TRIARIUS

August 1, 2020

HONDURAS

Prevention and Security Bulletin on
Terrorism and the New Threats

EDITORIAL

In the midst of the crisis generated by the COVID-19 pandemic, we have seen how health sector personnel have taken on the challenge of defending society from such a threat, even at the risk of their own safety. From TRIARIUS we say THANK YOU!

We open this edition with an interesting article by Colombian analyst Juan David Urrego, where he addresses the issue of vandalism in Colombia. We will know through this reading the fundamental legal framework to understand the phenomenon and the responsibilities of the different actors in a context of rights and duties.

We then go on to review the issue of stateless persons, the terrible situation they are going through, and the latent danger that these people may transition to crime and violence, dragged by their need for solutions to their hardships. We thank the Argentine analysts Crudi and Carracedo for this valuable contribution.

After reading the article by Argentine analyst Micaela Abril Álvarez, you will surely feel very worried and vulnerable, and you will want to supervise the video games that your children use.

Step by step, the Argentine analysts Taverna and Cárdenas, enlighten us on the issue of critical infrastructure protection, and although they focus on the Argentine Republic, the theoretical component of their article, as well as the essence of their proposal, can be extrapolated to any of our countries. We can learn a lot from their work.

In another important contribution, Julian Urrego, a Colombian lawyer, explains in detail the legislation that governs the issue of possession and carrying of traumatic weapons in Colombia.

We then travel to the Caucasus with Guadi Calvo, our senior analyst, to learn about the latest developments in the conflict between Armenia and Azerbaijan, and its implications for regional and global geopolitics. Closing this edition with a note about the Scan Eagle and Night Eagle UAVs, which operate in the Colombian Military Forces.

Thank you for reading us.

Know to win!

Douglas Hernandez

Editor

This newsletter has a Spanish version.

TRIARIUS 076

Content:

TRIARIUS

The situation with the current pandemic has multiple edges, which require multiple analyses. Various approaches to the phenomenon are necessary to try to understand what happened, and it is also necessary to look into future scenarios related to new pandemics -spontaneous or provoked-. Due to scientific, technical, technological and legal restrictions, developing a nuclear weapon is an almost insurmountable challenge for most countries in the world, but not developing a deadly virus and using it as a weapon of mass destruction. Today, we have all appreciated the destabilizing power of one of these microorganisms, and its global reach. It is perfectly possible that some rogue governments, and terrorist groups of whatever aetiology, are considering the possibility of getting hold of deadly viruses and using them as a weapon. It is a viable plan for a terrorist group to release a virus of the caliber of the current one, in the main cities of the enemy, while their followers and their families isolate themselves in a remote region, preventing access to travelers who could be infected. They would cause chaos and mass destruction, while they preserve themselves...

On the cover, **Honduran Special Forces Soldier**.
See more information at the end of the magazine.

TRIARIUS privileges freedom of expression, however, the responsibility for what is said in the articles is exclusive to their authors.

Vandalism and Public Order in Colombia

By Julián David Urrego Atehortua (Colombia)

Group of violent protesters in the city of Bogotá.

In this writing I have proposed to analyze, legally but also, in a not so technical and simple way, understandable for all, this issue of protests in public settings as well as the rights we have against them, counteracting them with vandalism and, duties and obligations of mayors as police authorities.

It is important to point out that we Colombians have rules that regulate us and allow us, in the first place, to have a north as a society, that is, they answer the question: Where are we going as a nation? And secondly, some rules of coexistence that allow us to interact with each other in a civilized manner within the framework of respect for the rights of the other.

Within this context we can say that the north of our society is a fair political, economic and social order, which we can find in the constitutional preamble, which preaches:

"*The people of Colombia,*
in exercise of its sovereign power, represented by its delegates to the National Constituent Assembly, invoking the protection of God, and in order to strengthen the unity of the Nation and ensure its members life, coexistence, work, justice , equality, knowledge, freedom and peace, within a legal, democratic and participatory framework that guarantees a **fair political, economic and social order** *, and committed to promoting the integration of the Latin American community, decrees, sanctions and promulgates the following* political constitution *."*
-underlining and bold outside original text-

In Colombia then, the laws are hierarchical, finding at the top, as a norm of norms, our Political Constitution, below it, the laws that the Congress of the Republic makes and for the purposes of dealing with public order we have, below the laws, the municipal decrees issued by the mayors.

In this way, we enter the present exhibition, as follows:

Of the rights of those who express themselves in public space.

In the first place, referring to our maximum norm, the political constitution, we find:

"**Article 37:** *Any part of the people can meet and demonstrate publicly and peacefully. Only the law may expressly establish the cases in which the exercise of this right may be limited.*

And **article 38**, which tells us:

"The right of free association is guaranteed for the development of the different activities that people carry out in society."

Being clear about our right to assemble and **to express publicly and peacefully** our ideas, let us then see how Law 1801 of 2016 regulates this exercise, as indicated in article 37 of the aforementioned political constitution:

Article 53 "*Any person can meet and demonstrate in a public place in order to expose ideas and collective interests of a cultural, political, economic, religious, social nature or for any other legitimate purpose.*

For such purposes, notice must be given in writing before the first administrative authority of the place or by email. Such communication or mail must be signed by at least three people.

Such notice shall state the date, time and place of the projected meeting and shall be submitted 48 hours in advance, indicating the proposed route.

Any meeting and demonstration that causes alterations to coexistence may be dissolved. (…)"

- **Underlining outside original text-**

In this order of ideas, we are clear that as citizens we can express our political ideas in the public space, but within the framework of current regulations, that is to say in a peaceful manner and notifying the administrative police authority - mayor - what the route will be planned in the march or if it will be a static activity but developed in the public space.

Of the rights of those who do not participate in public demonstrations:

The above has a reason; And it is that, in a society, there are duties and rights, especially with regard to the issue that we have been addressing and, although citizens have a right to demonstrate publicly and peacefully, the administration or mayor also has an obligation to guarantee the free mobility of who also as citizens decide not to participate in marches, stoppages or strikes, let's see the rights of these:

"Article 24 CN: Every Colombian, with the limitations established by law, has the right to move freely within the national territory, to enter and leave it, and to remain and reside in Colombia."

"Article 25 CN: Work is a right and a social obligation and enjoys, in all its forms, the special protection of the State (...)"

In this way it is clear to us that although a part of the citizenry has the right to demonstrate publicly and peacefully against a political position that they hold, another part of the citizenry has every right to have their mobility in the city regulated and guaranteed. and especially when it comes to commuting to or from a workplace.

Of the obligations of Mayors in front of some and other citizens.

Taking into account this entire context of rights, it is important to observe the obligations of the municipal or district Police authorities -mayors-, which we find in Law 1801 of 2016, as follows:

"Article 54: The district or municipal mayors, except in exceptional circumstances or force majeure , must authorize the temporary use of roads within their jurisdiction for acts or events of exercise of the right of assembly or public and peaceful demonstration in public space. In the case of the main arterial roads or collective public transport corridors, an effective diversion plan must be established for the mobilization of citizens who do not participate in the act or event, as a measure to protect the rights of other citizens.

-you underline out of original context-

Remaining with the above, it is very clear that with this obligation of the police authorities the rights of both citizens who demonstrate in public space and those who mobilize in it are protected.

Now, we move on to an important part and that is vandalism and matters subject to criminal law, for which we will first see the meaning of the words, vandalism and vandalism which, according to the dictionary of the Spanish Royal Academy, they mean:

"Vandal: Said from a person: what commit Actions own from people wild Y destructive (…)"

"Vandalism: Spirit from destruction that no respect thing some, sacred neither profane (…)"

In this order of ideas, we will classify as a vandal that citizen who:

First: since there is a route and some permits by the district or municipal mayor's office for the use of public space in demonstrations, it decides to take over the roads that are not authorized by means of force or violence.

Second: existing different alternative means of communication and social networks decides to violate the public space of all, in order to communicate through graffiti, scratches and insulting writings own messages of their individual and particular understanding of the country's political situation.

Thus, we could leave this definition of vandal and vandalism there, only in the definition, but it is important that the reader within an academic exercise understands that, in our criminal legislation, there are the following crimes:

LAW 599 OF 2000 COLOMBIAN PENAL CODE.

ARTICLE 173. SEIZURE OF AIRCRAFT, VESSELS, OR MEANS OF COLLECTIVE TRANSPORTATION. Whoever , by means of violence, threats or deceitful maneuvers, seizes a ship, aircraft, or any other means of collective transportation, or alters its itinerary, or exercises its control, will incur, for that conduct alone, a prison term of one hundred and sixty (160) to two hundred and seventy (270) months and a fine of one thousand three hundred and thirty three point thirty three (1333.33) to four thousand five hundred (4,500) current monthly legal minimum wages.

ARTICLE 182. ILLEGAL CONSTRAINT. Whoever, outside of the cases specially provided for as a crime, constrains another to do, tolerate or omit something, will incur in prison from sixteen (16) to thirty-six (36) months.

ARTICLE 265. DAMAGE TO OTHERS' PROPERTY: Whoever destroys, renders useless, makes disappear or in any other way damages another's property, movable or immovable, will incur a prison sentence of sixteen (16) to ninety (90) months and a fine of six point sixty-six. (6.66) to thirty-seven point five (37.5) current monthly legal minimum wages, provided that the conduct does not constitute a crime sanctioned with a higher penalty.

The penalty will be from sixteen (16) to thirty-six (36) months in prison and a fine of up to fifteen (15) current monthly legal minimum wages, when the amount of the damage does not exceed ten (10) current monthly legal minimum wages.

If the damage caused to the offended or harmed party is compensated before a first or sole instance sentence is handed down, there will be a place for the issuance of an inhibitory resolution, preclusion of the investigation or cessation of the procedure.

ARTICLE 266. CIRCUMSTANCES OF PUNITIVE AGGRAVATION. The penalty will be increased by up to a third, if the conduct described in the previous article is committed: (...)

4. On objects of scientific, historical, assistance, educational, cultural, artistic interest, on goods for public use, of social utility, or on goods that make up the cultural heritage of the Nation.

-Bold out of original context-

ARTICLE 429. VIOLENCE AGAINST PUBLIC SERVANTS. Whoever exercises violence against a public servant, by reason of his functions or to force him to execute or omit some act of his office or to carry out one contrary to his official duties, will incur in prison from four (4) to eight (8) years.

Concluding finally that an act of vandalism within the framework of a seizure of public space that is not authorized by the mayor's office can be classified as a crime and also originate, in light of article 94 of our criminal legislation, the obligation to compensate the damage.

ARTICLE 94. REPAIR OF DAMAGE. Punishable conduct gives rise to the obligation to repair the material and moral damages caused by it.

It will therefore correspond, and to conclude this document, to the district or municipal mayor's office to guarantee the rights of all its associates through the exercise of their rights and especially their duty to protect coexistence in their categories of security and tranquility, which pray:

Security category: guarantee the protection of the constitutional and legal rights and freedoms of people in the national territory.

Tranquility category: Ensure that people exercise their rights and freedoms, without abusing them and with full observance of the rights of others.

Image Source:
https://www.alertapaisa.com/noticias/nacional/por-que-los-vandalos-quedan-libres-en-pocas-horas-en-colombia

References
Political Constitution of Colombia. Constitutional Gazette No. 116 of July 20, 1991
Law 1801 of 2016. By which the National Code of Citizen Security and Coexistence is issued. Official Gazette
No. 49,949 of July 29, 2016.
LAW 599 OF 2000. By which the Penal Code is issued. Official Gazette No. 44,097 of July 24, 2000
Royal Spanish Academy. Spanish dictionary. www.rae.es

Julian David Urrego Atehortua
(Colombia) Lawyer.

Stateless: the ghosts of the international system

By Marianna Crudi and Alberto Carracedo (Argentina)

The purest manifestation of a threat to human security is the invisible one, the one suffered in the solitude of a nomadic destiny and with no possible return. With the disinterest of others, whether they are simple citizens who ignore the presence of the newcomer or governments that capture him in local intrigues for which it is necessary to find those responsible. After all, what better than to observe with suspicion those who do not have a country to protect their own.

Thus, statelessness, the lack of recognition of a person's nationality, becomes the starting point of a life full of challenges, of silent suffering, of steps without a certain direction. Probably most individuals are not really aware of the privileges that shelter and protect under the protection of nationality, of the apparently insignificant belonging to a common and shared past in a citizenship, an amalgam of histories, challenges and efforts that are inherited with the land we walk since we were children.

Nationality becomes, then, the gateway to a life that would seem ideal, one in which all people are free, worthy and equal, enjoying the same social, civil and political rights; and in which there are authorities that ensure their safety.

However, the unreality of this idealism of the dream life faces a disfigured version in real life in which the lucky and the unlucky, nationals and stateless people coexist.

Needless to say, this story is not new and the reasons that explain it are rooted in the political, legal, religious and social system. It is its multiplicity of causes that complicate the resolution of the conflict, which deepen the cracks in a society that, after all, is inhabited by all, the privileged and those who are not.

In this context, the concept of human security bursts in at the end of the 20th century, revolutionizing traditional theorizing.

Previous perceptions, whose objects have been the States and the sole purpose of defending national sovereignty materialized in the territory, maintaining the very survival of the unit in the face of an anarchic international context; They are understood when considering world history as a story of experiences filled with warlike confrontations in which the protection of one's own resources and military capabilities became the main premises.

In this new approach - human security - security is associated with the well-being of the population. Where the well-being of a person originates in their integrity, multiplies with their freedom and is realized in its entirety with the opportunity to satisfy basic needs.

Not having a nationality could be mistakenly understood as a condition of eternal freedom; but this idea of being free is not enough, if freedom does not allow the individual to be happy. No person could be happy or enjoy apparent freedom if they suffer from hunger that they cannot satisfy, health problems that cannot be taken care of, and if they live surrounded by conditions that threaten their integrity and that of their family.

And, although a life of this style, without the enjoyment of opportunities to grow, would seem inconceivable, at least in the threatening extreme in which statelessness is consolidated, the only truth is that there are millions of people under this condition. Homeless state protection and often expelled from the social system. His disengagement from the community is surrounded by despair and need, sometimes generating elements of resentment.

The social anomie that characterizes the stateless state becomes an opportunity for those with the most terrifying ends to appear as saviors. No one is saved from this fate when necessity takes precedence over morality. Children, youth and adults, individually or entire families, regardless of their race or religion, are seen as members of an illegal system whose sole purpose is the generation of wealth at the expense of their servants and through their exploitation.

Thus, international organized crime, illicit trafficking networks for drugs and chemical precursors, human trafficking for the purpose of sexual and labor exploitation, forced labour, slavery and terrorism, come to be conceived as the closest horizons of the excluded from societies, from the denied of the nation. Of those who have no choice in the face of such aberrations and give up their lives in the hope of being able to get out of such hells in the future.

According to the United Nations High Commissioner for Refugees (UNHCR), by the end of 2019 there were 4.2 million stateless people in the world (1) and, although most of these people are in Asian countries such as Myanmar, Kuwait, Thailand and Iraq, it would be naive to think that it is a problem that is foreign to our reality. Due to both the quantity and the ability to co-opt and transfer the aforementioned criminal organizations, it is a potential breeding ground for damage and terror.

A latent threat to the integrity of the people who use our region as a factory, transit and destination. One misfortune, among many, that condemns Latin Americans to live in the most violent continent in the world (2).

The stateless are a palpable exposure of humiliation to people, with potential projection on the entire world. Helplessness and lack of protection available to those who offer only one hope. True ghosts of the international system.

Stateless people live in a world where home means nothing to them, and where it seems that, as Hannah Arendt anticipated, there is a right to have rights. And so, the deprivation of having a recognized place in the concert of nations it is the basic manifestation of the violation of a person's human rights.

Already the German philosopher - who experienced first-hand the heartbreaking advances of Nazism - pointed out that people without rights "are deprived, not of the right to freedom, but of the right to action; not of the right to think what they please, but of the right to opinion" and, what is worse, "privileges (...), injustices for the most part, favorable and unfavorable events, happen to them as accidents and without any relation to what they do, did or can do" (Arendt, 1951: 247) (3).

Saving the distances that separate us from the historical moment in which Arendt wrote the previous quote, and taking the necessary precautions to allow such an analogy, it is possible to affirm that the world today has very similar characteristics to those of the worst decades of the last century.

The international system must commit itself so that the stateless cease to be ghosts and become embodied in new, dignified and self-sufficient lives. But this will not only be a duty of the government leadership but of society as a whole.

The incipient century requires a new social contract that puts in check all that manifestation that violates the human rights of people, true human rights and not a barrage of light or ideologically biased declarations.

It is not going to be a thing that necessity leads those without a country to mutate into demons at the hands of the devil himself.

References
(1) https://www.acnur.org/datos-basicos.html
(2) https://www.unodc.org/documents/data-and-analysis/gsh/Booklet2.pdf#page=18
(3) Arendt, H. (1951). The origins of totalitarianism.

Image Source:
https://sites.google.com/site/human-rightsgregcaro777/-what-are-the-human-rights

Marianna Anabel Crudi
(Argentina) Degree in Government and International Relations (UADE), Diploma in Business and International Relations (WYA), She has completed a Master's Degree in National Strategic Intelligence from the National University of La Plata (UNLP). Director of the Institute of Transnational Affairs at the Fundación Pro Humanae Vitae. Researcher at the Center for Contemporary Middle East Studies (CEMOC-CARI).

Alberto Carracedo
(Argentina) Former Infantry Officer of the Argentine Army (CMN), Bachelor of Administration (UNPA), Master of Business Administration (UB). He has completed the Master's Degree in National Strategic Intelligence from the National University of La Plata (UNLP). Undergraduate and postgraduate university professor, and analyst of aspects that make security and defense from the economic sciences. Member of the Global Intelligence and Security Community (CISEG).
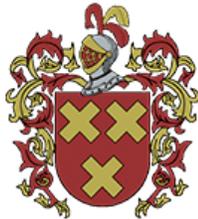
fuerzasmilitares.org
el portal militar colombiano

Islamic radicalization in video games: "A war without borders"

By Micaela Abril Álvarez (Argentina)

Radicalization in Networks

In the present work, in the absence of official definitions of the words "terrorism" and "radicalization", we will define the latter as "the process in which an individual adheres to radical opinions, points of view and ideas, tending to promote of the conflict and use of violence, which can lead recruited individuals to commit terrorist acts (1)."

From the Caliphate to the Cybercaliphate

The process of globalization opened its doors to a continuous technological advance and an interconnected world. Without going into details, we will establish a midpoint on the positive and negative perspectives (2) of globalization, where many of its benefits can be used to transgress order and social welfare.

In recent years, terrorism has stood out for the use of computer tools or "Islamic Propaganda", not only to spread its message, but also for recruitment and radicalization through social networks. The relative anonymity of online users and the instant global connectivity of the 21st century offers a long list of advantages for those who wish to carry out their crimes without being discovered.

The Daish terrorist organization (3), managed to adapt to these new modalities, and migrated towards a "virtual caliphate" after losing the occupied territories in Syria and Iraq.

Capture in networks

The proliferation of social media platforms used by terrorists and radicalized has alternated over the years; From Twitter, where Abu Mohammad Al - Julani (4) encouraged his followers to actively participate, "make your computer a bomb and not stay in the comfort of Telegram ", to Diaspora, Friendica , Quitter , Justpaste , Ask.fm, Soundcloud , TikTok , Sarahah17, and Mixlr after their accounts were blocked.

They use certain websites, radio stations, promotional videos of Clanging of the Swords 5IV and its magazine Dabiq to spread their ideology and infiltrate the network without leaving a trace by using Tor and their own encryption software. In addition, it is usual to see the use of steganography to avoid cyber espionage . This technique allows you to hide data files in photos making it look like any other.

also use encrypted mobile services such as Viber, Surespot , Wickr, FaceTime, Kik , Skype, WhatsApp and Telegram to communicate .

Through the Swarmcast model (6), sympathizers spread and viralize terrorist material through social networks.

Despite the fact that various social networks are investing in artificial intelligence-based programs to control the spread of terrorist propaganda, extremists continue to find alternative ways to spread their messages. International law and policy have not been enough to prevent extremists from using the World Wide Web as a strategic asset.

dissemination of propaganda

Daish uses propaganda and misinformation by spreading its ideology to as many people as possible in multiple languages. In February 2015, former President Obama argued: "The high-quality videos, the online magazines, the use of social networks, the terrorist Twitter accounts, everything is designed to attack today's youth online, in the Cyberspace". On his Twitter platform, he shares videos, texts, memes, infographics, links to his magazines and other media. His followers upload terror-inspiring videos daily, broadcast live from the battlefield, messages depicting a utopian life under the Islamic caliphate.

Video game

The Daish not only limited himself to social networks, but also turned to video games to attract young people, appealing to online FPS games in English (first person shooters) such as Call of Duty , Grand Theft Auto, Counter Strike, ARMA III, Battlefield , among others.

According to Global Terrorism Index 2019 (7) this "Allows the Daish to tap into the roughly 57% of the two billion who play first-person shooters, most of whom represent their target demographic: young, mostly male, and tech-savvy. "

The strong correlation between the personal experiences of individuals and the psyche of young people means that there are vulnerable people, with a greater tendency to radicalization. Risk factors such as anomie, Islamophobia, injustice (real or perceived), exclusion, religious extremism, not feeling accepted in society, perceived discrimination and lack of identity may be contributing to the radicalization of Muslims in European soil. The role that the Internet and certain social networks can play according to the European Commission (2005) is also emphasized. These variables make manipulation easy work to exploit channeled feelings of hate, frustration, and revenge. This is where the adaptations of the original video games play a fundamental role in consolidating a subculture of violence, unleashing systematic hatred against infidels and apostates, reaching the dehumanization of their targets.
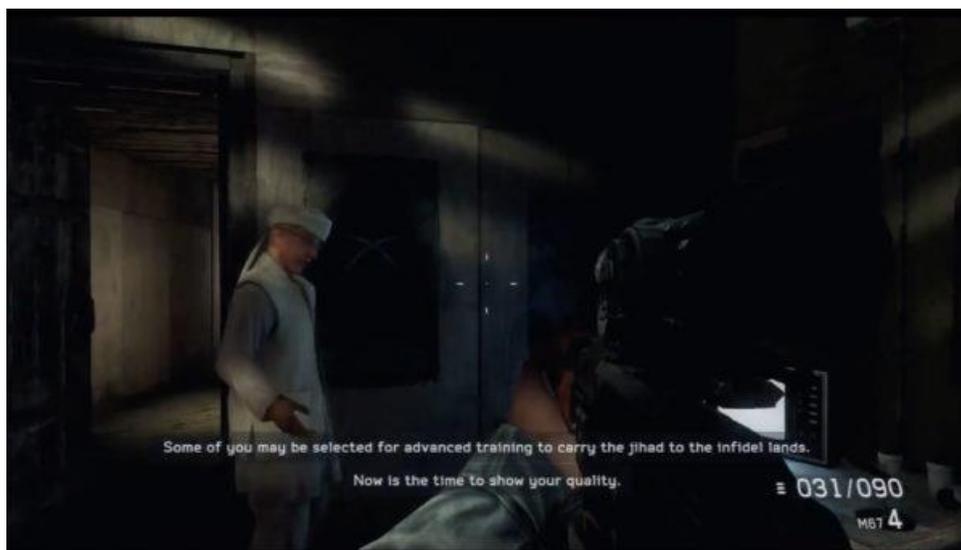
Image 1 Jihadi mock training (Source: Aim Down Sights . 2018)

Absorbed in a parallel world where it is possible to be whoever we want, we are faced with a scenario that allows terrorist acts to be carried out without consequences, which offers us players fully committed to choosing the side of the terrorists, interacting and sharing their ideals with other players.

Image 2 GTA (Source: Rayal Al -lawheed)

In terms of its development, it is not difficult to make changes to the original GTA game by customizing your character skins, downloading them via the Deep Web, or playing opposite roles similar to the US Army and Modern Warfare 2. The Game reached its popularity in September 2014, based on a Google search in Arabic using the term "Download Salil al -Sawarem game ". (8)

It is called " Salil al -Sawarim " in Arabic (The clanging of the Swords), which is a first-person shooter (FPS) game. Its cover reads: "What you do in the game, we do on the battlefield." In other words, the kinds of actual armed confrontations Daish engages in are similar to the virtual wars produced in Western video games.

The games are characterized by maintaining an aesthetic identical to the original. In the case of the GTA trailer published by Daish, it shows images of explosions, attacks with sniper rifles and gunfights. Its quality and resemblance to the original game would confuse many if the nasheeds (religious songs), the Daish banner at the top of the screen, and the Arabic subtitles call for the fight against American forces and the " Safavid Army ", reference to Iranian or pro-Iranian forces .

Image 3 Grand Theft Auto (https://theintercept.com/2014/09/17/grand-theft-auto-isis/)

The author of the adaptation is unknown because it is not produced by the Daish's centralized Ministry of Information, such as Al- Hayat , Al - Furqan and Al- Ethar, especially since the group opposes entertainment activities such as listening to music or games that can "divert attention from prayer and faith."

It's also unclear whether or not the game was actually produced; since the links that lead to the video game lead to torrent websites that do not work or to files with an unthinkable weight for a game with these graphics. Therefore, the game is believed to have been developed by some Daish sympathizers, probably outside the Middle East region.

Image 4 and 5 GTA. Daish banners can be seen

Image 6 GTA references the 9/11 attack, clearly showing skyscrapers about to be destroyed.

It is important to reinforce that the empirical violence of terrorism is beyond our reach if governments do not take the corresponding measures. What is at stake is the symbolic power of terror over us through our consumption and reproduction of its image in video games.

There is a tendency to demonize this type of game as violent for children when the PEGI +18 requirement appears on their covers, being only suitable for adults. However, we do not only find extremist material in first-person shooters, as is commonly believed. Modifications have been made of "The Sims", where a terrorist kills Muslims inside a mosque, and Minecraft, where the player shoots civilians with a semi-automatic rifle .

The process of radicalization through video games comprises four steps:
1. Recruitment by chat
2. Invitation via Tor or Twitter
3. Disclosure through the Deep Web.
4. Communication via Telegram or other mobile services.

In this way, we see that terrorism involves a whole reality of symbols, of geopolitics, of historical social narratives, and of real-world politics unfolding in the present. This sets it apart from any other violent game. You can no longer talk about the violence that a game provides as entertainment. Not to be missed is a game that allows you to choose a bomb vest as your weapon. However, quoting FBI agent Ali Soufan : "The real battle lies in the battle against the ideas and methods that terrorists use to recruit, if we are not able to act against these ideas, this war will never end." In other words, we will never be able to really fight terrorism if we continue to see it as a certain substance and not what it really is, a methodology.

It causes an abduction of the personality of radicalized young people, who leave behind the life they once had, giving themselves completely to an external cause, prisoners of an ideology that they not only became their own, but would sacrifice thousands of lives for it.

In conclusion, given the existing possibility of being radicalized from anywhere on the planet and from the comfort of our home, it is the responsibility of each Nation to establish a Critical Infrastructure Protection Plan, as well as national and international cybersecurity cooperation strategies, in order to protect ourselves, prevent and combat terrorism in a viable way.

Notes
(1) Understood as the act of instilling terror or fear in the population, for political, religious or economic purposes.

(2) It refers to the negative Marxist perspective and Hilferding 's Financial Capital as the predominance of capital, imperialism and the hegemonic power of a minority over the majority, and to the optimistic perspective, commonly found in currents

neoliberals, which sees the processes of globalization as the emergence of a new era of opportunities, free markets and economic growth for new actors.

(3) Or erroneously called by some media as Islamic State

(4) "He is a Syrian jihadist terrorist, commander-in-chief of Tahrir Al - Sham , the Syrian branch of al-Qaeda. In addition, he was emir of his predecessor organization Jabhat al - Nusra , like this one, adhered to al-Qaeda."

(5) Documentary film made by Daish as propaganda material. In it they

They highlight executions and torture of their prisoners.

(6) This model suggests that sympathizers gather like a swarm of bees or birds that are always rearranging themselves and are ready to pounce and pounce at any given moment.

(7) Institute for Economics & Peace. Global Terrorism Index 2019: Measuring the Impact of Terrorism, Sydney, November 2019. Available from : http://visionofhumanity.org/reports (accessed 11/29/2019)

(8) " Salil al -Sawarem " is also the name given by Daish to their religious chant, which should be distinguished from the video game.

References

Ahmed Al -Rawi (2018). Video games, terrorism, and ISIS's Jihad 3.0, Terrorism and Political Violence, 30:4, 740-760, DOI: 10.1080/09546553.2016.1207633

Cori E. Dauber, Mark D. Robinson, Jovan J. Baslious , and Austin G. Blair. Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos. Perspectives on Terrorism

Vol. 13, No. 3 (June 2019), p. 17-31 (15 pages)

Ahmad M, Shehabat . Beyond Twitter Revolutions: The Impact of Digital Media Logistics on Terror Networks of Communication in Iraq and Syria from 2014 on Terror Networks of Communication in Iraq and Syria from 2014 to 2016.

Amid Telegram Crackdown, Jihadists Seek Alternate Platforms While Some Hold Steadfast

Image Source:
https://fundacionaprenderamirar.wordpress.com/2017/11/29/pasos-para-evitar-la-adiccion-a-los-videojuegos/

Micaela April Alvarez

(Argentina) National Technological University. Buenos Aires Regional Faculty. Professional Specialization in Terrorism and Cybersecurity.

System for the Protection of Critical Infrastructures of the Argentine Republic: Cyber intelligence for decision making

By Agostina Taverna and Rodrigo Cárdenas Holik (Argentina)

Summary - Considering the rise of cyber threats and cyber attacks against critical infrastructures in the world, it is clear that Argentina must be prepared to anticipate, prevent, protect and defend those infrastructures that provide essential services. It is the State that has the responsibility to guarantee the normal and continuous operation of said services, through the elaboration of national regulations by the Legislative Power and their compliance by the Executive Power, in order to avoid any impact on human life, the economy, the exercise of human rights and individual freedom as well as national sovereignty.

Faced with this, the objective of this work is to raise the need to create a national and institutional system, specialized in the subject, which, through an innovative and multisectoral scheme, with inter-agency articulation , works symbiotically with others of its style and existing , in favor of organizing the Public Administration. With this purpose, concepts such as intelligence, cyber intelligence , cyber threats , cyber attacks, cyber security and cyber defense are presented around the protection of critical infrastructures, with the ultimate goal of deciding which path Argentina should take under future scenarios and prospects, enhancing the possibility of making strategic decisions for our country .

Keywords - cybersecurity - intelligence - cyberintelligence - critical infrastructure national protection system - cyberthreats - prevention.

INTRODUCTION

Argentina has a series of organizations, at the national level, with different functions and scopes, whose ultimate goal is to protect the country against threats, without distinction of origin, the actors involved or the way in which those actions are carried out. In the face of a war or a crime, the State has existing elements established by law whose action in a coordinated, joint and cooperative manner would allow decisions and measures to be taken to guarantee sovereignty, protect the rights and guarantees of society as a whole and its heritage, as well as the representative, republican and federal system established by the National Constitution. On the other hand, part of the stability and durability of a democratic society is based on the population's confidence in the State.

For this, the authors consider that it is essential that the National Public Administration be the one to guarantee the normal and continuous operation of essential services - supported by infrastructures considered critical - whose responsibility falls on public organizations and private entities with state control bodies. The partial or total interruption of any of these services could generate chaos, confusion, disturbance of public order, panic, affect health and human life, damage to economic development and territorial integrity, as well as uncertainty about the perpetuity of a constitutional government.

In order to avoid this and considering the national, institutional and governmental systems that currently exist, it will be necessary to articulate all those actors that are related to the protection of said critical infrastructures in favor of safeguarding the republic and the values it represents, in addition to establish the responsibilities of each one to build the base that would allow preserving cyberspace and services considered essential in Argentina. To this end, it will be essential that the inter-agency and multi-level link weigh, through a strategic vision, cybersecurity and cyberdefense (through decision-making tools such as cyberintelligence) as pillars of information protection that serve as steam for a machinery that provides substantial benefits to society.

STATE OF THE ART

Institutional and national systems in Argentina

The Royal Spanish Academy asserts that the term system comes from the late Latin systēma , and this from the Greek σύστημ α sýstēma and presents various definitions where "a set of things that are related to each other contribute to a certain object" [1]. Despite being a general definition, it is possible to extrapolate it to the concept that an institutional system integrates and brings together a set of elements that, related to each other in an orderly way, contribute to the fulfillment of a specific object or function. In addition, "an integrated system is a link to conform to models of shared values, in the interest of the subjects" [2] where the institutions or elements must make voluntary, directed and coordinated efforts to fulfill their mission.

In Argentina, considering the theme to be developed in this paper, it is possible to find different national institutional systems that exclusively bring together governmental elements, as is the case of the National Intelligence System (SIN), the Internal Security System (SSI) and the Security System. of National Defense (SDN) whose guidelines are defined by the President of the Nation. In general terms, these systems are characterized by grouping different bodies or institutions of the public sphere that maintain their main functions and objectives, but are brought together in an integrating system in order to guarantee sovereignty, safeguard the rights and guarantees of society as a whole. and its assets, as well as the representative, republican and federal system established by the National Constitution.

Specifically, the SIN brings together the Federal Intelligence Agency (AFI), the National Directorate of Criminal Intelligence (DINICRI) and the National Directorate of Strategic Military Intelligence (DINIEM), and is defined as the "set of functional relationships of the agencies of intelligence of the National State, directed by the Secretariat of Intelligence for the purpose of contributing to decision-making in matters of external and internal security of the Nation" [3]. On the other hand, the Internal Security System is made up of the President of the Nation, the governors of the province adhering to Law No. 24,059, the National Congress, the Ministers of the Interior, Defense and Justice, the Security Police Airport and the provincial police of those provinces that adhere to the norm as well as the National Gendarmerie and the Naval Prefecture, and "has the purpose of determining security policies as well as planning, coordinating, directing, controlling and supporting the national police effort aimed at compliance of those policies" [4]. On the other hand, the National Defense System "will be oriented to determine the national defense policy that best suits the country's needs, as well as its permanent updating" [5] and composed of the President of the Nation; the National Defense Council; the Congress of the Nation; the Minister of Defense; the Joint Chiefs of Staff of the Armed Forces; the Army, Navy and Air Force of the Argentine Republic; National Gendarmerie and Argentine Naval Prefecture in the terms prescribed by this Law; the People of the Nation through their active participation in the essential issues of Defense, both in peace and in war, in accordance with the rules that govern mobilization, Military Service, Civil Service and Civil Defense.

<u>Intelligence</u>

Currently, Argentina has the National Intelligence Law (Law No. 27,126 of the year 2015) which establishes the legal, organic and functional bases of the SIN. In a complementary manner, the New Doctrine of National Intelligence approved the organic and functional structure of the AFI and makes explicit that "national intelligence is an activity that falls within the framework of the social and democratic constitutional state of law, fundamentally aimed at producing knowledge about the problems – risks, conflicts – inscribed in national defense and internal security, always based on the protection and promotion of the political, institutional, social, economic and cultural interests of the Argentine people" [6]. The authors consider that these problems - especially terrorism, organized crime and actions that threaten cybersecurity - must be addressed for the purposes of prevention and/or conspiracy, with the aim of safeguarding, protecting and stabilizing the democratic system. . It is our opinion that, in addition, the National Intelligence Plan should contain the set of actions aimed at covering the need and demand for information for decision-making and implementing policies that guarantee the democratic state of our nation.

The production of national intelligence comprises a series of activities known as: strategic national intelligence, counterintelligence, criminal intelligence and military strategic intelligence. The first contemplates the production of intelligence from the comprehensive analysis of the set of problems that affect national defense and internal security. This superior product is developed by professional staff belonging to the governing body of the SIN, the AFI. Counterintelligence includes knowledge of the deployment and intelligence activities carried out by national or foreign individuals, groups or agencies, which may affect national defense and internal security. In other words, counterintelligence must be generated by all members belonging to the SIN. On the other hand, criminal intelligence refers to complex criminal problems of federal relevance related to terrorism, attacks against the constitutional order and democratic life, organized crime and attacks against cybersecurity. This is the faculty of the DINICRI. On the other hand, military strategic intelligence is related to possible risks and/or conflicts generated by aggressions of external origin perpetrated by armed forces belonging to other States against the sovereignty, territorial integrity or political independence of our country. Based on the foregoing, this intelligence corresponds to the DINIEM portfolio.

In any of its dimensions, the intelligence product is based on a circular process known as the intelligence cycle [7], which is made up of a series of stages whose iteration must occur according to the phenomenon under analysis. The stages that make up the cycle are: direction, obtaining, elaboration and dissemination.

Fig. 1. Intelligence cycle: "ideal" model.

In the work "The Complex Intelligence Cycle: an agile tool to operate in a network" [8], the classic cycle composed of these four phases is evaluated from a critical perspective. However, other countries have sub-phases or add other stages [9] such as, for example, the Spanish process which considers that the preparation stage has sub- phases such as assessment, analysis, integration and interpretation. In general terms, it is disconcerting to observe that, despite being a cycle and assuming constant feedback, it is stated that the final stage of the intelligence cycle is diffusion.

In the same line of ideas, Javier Jordán reviews the intelligence cycle [10] and clarifies that according to the ideal model, the intelligence process follows the same four phases where:

(1) During the direction stage, the demands and needs of the governmental and political authorities are presented. These are transformed into specific requirements, which initiates the assignment of tasks and resources.

(2) In the obtaining stage, information is searched for and collected, which is sent to the analysts once processed. There are several means and techniques of obtaining information, such as geographic and image intelligence, human intelligence, signals intelligence, measurement and signature intelligence, web intelligence, open source intelligence and technological intelligence, among others. [eleven].

(3) During the elaboration stage, the analysts receive the information which is evaluated, analyzed, integrated and interpreted. The result is reflected in a document or report for the decision maker.

(4) Finally, in the diffusion stage, the resulting product known as "intelligence" is delivered. In case greater clarity is required or there are new needs, the cycle could be reactivated.

Within the framework of the problem of cybersecurity in Argentina, the third annex of Decree No. 1311/2015 shows that the AFI has in its functional structure the Operational Directorate of Intelligence on Cybersecurity composed of the Directorate of Computer Intelligence and the Directorate of Intelligence on Computer Crimes. The Computer Intelligence Directorate produces intelligence related to "[…] the risks and conflicts linked to or derived from the use of information and communication technologies that affect national defense or internal security" [12]. On the other hand, the Intelligence Directorate on Computer Crimes produces "[...] intelligence oriented to the knowledge of activities that could configure computer crimes in any of its forms and modalities" [13] through intelligence officers and analysts specialized in cybersecurity . Said structure and organization chart allow us to deduce that intelligence on cybersecurity is produced. However, can we consider this as cyber intelligence ?

cyber intelligence

In recent times, cyber attacks have been transformed and are considered sophisticated and dynamic [14], being able to largely overcome the cyber defense and cyber security measures deployed. Faced with this, innovative solutions are required - from strategies to the use of preventive and/or defensive tools - that adapt to the complex nature of new cyber threats and cyber attacks. One of these tools could be the so-called cyber threat intelligence or cyber intelligence .

From what has been analyzed so far, we could infer that any cybersecurity event and/or incident (obtainable through sensors and devices in an active or passive way) can be conceived as the information to be used within the intelligence cycle for the analysis of cyber threats and the prevention of cyber attacks. Indeed, and because the source is a component of information and communication technologies (ICT), we could say that, through the intelligence cycle, the final product would be cyberintelligence .

In short, in this article we will consider cyber intelligence as the product that is obtained, processed, analyzed and disseminated when the information acquired is related to cybersecurity events and/or incidents. Cyber intelligence has the purpose of making decisions and countermeasures necessary to minimize the risk of occurrence of a cyber attack or the capabilities of an actor, whether criminal or state [15]. In the event that the risk materializes, cyber intelligence should present a scenario where the impact is slight enough to guarantee the resilience and continuity [16] of, for example, critical national information infrastructures.

Cyber threats and their global effects: Argentine critical infrastructures

It must be stated that any interruption - partial or total - in the provision of an essential service could result in catastrophic consequences, among which the impact on human life, the destruction of State institutions and external economic effects stand out. Indeed, the stability of the country and the citizen's trust in the State would be compromised if there were a massive and coordinated attack on one (or several) of the sectors defined as critical infrastructure (IICC). Some sources of threats to such infrastructures are foreign states, organized crime, terrorist organizations, and hacktivists ; which may be aimed at industrial espionage, data theft, sabotage, unavailability of the service, exploitation of malicious code, illicit disclosure of content and conflicts between nations, among others.

A threat is what an organization defends itself against [17], that is, in the event of an event, it must be prepared to respond to it. For this reason, organizations carry out a risk analysis (the second annex of Resolution No.

1523/2019 defines it as "a process that includes the identification of information assets, their vulnerabilities and the threats to which they are exposed, as well as such as the probability of occurrence and their impact, in order to determine the appropriate controls to treat the risk"), which allows understanding the nature of the risk and determining its level. It is the weaknesses (in the form of vulnerabilities) and the threats (in the form of risks) that must be weighed in order to guarantee the continuity of any organization, knowing that cyberspace is a vector that directly or indirectly connects the IICC with the world.

Regarding cyber threat , Resolution No. 1523/2019 defines it as a "threat to systems and services present in cyberspace or reachable through it" and must be detected as soon as possible since the response time is essential. For this, it is possible to obtain anticipation capacity by knowing the actors, their methods, their capacities and their successes in similar scenarios. A study [18] stipulates that the average detection time of a cybersecurity incident is 206 days and that it takes an average of seventy-three (73) days to contain it, this is called the "life cycle of a breach". ". To reduce that time, threat hunting concepts are applied . hunting , an activity similar to threat detection [19], where attack hypotheses are proposed as a proactive initiative, the capture of information through telemetry and the use of targeted attacks, among others. Indeed, the information that is generated in the components of a network of interconnected elements about cybersecurity events or incidents can be captured and analyzed in order to prevent the expansion of the incident and contain the effect [20], maintaining the resilience of organizations considered as critical infrastructures from the tactical point of view of a sensor at the endpoint level that has a strategic value in the IICC as a whole.

At a global level, there is a history of cyberattacks that have affected critical infrastructures, such as the one that occurred in Estonia in May 2007 – considered the first act of cyberwarfare. There, following a conflict over the relocation of a statue of a Russian World War II hero, Estonia suffered several coordinated cyberattacks that affected financial, police, emergency services, the parliament, ministries and news services [21]. . On the other hand, in 2010 the Natanz plant (Iran) suffered damage to the uranium enrichment centrifuge system as a result of an infection by the malicious code known as stuxnet [22]. It is possible to find another example of a cyberattack that occurred in 2012, where the oil and gas pipeline company Saudi Aramco was affected by another malicious code that lost 30,000 jobs. Five years later, in Ukraine, another malicious code impacted the distribution of electricity in December 2015, which caused a town of around 1.5 million inhabitants to lose electricity [23]. In 2017 there was a wave of various ransomware -type malicious codes whose purpose was to extort money from individuals and organizations in cryptocurrency format to decrypt the information residing on victims' hard drives [24]. Closer in time and during the covid-19 pandemic, Australia suffered a series of sophisticated cyberattacks and under the alleged sponsorship of a sovereign state in June 2020. According to what was expressed by the Prime Minister of that country, Scott Morrison, this affected government, industries, political organizations, education, health, providers of essential services, and operators of other critical infrastructure [25].

In general terms, these cyberattacks are characterized by being sophisticated, volumetric, of diverse origins (including possible government support and financing), with campaigns that can last from days to years, and with a high level of impact on the operation of the IICC. , which must not escape the eye of the national authorities. Luis María Mozzoni affirms that "Argentina is one of the countries with the highest internet penetration rate in the region, considering the amount of strategic natural resources such as oil, gas, fresh water, biodiversity or strategic minerals that we have in our extension. geographical" [26], it would not be unreasonable to notice the idea that cyberattacks could soon impact our country.

In Argentina, the IICC were defined generically as "those that are essential for the proper functioning of essential services of society, health, security, defense, social welfare, the economy and the effective functioning of the State, whose destruction or disturbance, total or partial, affects and/or impacts them significantly" [27] while critical information infrastructures "are the information, operation and communication technologies, as well as the associated information, which are vital for the functioning or the safety of Critical Infrastructures" [28]. In both cases and through this same resolution, eight identification criteria were established for said infrastructures and eleven sectors such as energy, ICT, transport, water, health, food, finance, nuclear, chemical, space and State. Among the sectors to consider could be infrastructures considered as critical whose responsibility is both public organizations and private companies.

In adherence, in July 2017, through Decree No. 577, the Cybersecurity Committee was created, made up of the Ministries of Modernization, Defense and Security. Two years later, through Decree No. 480/2019, its composition was expanded with representatives from the Secretariat for Strategic Affairs, the Ministry of Foreign Affairs and Worship, and the Ministry of Justice and Rights as a result of the global reach and international approach to threats. The creation of the Committee is based on the need to obtain the "capacity to respond to

large-scale security incidents, legislation on the matter, the protection of critical infrastructures, the ability to collaborate with other countries, as well as the security culture developed by citizens" [29]. As its main objective, the Committee had to prepare the National Cybersecurity Strategy and the action plan that would allow its implementation in coordination with the competent areas of the National Public Administration, in addition to "establishing the guidelines and criteria for the definition, identification and protection of national critical infrastructures" [30].

The strategy, approved and published in May 2019, is considered a foundational and living document, whose update would accompany the evolution of technologies. There, the essential principles and eight central objectives of the country are defined with regard to the protection of cyberspace, on which the deployment of concrete actions is expected. The eighth objective refers to the protection of national critical information infrastructures and includes the promotion of the definition, identification and protection of said infrastructures, as well as the articulation of the public-private sector for the construction of detection capacities, protection and response to threats of attack, the strengthening of cooperation for the exchange of information or knowledge that allows the development of a common culture regarding the protection of the IICC and that is built on the basis of mutual trust.

PROPOSAL

In this article, the need to create the System for the Protection of Critical Infrastructures of the Argentine Republic (SIPICRA) is raised, made up of all the actors - both public and private - that are related to critical infrastructures declared as such and their protection. In addition, the importance of articulating this System with the SIN with the aim of increasing the prevention and resilience of Argentine critical infrastructures through the production of cyber intelligence is raised .

ARGUMENTATION

In favor of fulfilling the eighth objective of the strategy, the authors consider it essential that Argentina identify the infrastructures that provide essential services and determine their criticality based on a diagnosis that allows recognizing those information assets, systems and networks that are in true critics. Based on this, a risk analysis should be carried out, an adequate strategy for its management should be designed, together with a National Plan for the Protection of Critical Infrastructures that contains effective prevention and protection measures against possible threats both at the level of physical and ICT security.

On the other hand, with the identification, determination and declaration of the national IICC in Argentina, it will be necessary to establish the rights and obligations of each of the infrastructures - whether grouped by sector, generalized or specific - in order to carry out the monitoring and control required for their protection and defense. Likewise, based on the criticality of each infrastructure, sectoral and security strategic plans and programs must be developed for operators and human capital that contemplate risk reduction and increased resilience.

Undoubtedly, the breadth of the concept of IICC and the multiplicity of affected sectors requires addressing its protection in a comprehensive and multidisciplinary manner. Even critical infrastructures rarely work in isolation, but, on the contrary, they tend to be grouped as a result of their dependency or interdependence where information and communications technology converge. Faced with this, joint work is required with all those sectors and agents that are related to which the authors consider should be created, through a multipurpose and transversal scheme, the Critical Infrastructure Protection System of the Argentine Republic.

Under this new paradigm of improving institutions to meet the most essential objectives for a Nation, its institutions and its people, the authors consider that SIPICRA would bring together such institutions and elements from the public and private spheres, and this effort should be characterized by be intersectoral, multilevel and created by law.

In principle, the Critical Infrastructure Protection System of the Argentine Republic should be made up of users, human resources, operators, owners, manufacturers, research, development and innovation institutions, regulatory authorities of the sectors, as well as public sector bodies. and from the private sector that have responsibilities and are related to the proper functioning of the essential services provided by said infrastructures. In addition, it should be headed by an organization whose primary responsibility is to supervise compliance with the regulations, norms, policies and plans of the subject matter; the articulation and coordination of the members

of the National Defense, Internal Security and National Intelligence Systems (taking into account the functions related to the protection of the IICC) and those critical operators that come from the public and/or private sector.

From the creation or determination of the body responsible for the SIPICRA, it will be necessary to include in it a dependent direction whose main function is the effective identification of the infrastructures considered critical based on an objective and reasonable methodology that quantitatively weights the criteria of identification established in the regulatory framework that should be developed. Likewise, this department should be responsible for determining the infrastructures considered critical, as well as managing and regularly updating the inventory with a "confidential" security classification that contains complete information such as the description of the infrastructures, how to contact the personnel of the same, geographic data, evaluated risks, among others. It is necessary to accompany the idea that "it is essential to expose [in the inventory] the link between services and assets and detail the facilities and systems (software, hardware, communications, etc.) that provide them, as well as the people involved in the different processes" [31] for their due protection.

It is our opinion that the responsibility for developing and coordinating the Critical Infrastructure Protection System of the Argentine Republic falls on the national government, due to its importance and direct relationship with national security. Furthermore, society claims that the State is responsible for ensuring the safety and guarantees of continuity of vital services, even when the IICCs are in the hands of private operators and companies. Faced with this, the authors consider that the regulated approach is a positive kick to implement mandatory policies for the protection of critical infrastructures through clear and transparent legislation, whose functionality is that of an instrument that allows promoting the cooperation of all sectors and articulation of agents that are part of the system.

In addition to the identification, determination, and the rights and obligations that derive from the declaration as critical infrastructure, the authors consider that SIPICRA should contemplate the need to coordinate the monitoring and warning of those infrastructures to be protected. The importance of this is related to the possibility of taking measures to prevent and/or anticipate emergencies through early warnings. Furthermore, permanent monitoring allows the generation of key information for the development of prevention strategies and action protocols against vulnerabilities, attacks and cyber threats that could affect essential services for society. This information can be obtained from internal sources (such as firewalls, router logs, and decoys - honeypots and honeynets - of critical infrastructures) or external sources (for example, vulnerability databases, forums, social networks, or information from the Internet). dark web among others). Taking into account the Argentine context, the authors consider that the State should incorporate into the System those existing organizations that currently have access to this information (such as incident response teams and security operations centers), in order to orchestrate and linking the information that is generated, as well as promoting the increase of monitoring systems at the national and international levels.

In parallel to this, because "the collection of information does not automatically translate into better results in the decision-making process" [32] and in favor of coordination between systems, this information could be shared with the Intelligence System. National. with the objective of, within the framework of compliance with the intelligence cycle, raising timely and pertinent cyber intelligence as a final product and producing a decision-making tool to anticipate and prevent any partial or total affectation of the infrastructures that provide essential services. As Nikolaos says Tsouroulas , "… .knowing and understanding our adversaries is crucial if we want to anticipate and detect new attacks that escape our defensive solutions. At this point, threat intelligence comes into play, providing us with the necessary information …"[33].

It is undeniable that, in pursuit of the prevention and protection of the IICC, the collection, analysis, integration and evaluation of the information provided by public and private sector organizations, as well as the security and police forces, and the armed forces (in addition to those sectors considered strategic) could be a considerable advantage against any cyber threat or cyber attack. Based on this, all the agencies belonging to the National Intelligence System - given the *expertise* of human resources, experience and internal processes - should closely collaborate to carry out the evaluation of threats and the analysis of risks on critical infrastructures. This would allow the design and presentation of the information (already considered as intelligence), through the use of adequate and secure communications mechanisms, to the person in charge of the Critical Infrastructure Protection System of the Argentine Republic with the aim of providing an early warning and reducing (or avoid) the probability of occurrence of a catastrophe.

There are various risk analysis methodologies (for risk management) and threat modeling (for the secure development of secure software) that are based on threat intelligence to propose possible scenarios, actors,

activities and modalities (forms of exploiting threats). vulnerabilities), which may be part of the cyberintelligence production process for the agency responsible for SIPICRA.

Indeed, the authors consider that the exchange of information is one of the most important elements regarding the protection of critical infrastructures, which does not escape the need to generate trust between the systems that would make up the Protection System. of the Critical Infrastructures of the Argentine Republic, such as the SIN. This exchange provides a better understanding of cyber threats , risks, dependencies and foreseeable effects, for which it is essential that it be agile and bidirectional, in order to increase the probability of designing and implementing appropriate countermeasures and preventing attacks that could partially or totally affect the IICC. Some of the benefits of such sharing are: it raises awareness of the need to protect IICCs (particularly related to business continuity management and risk management); improves the level of education, education and training, and knowledge on the subject; As information is shared, the skills of the operators and members of the system are increased and, even, the responsible body can address all or part of the System with specific information with an adequate security classification that prevents any disturbance of the IICC . The intelligence to be shared may be considered of a strategic, operational and/or tactical nature, and could occur within the framework of vulnerabilities and threats, allowing the promotion of coordinated efforts within industrial networks in favor of strengthening and safeguarding critical services. and productive.

CONCLUSIONS

The existence of various cyber threats, added to the international history of cyber-attacks against critical infrastructures, shows that organizations and agencies in the world have not been able to coordinate their cyber defense and cyber security mechanisms in favor of protecting them and society in general. general. Unfortunately, the Argentine Republic is not the exception.

Our country has a series of systems, understood as the set of public bodies that work in a coordinated and cooperative manner in order to safeguard the values of the republic, sovereignty, rights and guarantees, and the democratic system established by the Constitution. National, while protecting society as a whole. However, all current systems that have some level of incidence on critical infrastructures or national strategic objectives within their scope and objectives, are not coordinated in pursuit of their protection.

Faced with this existing organization, the authors consider that creating the Critical Infrastructure Protection System of the Argentine Republic will allow the coordination of all existing systems in pursuit of the protection of society and services that are essential through the use of an innovative scheme. and multisectoral, whose articulation will require joint efforts to guarantee a common understanding and a clear objective, with an excipient effect. Likewise, it may consider cybersecurity and cyber defense as pillars of the protection of the IICC and essential services, as well as cyber intelligence as an essential tool to decide which path Argentina should take under future scenarios and prospects.

Indeed, SIPICRA - through joint work with the National Intelligence System - not only means more capabilities for the identification, detection and mitigation of cyber threats and cyber attacks through the production of cyber intelligence , but also that all actors have a common language to understand the phenomenon and apply the necessary techniques in order to manage the countermeasures that guarantee the resilience of the critical infrastructures of the Nation and, ultimately, the democratic values of society.

References
[1] Royal Spanish Academy: Dictionary of the Spanish language, 23rd edition. Spain, 2019. Retrieved from: https://dle.rae.es/sistema
[2] M. Herrera Gómez, AMJ Castillo, "Generation and transformation of social institutions: morphostatic processes and morphogenetic processes". Spain, 2004. Spanish Journal of Sociological Research (REIS), No. 107, p. 49-88.
[3] Infoleg , Law No. 25,520, article 2, subsection 5. Argentine Republic, 2001. Retrieved from: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm
[4] Infoleg , Law No. 24,059, article 6. Argentine Republic, 1992. Retrieved from: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm
[5] Infoleg , Law No. 23,554, Article 7. Argentine Republic, 1988. Retrieved from: http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm
[6] Infoleg , Decree No. 1311, Annex 1, Page 12. Argentine Republic, 2015. Retrieved from: http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm

[7] National Intelligence Center, "The Intelligence Cycle". Retrieved from https://www.cni.es/es/queescni/ciclo/
[8] L. Martinez Viqueira , "The Complex Intelligence Cycle: an agile tool for networking", Spanish Institute for Strategic Studies. Spain, 2016. Retrieved from
http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO50-
2016_CicloInteligComplejo_MartinezViqueira.pdf
[9] JM Díaz, C. Greciano, " CRITICAL ANALYSIS OF THE INTELLIGENCE CYCLE" in Intelligence and Leadership - Leading intelligence. 2017. Retrieved from https://inteligenciayliderazgo.com/wp-content/uploads/2017/11/analisis-ciclo-inteligencia.pdf
[10] J. Jordan , "A Review of the Intelligence Cycle", Defense.com. Spain, 2016. Retrieved from
https://www.defensa.com/analisis-gesi/revision-ciclo-inteligencia
[11] M. Kamiński , "Intelligence Sources in the Process of Collection of Information by the US Intelligence Community". 2019. Retrieved from
https://www.researchgate.net/publication/340647256_Intelligence_Sources_in_the_Process_of_Collection_of_
Information_by_the_US_Intelligence_Community
[12] Infoleg , Decree No. 1311, Annex 1, Page 66. Argentine Republic, 2015. Retrieved from:
http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm
[13] Infoleg , Decree No. 1311, Annex 1, Page 67. Argentine Republic, 2015. Retrieved from:
http://servicios.infoleg.gob.ar/infolegInternet/anexos/245000-249999/248914/norma.htm
[14] W. Tounsi , H. Rais , "A survey on technical threat intelligence in the age of sophisticated cyber attacks ", Elsevier. France, 2017. Recovered from
https://www.researchgate.net/profile/Wiem_Tounsi/publication/320027747_A_survey_on_technical_threat_intel
ligence_in_the_age_of_sophisticated_cyber_attacks/links/59fc7cb70f7e9b9968bd9e02/A-survey-on-technical-
threat-intelligence-in-the-age-of-sophisticated- cyber-attacks.pdf
[15] Ernst & Young, "Cyber threat intelligence − how to get ahead of cybercrime". 2014. Retrieved from
https://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-
cybercrime/$FILE/EY-cyber-threat-intelligence-how -to-get-ahead-of-cybercrime.pdf
[16] Bank of England, "CBEST Intelligence-Led Testing. Understanding Cyber Threat Intelligence Operations. Version 2.0". England, 2016. Retrieved from https://www.bankofengland.co.uk/-/media/boe/files/financial-
stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf
[17] Threat Modeler, "Differences Explained: Threat vs. vulnerability vs. Risk". 2019. Retrieved from
https://threatmodeler.com/differences-explained-threat-vs-vulnerability-vs-risk/
[18] IBM Security, "Cost of a Data Breach Report." 2019. Retrieved from https://www.all-about-
security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf
[19] Tarlogic , " Threat Hunting , Improves the efficiency of detection and response to cyber threats". Retrieved from https://www.tarlogic.com/blackarrow-servicios-seguridad-ofensiva/threat-hunting/
[20] N. Tsouroulas , "Cyber Intelligence Based Detection and Response . Part 1: the basic pillars", Telefónica. 2018. Retrieved from https://empresas.blogthinkbig.com/deteccion-respuesta-ciberinteligencia/
[21] R. Ottis , "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", Cooperative Cyber Defense Center of Excellence. Estonia, 2008. Retrieved from
https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
[22] G. Romero Sanchez , "STUXNET: The first cyberweapon in history", Cronicaseguridad.com. 2018. Retrieved from https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia/
[23] INCIBE-CERT, " BlackEnergy and critical systems". Spain, 2016. Retrieved from https://www.incibe-
cert.es/blog/blackenergy-sistemas-criticos
[24] Redes Zone , "These have been the 5 most important ransomware attacks of 2017". Retrieved from
https://www.redeszone.net/2017/12/16/estos-los-5-ataques-ransomware-mas-importantes-2017/
[25] BBC News, "Australia cyber attacks : PM Morrison warns of 'sophisticated' state hack". 2020. Retrieved from https://www.bbc.com/news/world-australia-46096768
[26] L. M. Mozzoni . "Cyberwar, the attack on critical infrastructure as international policy and because Argentina has to work on this aspect." Blas Pascal University, 2019. Retrieved from:
http://www.vectus.com.ar/wp-content/uploads/2019/06/trabajo-final-API-UBP-Luis-Maria-Mozzoni.pdf
[27] Official Gazette, Resolution No. 1523/2019, Annex I. Argentine Republic, 2019. Retrieved from:
https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918
[28] Official Gazette, Resolution No. 1523/2019, Annex I. Argentine Republic, 2019. Retrieved from:
https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918
[29] Infoleg , Decree No. 577. Argentine Republic, 2017. Retrieved from:
http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm].
[30] Infoleg , Decree No. 577, Art. 2, inc. and. Argentine Republic, 2017. Retrieved from:
http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm
[31] M. Calvo Matalobos, "Ad-HOC Incibe - Protection of Critical Infrastructures". Spain, 2018. Retrieved from:
http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81225/6/mcmTFM0618memoria.pdf

[32] C. Gomes de Assis , "The new era of information as power and the field of cyber intelligence ", URVIO – Latin American Journal of Security Studies Number 19. Ecuador, 2016. Pg - 94-109 .
[33] N. Tsouroulas , "Cyber Intelligence Based Detection and Response . Part 1: the basic pillars", Telefónica. 2018. Retrieved from https://empresas.blogthinkbig.com/deteccion-respuesta-ciberinteligencia/

Image Source:
http://elite-formacion.blogspot.com/2018/07/el-sistema-nacional-de-proteccion-de.html

Agostina Taverna
(Argentina) National Technological University. Buenos Aires Regional Faculty. Professional Specialization in Terrorism and Cybersecurity.

Rodrigo Cardenas Holik
(Argentina) National Technological University. Buenos Aires Regional Faculty. Professional Specialization in Terrorism and Cybersecurity.

Carrying or possession of replica weapons against Colombian law

By Julián David Urrego Atehortua (Colombia)

The first thing that we must be clear about when addressing this issue is that in Colombia there is a monopoly on the manufacture and sale of firearms found in our national territory, for which it will only be the state that authorizes their use. bearing and possession.

However, according to Decree 2535 of 1993, of the Presidency of the Republic, in its sixth and following articles, weapons are classified as:

FIREARMS IN COLOMBIA

They are classified in

Weapons for Civil use   Restricted use weapons   Weapons of war or exclusive use of the Public Force
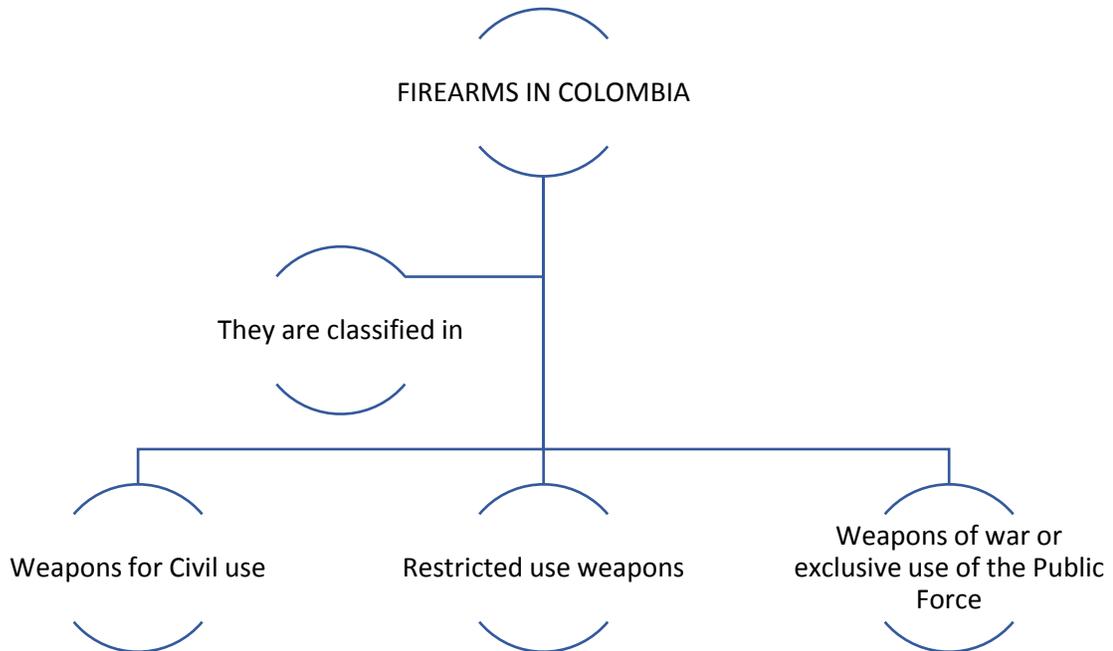
Taking into account the above, we will analyze only what corresponds to weapons for civil use, finding that according to the aforementioned decree, they are classified as:

ARMAS DE USO CIVIL

ARMAS DE DEFENSA PERSONAL   ARMAS DEPORTIVAS   ARMAS DE COLECCIÓN

All of the above require authorization by the Colombian Government for their possession and carrying.

In this article we will focus on weapons for **sports use**, which are defined in article 12 of the aforementioned decree, as follows:

Article 12.- Sporting weapons. They are the firearms that meet the necessary specifications to practice the shooting modalities accepted by the International Shooting Federation and the usual ones for the practice of the sport of hunting.

28

And about which, decree 2535/93 is emphatic when pointing out:

Article 16 (…) Sporting weapons will only be used in shooting and hunting activities, with the limitations established in the Law and the regulations, in particular the norms of protection and conservation of natural resources.

So that; In the first instance, it will be important to conclude that for the possession and carrying of a sports weapon, our affiliation to a sports club recognized by the Colombian shooting and hunting federation will be strictly necessary, as well as the respective government permit for its carrying and possession.

OF WEAPONS -REPLICAS-

Let's look at some exceptions:

Decree 2535/93

Article 25º.- Exceptions. Pneumatic, gas and long black powder weapons, including fist shotguns, do not require a permit to carry or possess.

In this order of ideas, the marketing, purchase, carrying and possession of this last class of weapons is legal, but their carrying has restrictions that we can find in Law 1801 of 2016, article 27, numerals 6 and 7, which enshrine the Prohibition of the same in certain scenarios, to understand it as a behavior that puts the life and integrity of people at risk and as such, making it clear that it is a behavior contrary to coexistence, let's see:

National Police Code.

6. Carrying weapons, cutting, sharp or similar elements, or dangerous substances in common areas or places open to the public. An exception is made for those who prove that such elements or substances constitute a tool for their sporting activity, trade, profession or study.

7. Carry pneumatic, air, blank, reduced lethality weapons or sprays , sprinklers, sprinklers or pepper spray or any element that is assimilated to firearms, in places open to the public where crowds of people are developed or in those where intoxicating beverages are consumed, or their irregular use is noticed, or a behavior contrary to coexistence is incurred.

In this way, the possession of weapons or replicas, in the aforementioned spaces, would give reason for the National Police to seize them and proceed with the imposition of a type 2 general fine, which for this year 2020 is TWO HUNDRED THIRTY-FOUR THOUSAND PESOS WITH EIGHTY CENTS M/L ($234,080) apart from the fact that entry to activity that involves complex or non-complex crowds of public would be prohibited and finally the property would be destroyed.

Precisely this last part, the destruction of the property, is the one that interests so many carriers of replica weapons, because as we have already seen, in article 6 already mentioned, there is an exception to carrying, which states: *It is excepted who proves that such elements or substances constitute a tool for their sporting activity, trade, profession or study.*

Situation that will have to be demonstrated with evidentiary elements oriented to exoneration, in the Police Inspection corresponding to the municipality of seizure of the weapon, within three days following the imposition of the subpoena and seizure of the weapon, in accordance with paragraph 1 of article 222 of Law 1801 of 2016 that enshrines the immediate Verbal Process of Police subpoenas.

In this regard, it is important for me to point out again, as we had already concluded, that the use of weapons -replicas- for sports activities will not be valid, as expressly stated by FEDETIRO:

Informamos que las actividades deportivas que se desarrollan bajo supervision de la Federacion Colombiana de Tiro y Caza Deportiva,no incluyen ninguna modalidad en las que se utilicen armas traumaticas, armas de fogueo o armas de airsoft. si requiere informacion de nuestras actividades, puede comunicarse con nosotros.

TRAUMATIC WEAPONS

Currently there is a legal vacuum regarding traumatic weapons, since these have not yet been recognized in the sports classification by the Colombian State and, due to their internal mechanisms, we cannot classify them as pneumatic, gas or black powder; reason why they would not enter the permit exceptions of the decree that we have been developing:

Decree 2535 of 1993

Article 25 Exceptions. Pneumatic, gas and long black powder weapons, including fist shotguns, do not require a permit to carry or possess.

In this order of ideas, there is no legislation in Colombia that regulates the commercialization (until now legal) the carrying and possession of these weapons.

However, in order to contribute to the debate on the subject, it is important to point out that, if we analyze the traumatic weapon, due to the impact and damage that its projectiles can have on the human being, it is clear that we are facing a weapon of reduced lethality, so much so that, in some countries, these are used for personal defense and in others, their use is prohibited.

TWO POINTS OF VIEW ON TRAUMATIC WEAPONS

LAW ENFORCEMENT PERSPECTIVE

The analysis then, that a police authority can carry out in the face of the seizure of these weapons, would have a legal basis, which would be precisely article 27, numeral 7 of Law 1801 of 2016 when it states: weapons of reduced lethality.

PERSPECTIVE OF THE CITIZEN OWNER OF THE WEAPON

On the other hand, the citizen could make use of the maxim of the law that points out: everything that is not prohibited is allowed, since in the absence of a classification of the traumatic weapon in the light of decree 2535 of 1993, the framework would not be clear. law applicable to its destruction, which is why its basis for defense at the instance of the Police Inspection would be the request for exoneration in order to request its return.

If this defense is not clear, the weapon could be destroyed, in accordance with the legal framework of Law 1801 of 2016, already cited.

These two perspectives allow us to make a second conclusion that the traumatic weapon may be seized, but it cannot be destroyed by the inspections when the aforementioned legal defense is advanced.

IS IT RECOMMENDED TO MODIFY THE BARREL OF A BLANK FIRM TO MAKE IT TRAUMATIC?

A common practice of some owners of blank weapons is the modification of the barrel so that they can be used with traumatic projectiles, this action alters the factory characteristics of the blank weapon, turning it into a magic weapon, which is totally prohibited, except fisto shotguns.

That is to say, that its carrying and possession would not only be prohibited, but could be subject to criminal sanctions, in accordance with Art 365 of the Colombian penal code.

ARTICLE 365. MANUFACTURING, TRAFFICKING, CARRYING OR POSSESSION OF FIREARMS, ACCESSORIES, PARTS OR AMMUNITION. Whoever, without permission from the competent authority, imports, traffics, manufactures, transports, stores, distributes, sells, supplies, repairs, carries or has personal defense firearms, their essential parts, essential accessories or ammunition in one place, will incur imprisonment. from nine (9) to twelve (12) years.

The same penalty shall be incurred in the case of handcrafted or handmade firearms, except fisto shotguns in rural areas.

-Bold and underline out of original context-.

OF THE TRANSPORT OF REPLICA WEAPONS

As a final recommendation, it is important that replica weapons be carried and transported in the original boxes in which they are sold, not in covers or fudges, nor in the waistband, because if it is done under these last mentioned modalities, it will be very feasible that are subject to seizure by the National Police, under the understanding that it is a behavior that puts the life and integrity of people at risk and, in case of being defeated in the administrative process before a police inspection, the same may be subject to destruction.

OTHER CONCLUSIONS

We end this writing, emphasizing that up to now we have cited two important conclusions, but the following will necessarily emerge from the text:

- The sale, carrying and possession of traumatic weapons is legal.
- A traumatic weapon can be classified as of reduced lethality, for which the seizure procedure of article 27, numeral 7 of Law 1801 of 2016 applies.
- The carrying or possession of sports weapons will only be valid if affiliation to a shooting and hunting club is accredited, which in turn is affiliated with the Colombian shooting and hunting federation.
- Possession of weapons -replicas- whether they are pneumatic, air, blank or reduced lethality, applies to the field of private property and not to public space.
- In the carrying or transportation of weapons -replicas- whether they are pneumatic, air, blank or reduced lethality, the argument that it is given for sporting purposes will not be valid.

- The card that comes with the replica weapons and that in its description only transcribes the Colombian legislation of Law 1801 of 2016 and Decree 2535 of 1993 is not valid as evidence.
- The membership card of a sports club will only be valid as evidence if said club is endorsed by the Colombian Shooting Federation.

References
http://www.cortesuprema.gov.co/corte/index.php/2020/04/30/corte-suprema-fija-limites-sobre-armas-de-fuego/
http://www.cortesuprema.gov.co/corte/wp-content/uploads/2020/04/SP911-2020.pdf
https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1540
http://www.fedetirocol.com/index.php/noticias/53-informacion-importante
https://www.youtube.com/watch?v=8usf9KelDXg&t=539s
https://www.youtube.com/watch?v=4_hMbrmwziE

Julian David Urrego Atehortua
(Colombia) Lawyer.

The caucasus again

By Guadi Calvo (Argentina)

Conflicto Armenio-Azerbaiyano

Once again the red-hot border between Armenia and Azerbaijan has made the news again, and puts the world in tension, due to the amount of interest and nations involved on both sides of the dividing line, which could drag the entire region into a war of historic proportions.

Between July 12 and 16, military actions took place that have left 17 dead, according to official data, five Armenian soldiers and 12 Azeris, in the Tavush - Tovuz sector , near Karabakh, where from 1991 to 1994 a war that left nearly 30,000 dead and a million displaced. The events occurred some three hundred kilometers from Nagorno- Karabakh , the usual battlefield for these clashes, which today is under the name of the Republic of Artsakh , a state without international recognition.

During the clashes in July, which would have been initiated by the interference of Azerbaijani -US troops in Armenian territory, according to its Ministry of Defense,

the Azeris would have lost a large amount of supplies, including drones that would have been shot down during the operations, which were exhibited in Yerevan.

To add more drama to the critical situation, Ankara released a statement saying: "Turkey will support any decision made by the fraternal Azerbaijani people in their just struggle." While Turkish Defense Minister Hulusi Akar , declared that: "Turkey and its army are ready to fully support Azerbaijan". What was considered as a direct threat by Armenia.

When the situation seemed to return to the "tense normality" that has prevailed on the border since the 1994 peace accords, signed in Bishkek, the capital of Kyrgyzstan, under Russian auspices, on July 27 in the early hours of the morning the Armenian military Ashot Mikaelián , was killed by an Azeri sniper, which increased tension even more and could undermine the efforts of regional structures such as the *Collective Security Treaty*

Organization or CSTO, made up of Armenia, Belarus , Kazakhstan, Kyrgyzstan , Russia and Tajikistan, for reaching a point of stability.

These border clashes are not the first to take place since 1994, in that same sector during 2014 and 2015, important clashes took place, but in 2016 what was known as "the four-day war" broke out, perhaps the most serious clashes. seriousness, in which some 300 soldiers from both sides died and many others were wounded.

This focus of instability places this small geographical sector at the center of international attention, since world-class players have economic, political, military and religious interests in the two nations in conflict. Such is the case of Turkey, which articulates its presence on the shores of the Caspian Sea with Azerbaijan and where it has a military base.

The Azeri nation, the only one in the world that shares borders with the Russian Federation and the Islamic Republic of Iran, has a

Muslim majority , with almost 96 percent of the 10 million inhabitants, and although of that majority, 85 percent is of *Shiite belief* , which places Tehran in that contest since the vast *Shiite community* is very well in tune with its neighbors to the south, the political leadership has built a strong alliance with Turkey, which beyond historical reasons , ethnic and religious, unites them by the always thorny relationship with Armenia, with a Christian majority, which has never forgotten the sufferings it has suffered at the hands of the *Ottomans* , whose maximum expression was translated into the genocide that extended from 1915 to 1917, in that more than one and a half million Armenians were killed by Turkish troops, a fact that Ankara refuses to recognize as such to this day.

For its part, Azerbaijan has a centuries-old lawsuit with Armenia, over Nagorno-Karabakh (or Upper Karabakh or Mountainous Karabakh), a territory with an Armenian majority, which both nations claimed for themselves and that despite the fact that during the Soviet era that conflict was wintered As soon as both nations proclaimed themselves independent republics in 1991, after the disappearance of the Soviet Union, it emerged with more force, which dragged the two nations of the South Caucasus into constant diplomatic and military confrontations.

Beyond the *Muslim* makeup of Azerbaijan, a major oil and gas producer, it has substantial relations with the United States and Israel, while its leadership, although it has never approached Iran, maintains a balanced relationship with Tehran, which did not prevent it from becoming a *Zionist enclave* . In 2016, the president, Ilham Aliyev , bought some $5 billion worth of military supplies from Israel, including drones, missiles, and ships. Azerbaijan became the third largest market for *Jewish* military exports , while Tel-Aviv is the second largest customer for Azeri oil . In October 2018, its Minister of Defense visited Tel-Aviv, to strengthen "military ties", which resulted in the construction of military installations, including an underground command and control center for Azeri intelligence, in the Azerbaijani capital. . In addition to Israel, it uses this territory to spy on Iranian nuclear facilities using drones that take off from local bases.

The increasingly difficult balance that Baku maintains, in its relationship with Ankara, Washington, Tel-Aviv and Tehran, could be unraveled as the tension between these countries increases, which could leave Azerbaijan in the middle of a conflict that would surpass, very much their own interests.

On the other hand, Armenia, allied with Iran and Russia, is key to Moscow, since, from Azerbaijan, the United States intends to market Azeri oil to Europe using the Baku - Tbilisi -Ceyhan pipeline, so that the countries of the *European Union* stop supplying themselves with Russian oil.

A troubled neighborhood

The South Caucasus has become one of the most tense regions in the world, at this moment as much or more than the Pakistan-India border in Kashmir. Since they play too many elements that can aggravate the situation from one moment to another. Given the military agreements between Azerbaijan and Israel, if the latter decided to attack Iran, their planes would be able to refuel on Azeri territory, instead of having to take to the air and return to Israel. According to notes revealed by the United States *Department of State ,* *President* Aliyev compared his relations with Israel to an iceberg: "nine-tenths are below the surface."

In addition to the fact that if Azerbaijan were attacked by some other power, Turkey would be forced to participate in its defense, since it is a strategic point of the expansionist policy towards the interior of *Islam* , proposed by President Recep Tayyip Erdogan , who in that same address has just set one of its most exquisite pearls, the *Hagia Sophia* , from Istanbul, who after more than eighty years has been converted back into a *mosque* . (See: Turkey: The Sultan in the Cathedral) . The question of the South Caucasus also adds a new focus of controversy between Ankara and Moscow, who are already staring each other in the face in Syria and Libya.

For its part, Tehran-Baku relations are steeped in mistrust as Iran, during the last decade of the 20th century, not only strongly claimed some border issues, but also encouraged the majority *Shiites* , who overthrow the civilian government, to adopt a political model similar to yours. Twenty years after that, the wounds in the Azeri political caste are still open.

In the last two years, the United States has given Baku military aid to increase its sea defenses. In "coincidence" with the important investments that the current North American president in his role as businessman has been making for more than ten years in that country.

For its part, Russia, as in Syria, also has a military base in Armenia, a country clearly hostile to Turkey, with whom they do not have official relations since the genocide, so Yerevan has explicit links with the *Workers' Party. of Kurdistan* (PKK), which has been waging a long and bloody war against Turkey since 1978, seeking the establishment of a Kurdish state.

Turkey, within the framework of the military maneuvers with Azerbaijan, which began last Wednesday the 29th, sent US-made *F-16 combat aircraft* to the Caspian country, in which helicopters also participated, these maneuvers are scheduled to be repeated during August. Since as stated by Erdogan . "Turkey will show no hesitation in opposing any attack on Azerbaijan."

The issue in the region is once again unpredictable, once again putting the Caucasus on a war footing.

Image Source:
https://www.elpais.cr/2020/07/14/azerbaiyan-afirma-haber-destruido-una-Instalacion-militar-y-maquinaria-bellica-de-armenia/
Modified by TRIARIUS

Guadi Calvo
(Argentina) Argentine writer and journalist. International Analyst specialized in Africa, Middle East and Central Asia.

Scan Eagle / Night Eagle Remotely Manned Aircraft in the Colombian Military Forces

By Douglas Hernandez (Colombia)

Remotely Manned Aircraft Night Eagle at F-Air Colombia 2019. Photo from www. Fuerzasmilitares.org

It was in 2006, when the Colombian Air Force received the first Scan Eagles, through the American company INSITU. This program was carried out in coordination with the US Southern Command , which facilitated the training of the first FAC operators. The aircraft measures one meter long by three meters wide, and weighs 19 kilos. Its compact size and low weight make it easy to transport in any kind of vehicle or aircraft, and its handling by a small group of men. Its cost is fully justified by the benefits obtained from its operation. With them there is significant fuel economy, they can fly up to 18 continuous hours, reach great heights, and take very high quality photos and video.

A FAC ART Scan Eagle team is made up of a Mission Commander, an Operator, an Image Analyst, and two Maintenance Technicians.

Currently the Colombian Air Force has more than 50 ART of the Scan Eagle and Night Eagle models, as well as a simulator developed nationally by the High Technology Corporation, CODALTEC, which is called SIMART, an acronym for ART SIMulator.

Given the good results obtained by the Air Force with the use of these aircraft, and with the intention of standardizing the equipment, the Colombian National Navy also acquired a batch of Scan Eagles, which operate from the FS-1500 Light Frigates and from the OPV-80 type patrol boats, but they are also used in coastal or inland operations, in support of the Marine Corps.

The Scan Eagles of the National Navy were shown to the public for the first time at the F-Air 2017 International Aeronautical Fair, knowing that they had been operational since the previous year in anti-narcotics maritime reconnaissance operations. It is worth noting that in the Management Report of the National Navy 2015-2018, it is indicated that the acquired model is the Scan Eagle, and that these teams are called the Naval Air Platform

System for Maritime Surveillance - PAVMA. It is noteworthy that with them intelligence, surveillance and reconnaissance operations have been carried out , with which it has been possible to locate Go -type boats Fast for its subsequent interception on the high seas, has also allowed the National Navy to detect vessels that carry out illegal fishing in Colombian territorial waters. And in support operations for the Marine Corps, they have facilitated the detection of illicit crops and drug laboratories, as well as illegal mining areas and fuel smuggling operations by river. Of course, all of the above has had a negative impact on the finances of the drug-trafficking and terrorist groups that operate in Colombia.

In particular, the use of the ART of the National Navy stands out, its low cost in the consumption of fuels and lubricants.

The National Navy has had the support of the Basic School of Remotely Manned Aircraft (EBART) of the Colombian Air Force, for the training of its crews.

In the magazine Semana (2016), the benefits of the ART of the Colombian Air Force are extolled. It is pointed out that a manned aircraft can have about 8 hours of flight autonomy, while the ART reaches 20 hours with day and night capacity. They also point out that for that year a Black Hawk helicopter could cost between 16 and 24 million dollars, but the most expensive ART of the Colombian Air Force barely costs 9 million dollars (they are probably referring to the Hermes 900). They also point out that "the ARTs are capable of ascending up to 19,000 feet, they allow communication in real time and their operational cost can be 40 percent less than that of a manned aircraft."

According to the same source, by 2016, the Colombian Air Force had more than 200 men and women operating ART systems nationwide. Confirming that each team is made up of five people, including "a mission commander, in charge of interaction with other aircraft and communication with the air traffic service; an operator, who is in control of the aircraft from the ground; an image analyst and two maintenance technicians."

In December 2018, the Basic School of Remotely Manned Aircraft (EBART) of the Colombian Air Force, was certified by the company INSITU, manufacturer of the ART Scan Eagle and Night Eagle in use by the FAC, endorsing the training processes that are carried out there. performed.

EBART has been operating since 2014 in the Air Combat Command No. 3, CACOM 3, in Malambo, department of Atlántico, on the Colombian Caribbean coast. The Director of the INSITU Training School traveled there to carry out the respective certification. It is worth noting that this makes EBART the first certified school of these ART in Latin America.

The Basic School of Remotely Manned Aircraft of the Colombian Air Force is dedicated to the education and training of Scan Eagle / Night Eagle pilots, technicians, flight instructors, and video analysts. At the time of obtaining the certification , more than 900 students from the Colombian Military Forces and the National Police had been trained in its facilities, as well as members of the Armed Forces of other Latin American countries, strengthening ties of cooperation , and strengthening its capacities to maintain public order and the fight against drug trafficking, terrorism, and new threats. In addition, these ARTs can be used for monitoring oil pipelines, preventing natural disasters, detecting and monitoring forest fires, preventing deforestation, and volcano monitoring, among other important applications.

References:
Week (2016). Drones join the ranks of the Air Force. Online resource, available at:
https://www.semana.com/nacion/articulo/militares-comienzan-a-usar-drones-en-operaciones/464063

Douglas Hernandez
(Colombia) Founder and director of the website www. Fuerzasmilitares.org, he works as a journalist specializing in security and defense. He is a contributor to *Air and Space Power Journal* - institutional magazine of the USAF, now called *the US Air Force Professional Magazine, American Continent* -, and of the Brazilian magazine *Segurança & Defesa* . He is a Sociologist and Master in Education from the University of Antioquia (Medellín, Colombia), a PhD student. He has a Diploma in International Relations.

Honduras
TESON (Tenacity)

The Specialized Troops in Jungles and Night Operations (TESON), are an elite body of the Honduran Armed Forces. It was created with the support of instructors from the US Special Forces and Rangers to act in all kinds of extreme conditions and inclement weather.

The TESON trainee needs to complete a training program similar to those given by the US Army to Army Rangers . Emphasis is placed on the ability to continue to operate under extreme physical and mental stress. The training of the first TESONs took place at the Támara parachute base, with the presence of US Army Ranges who arrived from Fort Benning . Advanced training took place near the Nicaraguan border in the La Mosquitia jungle . Jungle warfare and night operations were the main focus of instruction.

After that first group, the TESON Course was institutionalized, having graduated multiple promotions. It currently enjoys national and international recognition as one of the most demanding Special Forces courses in the region.

During the training, a physical and psychological resistance superior to the regular soldier is sought, to withstand all kinds of deprivation, discomfort and inclement in the combat zone, added to this, an unshakable spiritual and moral strength, for 54 days, training at night. and early morning.

Historical review of the TESON course in Honduras

The history of the men who make up the brotherhood of the Specialized Troops in Jungles and Night Operations (TESON) commando soldiers from Honduras is a legend steeped in courage, daring, bravery, resistance, and a great gift of outstanding command. It is a story of men whose prowess in the art of combat has rarely been surpassed, soldiers who make up a special operations unit that is trained to conduct operations behind enemy lines. TESONES are trained specifically for high security situations and as airborne parachute troops and amphibious operations specialists. They are agile and versatile soldiers trained and trained to carry out a series of specific tasks ranging from conventional operations to unconventional operations, they are adapted to operate as asymmetric forces and capable of operating independently, in direct support of any of the conventional military forces or other government elements.

The Training Center for Specialized Troops in Jungles and Night Operations (TESON), was created at the initiative of the chief of the armed forces, Division General Don Policarpo Paz García; Thus, in May 1976, the Second Tactical Airborne Infantry Battalion (II BIAT) was selected as the training center for the Honduran Commandos.

In the decades of the 70's, 80's and mid-90's in the badly remembered cold war when in addition to the problems of underdevelopment , Honduras also had to face the open and clandestine invasions of its territory by armed insurgent groups from the left and right, thereby their sovereignty and territorial integrity was threatened by these neighborhood conflicts. The military high command of that time to cover those border areas decided to conduct surveillance operations and intensive patrolling and for this it was necessary to create special units, thus deciding in 1976 to start the necessary training to re-empower and create elite units such as special forces. inaugurating in the special tactical group on May 21 of that year, the first course of specialized troops in jungles and night operations (TESON), culminating the training 27 new TESONES, 14 officers, 12 classes and 1 soldier who later became instructors of what is now the TESON training center, and in their original units they expanded the intention of the command by creating similar courses for the troops and improving the operational readiness of each one of them, with this a variety of courses were born such as: ATECI, COMMANDS, COUGARS, HUNTERS, DRAGONS, HIGHLANDERS, etc.

The course lasts 58 days, within which it is divided into three phases with a training that involves survival tests in highly extreme conditions simulating regular combat. During the training, physical and psychological resistance superior to that of a regular soldier is sought for withstand all kinds of deprivation, discomfort and inclement in the combat zone added to it an unshakable spiritual and moral strength for 58 days training at night and early in the morning.

- **First phase or basic phase:** The first phase lasts 18 days in which physically demanding activities are carried out, such as crossing obstacle courses, self-defense classes, and basic classes for a professional soldier.
- **Second phase or mountain phase:** The second phase lasts 20 days. In this phase, all the classes taught and seen in the classrooms of the training center are taken to the field, and at the same time, tasks are carried out in urban environments and aquatic.
- **Third phase or jungle phase:** The third and last phase has a duration of 20 days which is carried out entirely in the northern part of the country since it is in this sector that the most favorable terrain is found for the practice of the classes of jungle survival.

The TESON course begins its training in the Second Airborne Infantry Battalion, but uses different scenarios of the national territory that provide an adverse environment.

As winners of Fuerzas Comando

At the end of the course, they travel by air conducting an insertion operation, by parachuting, making use of the drop zone in Támara and taking control of a key terrain dominated by illicit association or drug trafficking groups.

With this last exercise, the new promotion of tesons will culminate, making clear the high operational readiness of the Army through its elite unit of TESONES, capable of developing operations and achieving the desired success with a conscientious, committed and reliable unit of this force under the Secretary of National Defense. There are more than 30 graduated promotions under the motto "After TESON nothing".

Sources:
https://sedena.gob.hn/2017/07/03/adiestramiento-extremo-reciben-en-curso-teson/
https://histriadeteson.blogspot.com/2018/

TRIARIUS

Por un mundo más seguro, estable y en paz