (NATO). Israel was threatened by "Anonymous"[1] with a cyber attack to its security; a virus affected US networks and caused losses for 3.5 billion of dollars; the Iran electrical station of nuclear fuel was attacked by a virus that destroyed the control system of the centrifugal reactor and left it out of service; United States of America created a Cyber Command (USCYBERCOM[2]).

All of these are news that appeared in the media, creating in many distracted observers some skepticism, sarcastic smiles and even tabloid press ideas to fill space in the newspaper and have an impact on public opinion.

If we observe the current situation of the context related to events expressed, in the Argentine Republic, we can highlight the intensive use of digital technology in everyday situations and at everyone's disposal, for example, purchasing a container of products from Shanghai by means of an e-transfer of thousands of Euros from a bank in Switzerland to another one in Hong Kong using a mobile phone from an office located in the ski center in Las Leñas (province of Mendoza, Argentina) is not impossible.

The National Program of Information and Cyber security Critical Infrastructure (ICIC, in its Spanish acronym) in Argentina is a project which has the purpose of promoting the creation and adoption of a specific regulatory.

Moreover, it is worth mentioning that international trade transactions, exports and imports from our country which in 2013 amounted to 157.028.000,00 dollars[3], were mostly made by using e- banking, internet and virtual networks.

Also, the security of the thousands of persons that commute in public transport in our country (air, sea and land) is controlled, in a significant percentage, by digital technology.

To have a reference, in 2012, in the Argentine Republic only by air, 9.557.129 passengers were transported. We can also add that every year around 14 billion electronic transactions are made in the national banking system, mainly, through private or virtual networks or the Internet[4].

The creation, in 2011, of the National Program of Information and Cyber security Critical Infrastructure (ICIC, in its Spanish acronym) in Argentina is a project which has the purpose of promoting the creation and adoption of a specific regulatory framework that aims at protecting strategic and critical infrastructure of the National Public Sector, inter-jurisdiction entities and civil organization or the private sector that may require it.

As regards the national defense section, we can highlight the Third Edition of the National Exercise of Response to Cyber Events in the destroyer ARA Almirante Brown, when the vice- admiral Marcelo Eduardo Hipólito Srur, commandant of Training and Enlistment of the Navy, declared that collaboration with the ICI is one of the strategic pillars of the Ministry of Defense[5].

Argentina and the Brazil extend strategies of cyber defense; represented by their respective ministers of Defense, engineer Agustín Rossi and Ambassador Celso Amorim. Both states, main actors of Mercosur, signed a joint declaration as to that.

In light of this situation, there may be questions, such as: what is the possible evolution of the great trends in this new geopolitical space? Do armed forces have a role in this virtual setting?

Finding answers to these questions encourage the effort to overcome the natural trend of working over the immediate situation and to think in the uncomfortable long term so as to go beyond the current situation and be ready for the uncertain tomorrow.

CYBER SPACE

In order to have a definition of cyber space, it is convenient to start discussing the Internet. We could define it as a "net of networks" and it is also known by users as the web or the cloud. It was created as an additional response to communications in US defense plans in case of a nuclear attack and consisted in a net and sub networks that allowed for decentralized interconnection of computers through a set of protocols called Transmission Control Protocol/ Internet Protocol.

At first, it was for military use and then, with scientists and intellectual people, it became a space for exchange of opinions and knowledge among the thousands of users that were incorporated on a daily basis.

These dynamics turned it and in the mid 80's, it called itself a "space of freedom, Independence and democracy" out of reach for the powerful. This primary community thought there was some shelter from the millenary game of social, economic and political forces that were in the center of the world.

Several NGO's[6] of different nationalities and ideologies promote this freedom.

However, such ideal situation has never been so pure if we think of the origin of the web, especially in these moments when governments and international organizations, which see the perspective and magnitude of irregular events such as the ones described before, consider the need to build some order for virtual activities.

Its infrastructure had a rapid evolution; the inclusion of networks and computers on the cloud was huge. Resulting statistics are surprising: 2.9 billion people (40% of the world

[1] Anonymous: This is an informal organization with a decentralized structure without a leader that allows for any computer attack in the name of an Internet freedom cause. Its tools and methods are a common feature in each of the actions of the movement: service denial attacks that leave websites out of line and, in some cases, the inclusion and setting online of personal information.

[2] USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to direct operations and defend information networks as specified by the Department of Defense and prepare to carry out a series of military operations in cyberspace in order carry out actions in all domains; assure freedom of actions to the United States and allies in cyberspace and prevent opponents from this.

[3] INDEC (National Institute of Statistics and Census, Argentina), Argentine Business Exchange, temporary date for the year 2012 and figures estimated for the year 2013, Buenos Aires, 2013.

[4] De Nigris, A. La bancarización en la Argentina [Banking in Argentina], Development Study Unit- Division of Economic Development, Santiago de Chile, 2008.

[5] Ministry of Defense, MD 343, May 14, 2014, Buenos Aires, Argentina.

[6] NGO is the acronym for Non- government organization. These are social initiative entities that have humanitarian purposes which are independent from public administration and are non- profit.

What is the possible evolution of the great trends in this new geopolitical space? Do armed forces have a role in this virtual setting?

population) and 6.8 billion devices (some PCs, smart phones, servers, among others) are linked to the web[7], 204 million mails are sent every minute, in Argentina there are 22 million users that spend an average of 5 hours a day online[8].

All elements implied in the figures described are within a greater context that contains them, Cyberspace.

PhD Roberto Uzal, in a simple manner, defines it as "Internet plus all networks which in some way or another, are linked to it"[9].

The existence of this environment created by men has an influence, changes and new perspectives in different areas of thought.

In a more specific orientation to the area of defense, we state the idea expressed by Colonel Flores:

> Cyber space is an operational domain whose distinctive and only feature is framed by the use of electronics and the electromagnetic context to create, store, modify, exchange and exploit information through systems based on Information and Communication Technologies (TIC's) and their related infrastructure[10].

As regards morphology, the different modes of intercommunication among devices, protocols follow the standard set by the OSI- ISO Model. This helps to create the Web as it allows intercommunication among networks and devices. The standard model describes 7 layers in communication: application, presentation, session, transport, net, data and physics.

In line with this, when recognizing the existence of cyberspace, there is a question of order, care or administration of the virtual world. In fact, the government of the United States has some privileges as to the governance of cyber community as the National Administration of Telecommunications and Information has the assignment/coordination at world level of IP addresses[11] to be developed in

[7] International Telecommunications Union. Available at http://www.itu.int/net/pressoffice/press_releases/2013/41-es-aspx#U7WkClcU8cA

[8] Diario Clarín. Available at http://www.ieco.clarin.com/tecnologia/estadisticas-Internet-millones-enviados-minuto_=_1167483520.html, June 25, 2014.

[9] Uzal, Roberto, May 21, 2014. Buenos Aires, Argentina..

[10] Flores, H. Non- terrestrial environments in future war: Cyberspace, Military Strategy Cabinet, Madrid, 2011.

[11] This number is the Access to Cyber space, it gives identity to the device that operates in it without which access and operation are not possible.

the virtual environment, a function carried out through the organization Internet Assigned Numbers Authority (IANA).

Surprisingly, the United States recently declared their intention to terminate, on their own, these privileges without saying who will they leave it to[12]. This possible change was the cause of different meetings, the most recent one was organized by the government of Brazil, Net-mundial[13], which was attended by representatives of the Argentine Ministry of Foreign Affairs and during which they defined two trends for the future governance of the internet: cooperation and consensus.

Moreover, they discussed about conflicts and their possible solution. As regards the legal framework to respond to actions against states, in this new setting, the position of broader consent is section 51 of the UN Charter, "Legitimate Defense".

As regards conflict resolution, it had acceptance of the participation scheme which was used in the case of the attack to Iran's oil platforms with the Flame virus (in May 2012): The nation attacked report the event to the UNO/ International Telecommunications Union and it sent inspectors to analyze this and issue a statement.

At this point, it is possible to seriously consider a new context of possible friction, strongly asymmetrical and anthropotechnic that may be reached by actions of state and non state actors[14].

From the perspective of Critical Geopolitics[15], and in a general manner, we can have the freedom to consider Cyber space as a geopolitical space subject to the game of power, interests and influence of individuals, organizations and states[16].

From the perspective of Critical Geopolitics, and in a general manner, we can have the freedom to consider Cyber space as a geopolitical space subject to the game of power, interests and influence of individuals, organizations and states.

STRATEGY

The new context under analysis hides complexity in which according to the perspective from which it is observed, there are national interests that may be promoted or limited by the positions adopted.

Today, in the virtual area of the Argentine Republic, we could say that there is a *status quo* as regards great irregular actions.

This situation, however, must not cause inaction as the international events lead to think the balance will be affected in the medium and long term. Evolution expected by great international actors foresees a catastrophic event called "Great Meteor" (a cyber September 11). This "attack" will mark a time before and after for cyber space power relations.

Such expectations and possible evolution lead to the preparation and implementation of a defense strategy for the national heritage in the new context that allows for the alignment of resources towards the purposes determined in the area, supporting as a decreasing strategic reasoning, the protection of national interests.

The National Executive Power is taking defense measures in the virtual environment. The germ is located in the Information Technology National Office through the ICIC.

The current situation turns economic factors into limits for the modification/ adaptation processes of infrastructure and, if we add the voluntary condition of recommendations by the Private Circumscription Program, these give rise to a series of situations that affect the integrity of a protective general strategy in case of possible threats.

The Ministry of Defense has the guideline of development of specific information systems security of the armed forces and, therefore, on July 14, 2014, the Cyber defense Joint Command was created.

In sum, we can describe the evolution of a hypothetical event in the current framework: in case of an irregular cyber action that aims at affecting or destroying elements of a vital system (electric power stations, oil and chemical companies, nuclear stations, air transit control), these entities will individually have the great responsibility to detect, identify and neutralize, in a primary situation, the threats posed to their systems and networks.

[12] Avni, B., Newsweek. Available at: htt://www.newsweek.com/2014/04/04/obama-wants-global-community-run-internet-it-could-end-hands-china-or-putin-248037.html

[13] Held in So Paulo, Brazil between April 23 and 24, 2014. It was attended by minister representatives of 12 countries (Argentina, Brazil, France, Ghana, Germany, India, Indonesia, South Africa, South Korea, Tunisia, Turkey and the United States) and 12 members of the international community of different interested parties. This committee has representatives of the International Telecommunications Union, the Department of Economic and Social Affairs of the United Nations and the European Commission.

[14] Ballesteros Martín, M.A., "The evolution of conflicts2, Panorama geopolítico de los conflictos 2013- Instituto Español de Estudios Estratégicos, 12, Madrid, January 2014.

[15] Rodriguez Garoz, R., "Scripta Nova", Revista Electrónica de Geografía y Ciencias Sociales. Available at http://www.ub.edu/geocrit/sn/sn-198.htm. An adaptation of the idea of space from a perspective of Critical Geopolitics. Critical Geopolitics studies planetarium space and its modes of production and reproduction, for which it will be necessary to see the interconnection of economic, political, symbolic, institutional or legal elements in the concrete historical human practice accepting the space aspect of social events. It faces a historical analysis of speech and practice of States.

[16] Koutoudjian, A., interview by J. Lucero, May 14, 2014.

RETHINKING STRATEGY: ROLE AND CAPACITIES OF THE ARMED FORCES

As a geopolitical environment, cyber space may give rise to theories and concepts of geopolitical science. Based on this, we can apply by analogy the arguments of Juan Recce as to "Scientific Occupation of Space"[17] and relate the Argentine space- strategic projection in the idea of national interest to technological development.

In order to do so, the advance on this new setting could be a dual- entity (for example, CONICET[18] and Ministry of Defense) which starts a technological innovation process that articulates the capacities of the Science and Technology Complex in the country with the logistical structure of the armed forces.

If this change is chosen, it is convenient for the executor to be capable of keeping and sustaining a strategic alert condition in light of the evolution of threats that require greater control with a defense model and a clear rejection of policies, attitudes and capacities of attack with the impact of power to third states.

Today, in case of a potential escalation of conflict, the different "layers" of state protection would respond according to its origin analyzing whether it lies in defense or security jurisdiction in the naturally complex framework of the issue with key reaction time which is not totally defined yet due to the new characteristics that cyberspace has.

The Defense White Book defines the domain of cyber space as a strategic interest, not only for the exercise of command and control and the operation in networks of defense systems, but also to prevent external state military threats that may take place using it as a way of execution or having it as a purpose[19]. There is no doubt that this would allow Defense to be capable of contributing to a better achievement.

The likely evolution towards participation of armed forces in a strategic alert national service of cyber threats would necessarily link the need to particularly consider the possible task with the Planning Cycle of National Defense through the Political Guidelines for National Defense. This document includes an analysis of the defense and security setting that identifies trends, risks and threats to national interests for the medium and long term[20].

The current analysis of Political Guidelines for National Defense available to the public and of researchers does not

[17] Recce, Juan, Fundación Argentina Ase. Available at http://argentinaase.org/atlantium

[18] National Council of Scientific and Technical Research (CONICET, in its Spanish acronym) is the main entity devoted to the promotion of science and technology in Argentina. Its activity is carried out in four great areas: Agro Science, Engineering and Materials Sciences; Biological and Health Science; Exact and Natural Science; Social and Human Science.

[19] Ministry of Defense, Argentina, Defense White Book, 2010, p. 48.

[20] National Executive Power, Argentina, Executive Order 1729/07. Political Guidelines for National Defense, City of Buenos Aires, November 11, 2007.

In case of a potential escalation of conflict, the different "layers" of state protection would respond according to its origin analyzing whether it lies in defense or security jurisdiction.

expressly include the setting under analysis, a situation that is considered to have been under changes upon the creation of the Cyber defense Joint Command.

Beyond formal considerations, the complexity of the situation presented requires special attention in the construction of knowledge that is certain as regards cyber space, which requires human resources specifically trained, informed as well as time.

The potential role of the armed forces may be analyzed in three levels that may be related to the short, medium and long term.

In the short term, the armed forces may carry out an activity of presence in cyberspace according to the scope defined by the Ministry of Defense.

That is, collaborating or participating in a Strategic Alert Service, focusing on the identification of possible attacks and their origin (attribution problem[21]) with the technology of "Analysis of Networks Flow"; a procedure that respects the legal mandate of protecting privacy of web users[22].

Moreover, making presence effective would imply delivering to cyber community a message of commitment to the protection of Argentine interests in this aspect.

In the medium term, the purpose would be to go towards a formal cooperation agreement in the regional context to formalize joint activities to respond to cyber events that are already being carried out with friendly nations, such as Brazil. The creation of a common regional front increases dissuasion of each member from irregular actions[23].

In the long term, considering growth in number and importance of critical systems, it is recommendable to have a protocol for the armed forces in case of potential threats of other states that try to affect the normal development of virtual activity of national and regional relevance, comparing it to the response expected in classical operational dimensions.

Including a new capacity implies to obtain means, develop doctrine and procedures for use, apart from the important training.

CONCLUSIONS

When analyzing virtual environments, we cannot be deceived by symbolic elements and forget that most of this relates to appearance[24]. Cyber space is a new setting that has its own and distinctive characteristics that require adaptation of existing protocols to successfully operate in it.

Security in this dimension depends not only on the existence of defensive means, but also on the capacity to know what happens within it, so as not to be surprised by irregular incidents. The setting of a cyber conflict is featured by its challenging and dynamic originality which takes a continuous and patient process of learning to achieve efficiency. The young Cyber Joint Command is a reference in these areas.

It is possible to go through the path of Scientific Appropriation of Cyber space in a dual work under the control of the Argentine State supported by a change of paradigm which, by means of Scientific Occupation of Space, has a position relatively favorable to the region, both for discussion of cyber space governance and the entrance to a world of possible opportunities for future generations that have the only limit of imagination.

The promotion of Science and Technology started by the National Plan of Science, "Argentina Innovadora 2020" gives a strategic, political and social framework proper to go further in the relation of Science, Technology, Defense and Economic Development[25].

There are opinions against any type of state participation as a control entity in virtual world, assigning responsibility of individual defense/ security to the individual or legal person that operates in that context.

Said position, in practice, leads to defense of a cyber attack that may render an oil distillery (critical system) useless as it happened in the case Bushehr- Iran to be required to the company itself. We could suppose that defense of an air attack against the same distillery and with the same purpose, making it useless, would also be the responsibility of the company.

A defense structure in cyber space does not imply an obliged attack to individual freedoms, as in terms of technology, it is possible to exercise an effective protection and pursuant to legal regulations if works are limited to the

[21] Garau Pérez- Crespo, C. "Sun Tzu's twitter", Revista General de Marina, 631, 2014. The problem of attribution: it is the difficulty to identify in a positive manner the author of attacks, it represents 85% of possible threats and its most important aspect is the inconvenience that represents for legal and jurisdictional treatment of cyber attacks, as well as the possible consideration of attack action under the prism of law of war.

[22] Uzal, Roberto, May 21, 2014. Buenos Aires, Argentina.

[23] Uzal, Roberto, May 21, 2014. Buenos Aires, Argentina.

[24] Anta, J. L. and Palacios, J., Revista Investigaciones Sociales, year IX, No. 15. UNMSN/IHS, Ed., Jul- Dec 2005. Available at: http://scholar.google.com/scholar_url?hl=es&q=http://revistainvestigacion.unmsm.edu.pe/index.php/sociales/article/download/7007/6201&sa=X&scisig=AAGBfm1wgQICZL50sUcyyt4noTl0u6bdFw&oi=scholaralrt

[25] Ministry of Science, Technology and Productive Innovation, National Plan of Science, Technology and Innovation: Argentina Innovadora 2020. Available at: htt://www.argentinainnovadora2020.mincyt.gob.ar/?page_id=312

Julio Gerardo Lucero
Commodore of the Argentine Air Force. Staff Officer. Systems Engineer. Bachelor in Aerospace Systems and Master in Information Systems Administration. He graduated from the Joint Forces Staff College in 2014 from the Master's Degree in Leadership and Joint Military Strategy. He is currently serving as Head of the Professional Technical Training Group of the Petty Officers School of the Air Force.

"Cloud" which does not involve private information, that is, if different layers are dealt with: Physics, Data and Model Net OSI- ISO[26].

From the perspective of concept and operation, we could consider cyber space as a frame system in which, by means of different technologies, states should control and supervise actions carried out so as to know if they are pursuant to law, social and/ or trade agreements and, also, to check that they do not threat national interests.

If we take the premise that cyber space environment is of national interest, this has to be taken as an integral unit. Therefore, it is recommendable to promote the creation of an executive cyber space authority at national level which protects Argentine interests and gathers state and private efforts against actions of interested parties.

In this sense, coordination entities created which are operating, as well as actions carried out by ministries and secretaries contribute to achieve that purpose.

Armed forces, because of the power they manage, are commanded by the Chief of state. They are the last tool to assume defense of a nation against an external military enemy. They are instruments the state has at its disposal to exercise defense of vital interests. As part of the Argentine state and subordinated to the legitimate authorities, they take the role defined by it in the topics dealt with.

However, the task already assigned of giving security to its own information systems may be complemented with a Strategic Alert state, within the framework of a Strategic Attitude merely defensive for the purposes of collaborating to take a minimum reaction time against attacks to critical systems.

Only a creative and integral strategy will allow to neutralize the harmful effects of irregular actions in cyber space. Inaction or mere reaction to strategic incentive caused by other actors are not enough, they engage our initiative and compromise the possibility of future generations to have the necessary freedom of action for their development and happiness.

[26] Uzal, Roberto, May 21, 2014, Buenos Aires, Argentina.