ISSN: 2538-9610 (on line)

TRIARIUS

Volume 2 - Issue 34

August 1, 2018

FRANCE

2538-9610

Prevention and Security Bulletin on
Terrorism and the New Threats

TRIARIUS

ISSN: 2538-9610 (Online)
Medellin Colombia
Volume 2 - Issue 34
August 1, 2018

Editor
Douglas Hernandez

Triarius Analysts
Ulises Kandiko León, Francisco Javier Blasco, Haylyn Hernández, Alfredo Campos, Douglas Hernández,

This newsletter is a publication of the International Observatory on Terrorism and New Threats. It is produced fortnightly, in pdf format, and its distribution is free.

Contact information:

Douglas Hernandez
Medellin Colombia
Mobile: (+57) 321-6435103
director@fuerzasmilitares.org
hernandez.douglas@hotmail.com

Editorial

We are pleased to announce that we have signed cooperation agreements with three organizations in our area are strategic. They are the Security College US (SCUS) of the United States, the Master Security Consulting (MSC) of Colombia, and the Learning Institute for Security Advisor (LISA) of Spain, all dedicated to advising on security issues and especially the training of human talent with the highest standards. We invite our readers to know and enroll in any of the programs offered and will certainly contribute to their professional development. Under such agreements, Triarius subscribers will receive special discounts. We are contributing in different ways to global security.

In this issue we bring you an interesting article Kandikó, who from Argentina delves into the issue of ciberamas, taking into account some basic premises. First, that cyberwar is a reality, second, that the technological advantage of power, if war becomes a vulnerability because of the ciberdependencia (a concept that was first played in this magazine), and thirdly that cyber weapons are low cost and high impact. Our expert in the fifth domain of warfare, makes a practical exercise to determine whether a country should develop cyber weapons, using the example of New Zealand. From this example each can develop a similar exercise for their own country.

A step followed Colonel Blasco from Spain, it takes a very precise analysis of the recent rapprochement between the US and North Korea, giving us light on the geopolitical implications of this process for other complex and full of uncertainty. Then Haylyn Hernandez, a Colombian analyst, reviewed the situation in the city of Medellin, presenting the stark contrast presented in this city full of urban innovations, but also so violent. It is very striking an appointment that is done there and says that cities are becoming more important than the States.

The Spanish analyst Alfredo Campos, leads us to revise the complex situation in the Central African Republic, a country convulsed by violent events of various kinds and intensity, and where the powers and some international organizations are present trying to stabilize the situation, and in many cases get some profit. Amid all this, ¼ of the population has fled, which realizes the magnitude of the problem.

Another article Kandikó, the Cyber Intelligence (CYBINT) focuses, in this work the analyst addresses the similarities and differences between traditional intelligence and one that develops or should be developed in cyberspace, according to their particularities. In this approach the problem the viability of traditional intelligence cycle in the fifth domain is questioned, and one of the alternatives to it is shown.

Finally, in the interest of contributing to the strengthening of managerial skills of directors or commanders of military or police units, an article that addresses the issue of strategic management of intellectual capital it is presented, and presents some tools that could be taken into account for this purpose.

Cognize to beat!

Douglas Hernandez
Editor

This newsletter has an English version.

Triarius 34 Content:

Triarius

We want to establish that are within the "new threats" we face in modern times, environmental problems. Care nature is critical to the survival of our species. It's not a fad, it's not even an option, now is some life or death. In this vein, we include in this magazine articles that address environmental problems and propose solution strategies. We invite our readers to make contributions in this regard.

Headlines, members of 13 Regiment of Dragoons Parachutists French Army. Please see the review of this unit at the end of the magazine.

Triarius favors freedom of expression, however, the responsibility for what is said in the articles, it is exclusive to their authors.

special international analysts that free us have submitted articles for this issue thanks.

Cyber weapons: military and diplomatic power to emerging countries and small states

Ulises Leon Kandiko (Argentina)

The issue of cyberwar is still a topic of interest in recent years, especially in developed countries. not less than the issue of cyber weapons also, and parallel to the large number of cyber attacks that have taken place, appears. While Cyberwar theme seems more developed countries, issues relating to the acquisition of cyber weapons by small States have received little attention. While they are individually weak, small states are numerous. Comprising more than half of the members of the United Nations and remain important for geopolitical considerations. Hand of it, these states are facing elections security investment increasingly difficult as the balance between global security, regional dominance and national interests is constantly evaluated, a clear example occurs in the poorest countries, where even Homeland Security issues are mixed with the resources of National Defense. An increasingly important factor in this election is the rising costs of military platforms and perceptions cyberwarfare can provide a cheap and effective strategic offensive capability to exert influence on the geopolitical rivals. Recall at this point, many analysts said the real concern Trump at the summit with Kim Jong-un was Cybernetics more than the nuclear program of North Korea threat. where even Homeland Security issues are mixed with the resources of National Defense. An increasingly important factor in this election is the rising costs of military platforms and perceptions cyberwarfare can provide a cheap and effective strategic offensive capability to exert influence on the geopolitical rivals. Recall at this point, many analysts said the real concern Trump at the summit with Kim Jong-un was Cybernetics more than the nuclear program of North Korea threat. where even Homeland Security issues are mixed with the resources of National Defense. An increasingly important factor in this election is the rising costs of military platforms and perceptions cyberwarfare can provide a cheap and effective strategic offensive capability to exert influence on the geopolitical rivals. Recall at this point, many analysts said the real concern Trump at the summit with Kim Jong-un was Cybernetics more than the nuclear program of North Korea threat. An increasingly important factor in this election is the rising costs of military platforms and perceptions cyberwarfare can provide a cheap and effective strategic offensive capability to exert influence on the geopolitical rivals. Recall at this point, many analysts said the real concern Trump at the summit with Kim Jong-un was Cybernetics more than the nuclear program of North Korea threat. An increasingly important factor in this election is the rising costs of military platforms and perceptions cyberwarfare can provide a cheap and effective strategic offensive capability to exert influence on the geopolitical rivals. Recall at this point, many analysts said the real concern Trump at the summit with Kim Jong-un was Cybernetics more than the nuclear program of North Korea threat.

While the offensive and defensive operations have their own characteristics, currently 5th domain can say that the balance of power between the offense and the defense has not yet been determined. In addition, indirect and intangible nature of cyber weapons estimate does not alter the fundamental principles of war and military conflicts can not win without help. On the contrary, it is likely that cyber weapons are more effective when used as a force multiplier and not just as a breaking capacity of the infrastructure. Consideration of the ciberdependencia, ie the extent to which the economy, the military and the government of a state dependent on cyberspace, is also very relevant to this discussion. Depending on the resilience of infrastructure, a strategic technological advantage can become a significant disadvantage in times of conflict. The ability to amplify conventional military capabilities, exploit vulnerabilities in the national infrastructure and control cyber space is, therefore, an important aspect for any warrior doctrine. The integration of these capabilities in defense strategies is the driving force in research and development of cyber weapons.

The nature of cyberwarfare

Cyberwar is increasingly recognized as the 5th domain of war. Its growing importance is suggested by their prominence in the national strategy, military doctrine and significant investment in relevant skills. Cyberwar criticism of features can be summarized in three points [i]:

1. Cyberwarfare involves actions that have a political or military effect.
2. It involves the use of cyberspace to offer direct kinetic effects or cascade having comparable to traditional military capabilities results.
3. Creates results that cause or are a crucial component of a serious threat to the security of a nation or carried out in response to the threat threat.

As for the cyber weapons, they are defined as the capabilities of the armed Cyberwar with those who have experience and resources needed to deliver and implement them.

In this emerging domain everything is possible to debate, however, many specialists consider offensive operations as dominant in the 5th Domain [ii]. Attacks can be launched instantly, and there is rapid growth in the number of networks and assets that require protection. After all, cyberspace is a target-rich environment based on network structures that favor access to safety. Considerable technical and legal difficulties as well as precise and proportionate retaliation, make accurate attribution of cyberattacks is a tense process. There is also the low cost of creating cyber weapons-the code is cheap- any weapon and released on the Internet can be modified to create the basis for new offensive capabilities [iii]. All this means that the battle space is open,

However, strategies that rely too much on the offensive dominance in the Cyberwar may be premature. For example, cybernetics dependence (critical infrastructure) is crucial to the strategic advantages that cyber weapons can provide. Uncertainty ruled that the dual-use nature of cyber weapons allows them to be captured, manipulated and placed against their creators. Equally important is the practice of "domain escalation" [iv]. As shown by an American policy still unproven, retaliation by the cyberattack can be applied by most destructive military capabilities [v]. And although the speed of a cyber attack can be almost instantaneous, preparing for sophisticated cyberattacks it is considerable. Stuxnet attack required resources to provide a technologically sophisticated espionage expansive state, industrial testing and clandestine delivery were so vital to their success. This shows that the true cost of advanced cyber weapons is not in its creation but in its targeting and deployment, reducing their ability to face future redistribution unforeseen threats.

One of the limitations that budding is being corrected, is given by its lack of physicality (concrete physical effect), although we see as Triton are changing that. As pieces of computer code, generate military effect only by exploiting vulnerabilities created by dependence on cyberspace. They can attack vulnerable infrastructure platforms and manipulating computer systems or acting as a force multiplier to traditional military assets. This can lead to disruption and control of the battle space, as well as providing additional intelligence when payloads are deployed. However, these effects are always side: cyber weapons per se still can not directly affect the battlefield without a device to act,

Ultimately, the debate about the balance of power in the Cyberwar and the relative power of cyber weapons will be decided by empirical evidence related to two factors:

The amount of damage caused by the commitment of cyber-dependent platforms.

To what extent major infrastructure disruptions erode the strength of political will and are exploitable by conventional military capabilities.

At the moment, there is a belief that conflicts not only win in cyberspace and that this applies both to small States and the great powers.

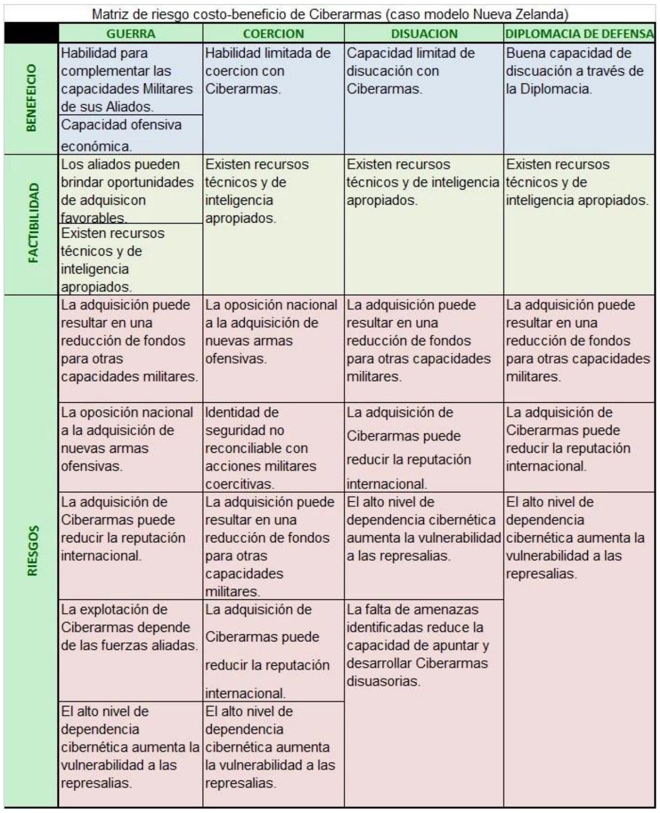
Use of cyber weapons by Emerging Countries and / or small states

To be worthy of investment, an arsenal of cyber weapons states must provide a political or military advantage over (or at least parity) their opponents. To judge whether a small state enough to justify its acquisition benefits, we must understand how you can use these capabilities. A non-exhaustive list of possible uses of cyber weapons including war, coercion, deterrence and defense diplomacy. His most prominent effect is likely to be altered and / or handling of military capabilities command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) and degradation of civilian support networks. Attacks on civilian infrastructure remain the most feasible, and automatic and attacks on military platforms are possible increasingly likely. The effective use of cyber weapons as a coercive tool is limited by the relative size and cyber dependence on an opponent and carries the risk that weapons act unexpectedly. Both units are shared when cyber weapons are used as a deterrent. This is due to the peculiar nature of the cyber domain, where both coercion and deterrence are based on the same aggressive forward recognition network of an adversary. Defense diplomacy can act as a deterrent, but it is only effective if the relevant military capabilities are credible and provable. The effective use of cyber weapons as a coercive tool is limited by the relative size and cyber dependence on an opponent and carries the risk that weapons act unexpectedly. Both units are shared when cyber weapons are used as a deterrent. This is due to the peculiar nature of the cyber domain, where both coercion and deterrence are based on the same aggressive forward recognition network of an adversary. Defense diplomacy can act as a deterrent, but it is only effective if the relevant military capabilities are credible and provable. The effective use of cyber weapons as a coercive tool is limited by the relative size and cyber dependence on an opponent and carries the risk that weapons act unexpectedly. Both units are shared when cyber weapons are used as a deterrent. This is due to the peculiar nature of the cyber domain, where both coercion and deterrence are based on the same aggressive forward recognition network of an adversary. Defense diplomacy can act as a deterrent, but it is only effective if the relevant military capabilities are credible and provable. This is due to the peculiar nature of the cyber domain, where both coercion and deterrence are based on the same aggressive forward recognition network of an adversary. Defense diplomacy can act as a deterrent, but it is only effective if the relevant military capabilities are credible and provable. This is due to the peculiar nature of the cyber domain, where both coercion and deterrence are based on the same aggressive forward recognition network of an adversary. Defense diplomacy can act as a deterrent, but it is only effective if the relevant military capabilities are credible and provable.

Possess or not possess cyber weapons, conundrum.

When assessing this situation are many factors to analyze, but here will be analytically evaluating a possible way for this peculiar decision making. Specifically, the proposed model is a basis for a comparative study and comprehensive state by state. It pays its maximum value when analyzed numerous states. This allows possible patterns of proliferation and a clearer picture of the landscape of this emerging threats. The outline of the basic process for analysis is provided in the following table:

Table 1. Risk matrix cost-effectiveness of cyber weapons



Matriz de riesgo costo-beneficio de Ciberarmas (caso modelo Nueva Zelanda)

	GUERRA	COERCION	DISUACION	DIPLOMACIA DE DEFENSA
BENEFEICIO	Habilidad para complementar las capacidades Militares de sus Aliados. Capacidad ofensiva económica.	Habilidad limitada de coercion con Ciberarmas.	Capacidad limitad de disucación con Ciberarmas.	Buena capacidad de discuación a través de la Diplomacia.
FACTIBILIDAD	Los aliados pueden brindar oportunidades de adquisicon favorables. Existen recursos técnicos y de inteligencia apropiados.	Existen recursos técnicos y de inteligencia apropiados.	Existen recursos técnicos y de inteligencia apropiados.	Existen recursos técnicos y de inteligencia apropiados.
RIESGOS	La adquisición puede resultar en una reducción de fondos para otras capacidades militares.	La oposición nacional a la adquisición de nuevas armas ofensivas.	La adquisición puede resultar en una reducción de fondos para otras capacidades militares.	La adquisición puede resultar en una reducción de fondos para otras capacidades militares.
	La oposición nacional a la adquisición de nuevas armas ofensivas.	Identidad de seguridad no reconciliable con acciones militares coercitivas.	La adquisición de Ciberarmas puede reducir la reputación internacional.	La adquisición de Ciberarmas puede reducir la reputación internacional.
	La adquisición de Ciberarmas puede reducir la reputación internacional.	La adquisición puede resultar en una reducción de fondos para otras capacidades militares.	El alto nivel de dependencia cibernética aumenta la vulnerabilidad a las represalias.	El alto nivel de dependencia cibernética aumenta la vulnerabilidad a las represalias.
	La explotación de Ciberarmas depende de las fuerzas aliadas.	La adquisición de Ciberarmas puede reducir la reputación internacional.	La falta de amenazas identificadas reduce la capacidad de apuntar y desarrollar Ciberarmas disuasorias.	
	El alto nivel de dependencia cibernética aumenta la vulnerabilidad a las represalias.	El alto nivel de dependencia cibernética aumenta la vulnerabilidad a las represalias.		

Each step is explained by a statement of purpose and is demonstrated through a case study. The subject of the case study is New Zealand, chosen because of their membership in the Five Eyes intelligence network and that identifies itself and is perceived as a small state. Ideally, every step of the framework is complete a group representing a variety of perspectives of the military, government agencies, and academic specialties.

Step one: Identify the basic characteristics of small states. The purpose is to identify the key characteristics of state within three categories: quantitative, behavioral and identity. It refers to quantitative measurements such as the land area, population and gross domestic product (GDP). Behavior refers to qualitative metrics on the behavior of a state, both nationally and within the international system. Identity refers to qualitative metrics that focus on how a state perceives its own identity. This article proposes that the metrics for each category may be freely used by properly informed analysts to assign a category resizable to any particular state. Instead, the definition and categorization are achieved by holding a sufficient number of overlapping features-some quantitative, some behavioral and other identity-based. Quantitatively, New Zealand has a small population (approximately 4.5 million), a small GDP (approximately $ s 197 billion), and a small area of land [vi]. It is geographically isolated, without borders with other countries. In the field of behavioral, New Zealand pursues a foreign policy focused on multilateral institutions. He is a founding member of the United Nations and was elected member of the Security Council for the period 2015-2016 after run on a platform of defending other small states. He participates in multiple alliances and has a special interest in the safety of the South Pacific [vii]. With respect to identity, self-identity of New Zealand emphasizes the values of equality, independence, non-aggression, cooperation and recognition of its status as a small state [viii]. Your security identity is driven by the lack of a perceived threat that allows New Zealand make security decisions based on principles and not on practicality [ix]. This was demonstrated by the ban on nuclear ships and nuclear weapons in New Zealand waters, and their subsequent exclusion of aspects of the informal Security Treaty Australia, New Zealand and the United States. However, despite the lower security, domestic opinion strongly supported the antinuclear policy,

Step Two: Identify the availability of resources and alignment of policies for the development, deployment and use of cyber weapons. The goal is to identify how the use of cyber weapons would align with current security policies and defense; If the state has the military capacity to exploit vulnerabilities caused by the deployment of cyber weapons, and in turn has the intelligence and technical resources needed to attack, develop and deploy cyber weapons.

Key documents in defense of New Zealand, references to the cyber domain mainly mention the defense against cyber attacks, with only two references to the application of military force to cyberspace. the acquisition of cyber weapons is not mentioned. Defense policy New Zealand has focused on military contributions to a safe New Zealand, an international order based on rules and a strong global economy. Because the probability of direct threats against the country and its closest allies is low, it has focused on peacekeeping, disaster relief, affordability and maritime patrol. New Zealand's army is small (11,500 troops, including reservists) with limited offensive capabilities and underfunding (only 1.1% of GDP). In consecuense,

New Zealand is a member of the Five Eyes intelligence network and, therefore, can access more sophisticated than most small states intelligence. This can be used to increase its ability to attack and deploy cyber weapons. It has a modern signal intelligence capability, hosted by the Communications Security Bureau Civil Government, which also has the responsibility of national cybersecurity. It is very likely to have the technical capacity to adapt existing cyber weapons or develop new ones, especially if you have the help of its allies. However, due to fiscal constraints, any additional funding for cyber weapons will probably come from the existing defense budget and, therefore, result in compromises with other capabilities [x].

Step Three: examine cyber dependence of small states. The purpose is to examine the dependence on cyberspace for their military capabilities and critical infrastructure, as well as its dependence on cybersecurity when compared with potential geopolitical adversaries.

New Zealand has a cyber dependence moderate to high, and the government, the business sector and civil society are increasingly dependent on services and online platforms. This dependence will increase. For example, the acquisition of new skills C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) to increase military adoption of principles of war centered networks would create new vulnerabilities. The ciberdependencia New Zealand is increased further by the limited experience in cybersecurity. No obvious military opponents, so their relative level of ciberdependencia is difficult to calculate.

Step four: analyze the behavior of the State against security models of competition. The purpose is to analyze how the State's conduct aligns with each model of competitor security and how the acquisition and use of cyber weapons can support or detract from this behavior. Cyber weapons stockpiles are used to achieve political and military objectives. These objectives depend on the behavior and identity of a State, which are difficult to quantify. However, it is possible degree of quantization using conceptual models security. A synthesis of recent scholarship safety in small states generates four models: the first focused on alliances, the second in international cooperation and the third and fourth identity, differentiated by competitive approaches (collaboration and influence, and defensive autonomy) [xi]. Alliances centered model presents small states with persuasive reasons to acquire cyber weapons. This applies both to balance the behavior (ie join an alliance against a State threatening) and drag effect (ie, enter an alliance with a state threatening) [xii]. Additional military resources provided by an alliance have greater opportunities to exploit vulnerabilities caused by cyber weapons. Cyber weapons can be reasonably profitable contribution to an alliance; a great power could even provide opportunities for preferential procurement for a favored ally. Alliances centered model presents small states with persuasive reasons to acquire cyber weapons. This applies both to balance the behavior (ie join an alliance against a State threatening) and drag effect (ie, enter an alliance with a state threatening) [xii]. Additional military resources provided by an alliance have greater opportunities to exploit vulnerabilities caused by cyber weapons. Cyber weapons can be reasonably profitable contribution to an alliance; a great power could even provide opportunities for preferential procurement for a favored ally. Alliances centered model presents small states with persuasive reasons to acquire cyber weapons. This applies both to balance the behavior (ie join an alliance against a State threatening) and drag effect (ie, enter an alliance with a state threatening) [xii]. Additional military resources provided by an alliance have greater opportunities to exploit vulnerabilities caused by cyber weapons. Cyber weapons can be reasonably profitable contribution to an alliance; a great power could even provide opportunities for preferential procurement for a favored ally. join an alliance against a State threatening) and drag effect (ie, enter an alliance with a state threatening) [xii]. Additional military resources provided by an alliance have greater opportunities to exploit vulnerabilities caused by cyber weapons. Cyber weapons can be reasonably profitable contribution to an alliance; a great power could even provide opportunities for preferential procurement for a favored ally. join an alliance against a State threatening) and drag effect (ie, enter an alliance with a state threatening) [xii]. Additional military resources provided by an alliance have greater opportunities to exploit vulnerabilities caused by cyber weapons. Cyber weapons can be reasonably profitable contribution to an alliance; a great power could even provide opportunities for preferential procurement for a favored ally. Cyber weapons can be reasonably profitable contribution to an alliance; a great power could even provide opportunities for preferential procurement for a favored ally. Cyber weapons can be reasonably profitable contribution to an alliance; a great power could even provide opportunities for preferential procurement for a favored ally.

New Zealand has a close military alliance with Australia and is a member of the Five Power Defense Arrangements. It has also signed agreements with the Organization cybersecurity North Atlantic Treaty and the United Kingdom. Previous alliances have focused on security and mutual defense rather than offensive capabilities. New Zealand, however, has a policy to complement Australia's defense capabilities. This could be achieved through the acquisition of cyber weapons, provided it is closely coordinated and integrated with the Australian Army. Therefore, this model evaluates the alignment of state behavior as medium / high and support of cyber weapons as medium / high.

The model of international cooperation means that small states can influence strengthening international organizations, promoting cooperative approaches to security and creating laws and regulations to restrict the powerful states. Small States acting under this model will favor methods diplomatic and ideological influence. As such, it is less likely to acquire cyber weapons. Instead, it is more likely to try to regulate cyber weapons similar to restrictions on biological and chemical weapons or lead efforts to explicitly incorporate them into the way international laws of war.

New Zealand generally has a multilateral approach to foreign policy and is a member of many international organizations. It has a long history of advocacy of disarmament and arms control, which conflicts with the acquisition of new categories of offensive weapons. This model evaluates the alignment of state behavior as high and support of cyber weapons as low.

Both models focused on identity (collaboration and influence versus defensive autonomy) focus on the analysis of the "security identity" of a small state. This develops from perceptions of "past behavior, images and myths linked to it have been internalized for long periods of time by the political elite and the population of the state" [xiii]. This identity can be based on a number of disparate factors such as ongoing security threats, perceptions of national character and historical consciousness. The security identity of a State may lead to a preference for any of the security models focused on the identity mentioned above. Regarding collaboration and influence, New Zealand identity achieves a balance between practicality and principle. It strives to be a moral and impartial state that promotes what it considers important values such as human rights and the rule of law [xiv]. However, we still want to work in a constructive way that allows practical solutions to difficult problems. The acquisition of cyber weapons is unlikely to advance in this model. Therefore, this model evaluates the alignment of state behavior as a means and supporting cyber weapons as low. If you want to work in a constructive way that allows practical solutions to difficult problems. The acquisition of cyber weapons is unlikely to advance in this model. Therefore, this model evaluates the alignment of state behavior as a means and supporting cyber weapons as low. If you want to work in a constructive way that allows practical solutions to difficult problems. The acquisition of cyber weapons is unlikely to advance in this model. Therefore, this model evaluates the alignment of state behavior as a means and supporting cyber weapons as low.

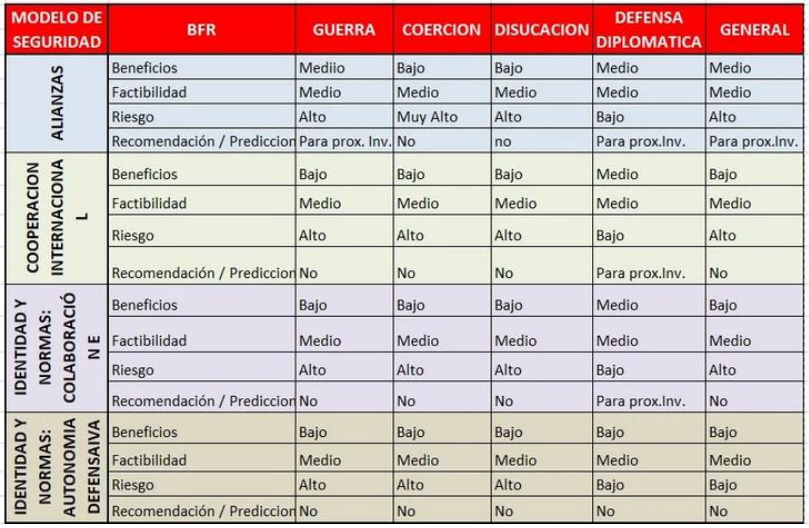
Despite its multilateral behavior, New Zealand retains some defensive autonomy and is proud to maintain independent views on major issues. Isolation and the absence of major threats have allowed him to retain some autonomy in its defense policy and maintain a small army. His independent and pacifist nature suggests that the acquisition of cyber weapons could be controversial. Therefore, this model assesses behavioral alignment state as a means and cyber weapons as support for low / medium.

Step Five: Analyze the benefits, feasibility and risk for each category of use of cyber weapons. The goal is to first identify the benefits, feasibility and risk of acquiring cyber weapons depending on each category of potential use, as shown in Table 1. Then, this information is analyzed based on the use of cyber weapons for different models security. as shown in Table 2. This results in a classification of benefits, viability and risk of each combination of use of cyber weapons and security model small state. This is followed by a general recommendation or prediction for the acquisition of cyber weapons under each security model and category of use of cyber weapons.

Step Six: recommend or predict cyber weapons acquisition strategy. The aim is to summarize the key findings, recommend whether a small state must acquire cyber weapons and predict the likelihood of such an acquisition. Key findings for the case that was used as a model are that it is unlikely that New Zealand get significant benefits from the acquisition of cyber weapons. This is due to their limited military capabilities, their foreign multilateral approach, broad participation in international organizations and pacifist identity security. Factors that could change this assessment and increase the benefits of the acquisition of cyber weapons include a greater focus on military alliances, the emergence of more obvious threats to New Zealand or their close allies, or changing security identity.

The product that delivers this matrix has considerable usefulness as a tool for decision support. When used by a small state as an input in the process of making strategic decisions, the outcome can be incorporated into the relevant defense capacity and policy documents. If the purchase is recommended cyber weapons, the result could be used to inform strategic, doctrinal and specific planning documents. It also provides a basis for potential cyber weapons capabilities under a standard acquisition model are analyzed.

Table 2. Matrix acquisition of cyber weapons



MODELO DE SEGURIDAD	BFR	GUERRA	COERCION	DISUCACION	DEFENSA DIPLOMATICA	GENERAL
ALIANZAS	Beneficios	Mediio	Bajo	Bajo	Medio	Medio
	Factibilidad	Medio	Medio	Medio	Medio	Medio
	Riesgo	Alto	Muy Alto	Alto	Bajo	Alto
	Recomendación / Prediccion	Para prox. Inv.	No	no	Para prox.Inv.	Para prox.Inv.
COOPERACION INTERNACIONA L	Beneficios	Bajo	Bajo	Bajo	Medio	Bajo
	Factibilidad	Medio	Medio	Medio	Medio	Medio
	Riesgo	Alto	Alto	Alto	Bajo	Alto
	Recomendación / Prediccion	No	No	No	Para prox.Inv.	No
IDENTIDAD Y NORMAS: COLABORACIÓ N E	Beneficios	Bajo	Bajo	Bajo	Medio	Bajo
	Factibilidad	Medio	Medio	Medio	Medio	Medio
	Riesgo	Alto	Alto	Alto	Bajo	Alto
	Recomendación / Prediccion	No	No	No	Para prox.Inv.	No
IDENTIDAD Y NORMAS: AUTONOMIA DEFENSAIVA	Beneficios	Bajo	Bajo	Bajo	Bajo	Bajo
	Factibilidad	Medio	Medio	Medio	Medio	Medio
	Riesgo	Alto	Alto	Alto	Bajo	Bajo
	Recomendación / Prediccion	No	No	No	No	No

Alternatively, the matrix allows a variety of actors determine the probability of acquisition of cyberweapons by small States, it could be used as a tool to develop predictive intelligence. Furthermore, when the matrix is used in a sufficient number of small states, it could be used as a base for broader predictions regarding cyberweapons proliferation. This would be particularly effective in geographic areas with a high concentration of small states. For the most powerful states, this could indicate opportunities for further cooperation cyberwar with geopolitical allies, perhaps even spreading to the sale of weapons or defense diplomacy. Conversely, the matrix could provide non-governmental organizations and academic opportunities to track the proliferation of cyber weapons and increase the visibility of the phenomenon among international organizations, policy makers and the general public. These results provide significant benefits to the broad spectrum of actors seeking stability and influence in the international order.

1D34S F1N4L3S

The evolution of the battlefields and their domains are not given in simple and immediate to industrial or technological developments form, before the appearance of each domain the preceding refused to give way. Virtue is to learn from the past, I said the old Niccolo Machiavelli "Anyone who wants to know what will happen, you should examine what happened, all the things of this world, at any time, have their counterpart in antiquity" deny the existence of the 5th domain of war, the use of cyber weapons as they will have physical effect is not recognizing what will happen soon. Recently, Donald Trump USA President ordered the Pentagon to take the initiative in creating the 6th Branch of the US Armed Forces, namely the Space Force, will brand him an adventurer, The model exhibited here also has a potential for significant prediction: any ability to forecast the acquisition of cyber weapons state by state and thus monitor the proliferation of these would be a great geopolitical benefit. In addition, the great Powers should not ignore the strategic impact that small states could have in this area. It is also true and valid recall in that regard to small states, their geopolitical rivals can deploy cyber weapons as a means to promote national interests in this sphere of influence.

Cyberspace is made by man, it is a highly evolving environment, technologically configured and not quite tangible, which requires to be studied, evaluated, analyzed and subjected to continuous research to master this new domain you will have to travel many miles or terabytes to achieve this, there's no doubt. This domain 5th understanding goes beyond the technological aspects and requires the integration of capabilities and cybernetic strategies in existing defense doctrines. Exposed part here is just a glance, is not intended as a guide only give ideas to assist in this process from the strategic decision to obtaining and doctrinal and operational integration.

References and notes

[I] Raymond C. Parks and David P. Duggan, "Principles of cyberwarfare," IEEE Security and Privacy Magazine 9, no. 5 (September / October 2011), 30; Andrew M. Colarik and Lech J. Janczewski, "Development of a strategy for cyberwar" seventh international conference on security and information assurance, December 2011, 52; Shakarian, Shakarian and Ruef.

[Ii] Fred Schrier, Document No. 7 on cyberwarfare, democratic control of the armed forces at work (Geneva: Geneva Center for the Democratic Control of Armed Forces, 2015), available at <www.dcaf.ch/content /download/67316/.../ OnCyber warfare-Schreier.pdf>; John Arquilla, "Twenty years of cyberwarfare," Journal of Military Ethics 12, no. 1 (17 April 2013), 80-87.

[Iii] PW Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Should Know (Oxford: Oxford University Press, 2014).

[Iv] Thomas G. Mahnken, "Cyberwar and Cyber Warfare" in America's Cyber Future, ed. Kristin M. Lord and Travis Sharp (Washington, DC: Center for a New American Security, 2011), available at <www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf>.

[V] Department of Defense (DOD), The DOD Cyber Strategy (Washington, DC: DOD, April 2015), available at <www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf >.

[Vi] Statistics New Zealand, "Key Index Statistics New Zealand", available at <www.stats.govt.nz/browse_for_stats/snapshots-ofnz/index-key-statistics.aspx#>.

[Vii] The Ministry of Foreign Affairs and Trade of New Zealand, "Foreign Affairs", March 2014, is available at <http://mfat.govt.nz/Foreign-Relations/index.php>.

[Viii] Ibid.

[Ix] Doctrine of the Defense Force of New Zealand, 3rd ed. (Wellington-based Defense Force New Zealand, June 2012), available at <www.nzdf.mil.nz/downloads/pdf/public-docs/2012/nzddp_d_3rd_ed.pdf>.

[X] Defense White Paper 2010 (Wellington: Ministry of Defense, November 2010), available at <www.nzdf.mil.nz/downloads/pdf/public-docs/2010/defence_white_paper_2010.pdf>.

[Xi] Joe Burton, "small states and cyber security: the case of New Zealand," Political Science 65, no. 2 (2013), 216-238; Paul Sutton, "The concept of small states in the international political economy", The Round Table 100, no. 413 (2011), 141-153.

[Xii] Joe Burton, "small states and cyber security: the case of New Zealand," Political Science 65, no. 2 (2013), 216-238.

[Xiii] Jean-Marc Rickli, "military policies of small European states after the Cold War: territorial strategies niche strategies" Cambridge Review of International Affairs 21, no. 3 (2008), 307-325.

[Xiv] Jim McLay, "New Zealand and the United Nations: Small State, Big Challenge"
August 27, 2013, available at <http: // nzunsc. govt.nz/docs/Jim-McLay-speech-Small-State-Big%20Challenge-Aug-13.pdf

Image source:
https://www.armytimes.com/resizer/M1idu3KQK7r5YGY2ngP5hurPqis=/1200x0/filters:quality(100)/arc-anglerfish-arc2-prod-mco.s3.amazonaws.com/public/NXP3Q667XZHG3BQ5PZ43GROJQM.jpg

North Korea and the United States "kiss" for the first time

By Francisco Javier Blasco, retired Colonel

I write this work first impressions of the agreements reached at the minimum long-awaited summit between Donald Trump (USA) and Kim Jong-un (Democratic People's Republic of Korea -RPDC- rather known as North Korea -CN) held in the city state of Singapore, under all kinds of precautions, precautions and safety measures to take significant steps toward denuclearization of CN and its integration into the international normality.

Summit, whose celebration has been several times in the limelight and in reference to its duration and apparent results are expected and predicted much and nothing at the same time. And given apparent success in running common policy and geostrategy that the International Community (IC) has rushed-even for point-in advance to the credit of Trump although in reality and like everything in the international arena, has several primary, secondary and many actors whose beneficiaries are several countries if they possibly enjoy them.

I have many official years and particularly trying to thresh, understand and explain how it has been possible to achieve the success of North Korea and weapons of mass destruction with so scarce economic resources, under such pressure and restriction, few or very few technical and natural resources to obtain and production of enriched uranium, its true purpose and ultimate ends thereof. I have written quite a few classified reports to my superiors and much about open source, the last of them on my blog listed chronologically on the subject [1].

In all of them, and with varying intensity and degree of development, have been popping up a number of common points, which are configured properly, make up what some time, I have come to call the strategy CN and its hereditary ruling dynasty. In summary, these critical and secondary points are concentrated on:

- The constant search for personal security guarantee North Korean regime;
- CN achieving respect as a sovereign nation and at the same level of other countries with nuclear weapons;
- Not receive assurances external aggression which implies continuity in its forms and modes of government;
- Full and final denuclearization of the Korean Peninsula as the ultimate goal and guarantee security;
- A large number of significant financial compensation to be determined and very difficult to quantify and officially end.

To achieve these goals has required CN: an iron hand on his population that has been subjected to all kinds of hardship and persecution unprecedented in the modern era; a powerful economic, military and technical support mutual benefits -of a priori and posteriori of China and Russia in some cases; and anxiety blind faith in the success of the program to stop being considered one of the great outcasts of the world; namely tighten and much rope without letting never break and find the right egocentric for that at the height of his exacerbated desire for prominence and complete cult of personality, he was able to skip to torera any protocol, judicious advice and did not take into account the risks of a negotiation that can be dangerous for them and their partners place,

Trump takes months to face, ignoring, abusing and threatening all its neighbors, allies and colleagues or not at all kinds of forums, alliances, treaties, agreements and conventions contained in head or even were the result of American initiatives. Almost none left standing, has broken or ramshackle all molds and has scuppered, decades and decades of efforts and negotiations of his predecessors in office and the imposing and overwhelming diplomatic and commercial machinery USA. He specializes in insulting leave their meetings, hastily and giving a tremendous slam - see last example recently after the G-7 in Canada-.

Since his appointment as US President and leader of the CI has vilified and especially despised Kim-Jong-un all kinds of nicknames, insults and derogatory epithets. He has repeatedly threatened the country with its destruction and sometimes repeated its intention to cancel the summit even few hours before the meeting. As a great strategist and expert dialogue, based yesterday duration and efectivad of it in personal smell and especially in your first impression.

However and despite all this, another egotistical and ruthless leader who not only despises people, but pursues them and makes them disappear for any reason whatsoever, and feels honored for his "beloved people", has resisted and overcome all obstacles and past insults and has not only shaken hands this morning at Trump but has spoken to him much more than expected time and even and beyond all calculation as previously filtered, shared table and tablecloth for several hours with him.

We all know that, because of the great pitfalls and difficulties "language and claims" of both countries to carry out certain production and adequate progress in the same between the respective commissions relationships is not easy, let alone sit their "special" leaders at the same table with a detailed program full of points of draft, properly priced and limited in substance and form and with a limit for application time. in addition, we must not underestimate the mutual distrust between both, While patents and based on no or very limited maintenance, neglect or premature rupture of agreements reached between the two countries recently or pretéritamente reasons.

no sureties for obvious reasons and mainly because Kim understands or should be aware that similar agreements or promises -in which personal survival was guaranteed to other proliferators satraps and weapons of mass destruction and Saddam Hussein or Gaddafi, if those abandoned all practices and programs- not respected long after and dismantle those believe them their respective facilities. Both had to suffer a ruthless persecution own flesh and nothing worthy killings of his "lifelong garantistas" Americans. This on a personal level; because we must not forget the recent denunciation and unilateral abandonment by the US of the agreement on Iran's nuclear program.

Depending on the above and the difficulty and complexity involved in the issue and its derivatives in the agreement and the lack of prior preparation and duration of the Summit, is very normal that has only been able to reach out and make public an undeveloped agreement of minimums that I would call "good intentions" and a bit of smoke pouring sale. Little has been what has been achieved, given the not much published. At this time and as a preliminary report, suffice as detailed as I've found in the Spanish press on the subject [2]. In that article, on your left and box, you can see reflected the four main points made and signed the agreement. a great deal of good will need to play more of what they said.

There are still many outstanding fringes. Fringes, nothing trivial as: the deadlines for their implementation and completion; phases and intermediate steps; end position to be reached; economic, social and technical compensation; degree, authority and integration policies peninsular where appropriate; actions to take with regard to the restoration of respect for human rights in CN; paper and extent of involvement neighboring countries affected, preferably China, Japan and South Korea should adopt; terms and conditions for the lifting of sanctions and restrictions; international and bilateral; level and time for the necessary partial dismantling of the huge North Korean military and the future role concerning the presence, deployment,

Many points, apparently untouched, or simply mentioned without elaborating. A value and importance such that the failure or lack of agreement on many if not all of them can ruin all this paraphernalia in the style of the great empires in the times when the Emperor on duty received with all pageantry, before sending stabbing, her until nothing worrisome threat or terrible enemy.

Today we can all sleep more peaceful, although awake or doze should not be abandoned. Some like CN will be less pressured, at least initially, others like the Chinese see, finally and after almost 70 years as boots and American nuclear weapons away from its borders and that as a result of the tremendous consumption of adrenaline its neighbors and consequently, the potential increase in US military nonchalance in the area, routes, conquests and new deployments by the South China Sea and are now less threatened and be faster.

South Koreans greatly and the Japanese in their share must decide whether to continue his career reset at any cost or, conversely, dedicate their efforts to improve other aspects of their economies.

It remains for me to understand, that's what Trump has won and the US in this paripé hugs and kisses almost. After the dazzling fireworks castle effect -at pure socialist style in Spain leveraging effect with some initial success in desperate situations, but in reality they have never threatened their homeland; will lose presence in the area as quickly and easily translate into less prestigious and most likely sell much less sophisticated weapons in an area that was in it, and which seeks to conquer economic and political Does looking to save and re-focus efforts in the Middle East? Is it just a matter of domestic marketing and external compensatory after a long list of international gaffes and blunders? Or only intended to mislead and is pursuing closer and more Chinese, Russians, Iranians and Indians [3]? Soon we will see, sure.

References

[1] https://sites.google.com/site/articulosfjavierblasco/corea-del-norte-algo-deja-vu
[2] https://elpais.com/internacional/2018/06/12/actualidad/1528766187_744971.html
[3] https://www.efe.com/efe/espana/mundo/china-presume-de-unidad-con-rusia-india-o-iran-frente-a-la-division-del-g7/10001 -3643910

Image source:
https://img.kyodonews.net/english/public/images/posts/710ac39eef20bca3eb59b18a4bd584b5/cropped_image_l.jpg

Medellin reality: between innovation and violence

By Haylyn Andrea Hernández Fernández (Colombia)

Globalization and rapid population growth have been decisive for models that organize the process of urbanization of the XXI century, therefore, the development of cities and their importance in the international arena has been increasing, even going to have a crucial role that goes beyond traditional state-centric conceptions. In this regard, sociologist Saskia Sassen, believes that "the cities are going to be more important than the States" states that there is a kind of geopolitical urbanized, which focuses on vectors or axes. More important than the US in terms of global geopolitics, will be the focus of Washington, New York and Chicago, in the case of China, will be Hong Kong, Shanghai and Beijing, and Turkey Ankara and Istanbul, become more important the country itself(Armada, 2013).

In Colombia, a city that makes the difference for innovation and cutting edge is Medellin. In 2017 the agency Australian innovation 2thinknow recognized Medellin as one of the most innovative cities in the world, the only one in Colombia that has managed to enter this index, this is a sign of the potential of the city, which allows attract investment and talent . Antioquia's capital is in the 'hub', later in the second, after 'Nexus', which is led by London; the cities 'HUB' are challenging territories, innovation activity centers, axes with influence on key economic and social sectors(El Tiempo, 2017).

However, the cosmopolitan metropolis has another side to show safety. Medellin closed 2017 with 577 homicides, 33 more than in 2016, 318 cases were attributed by the authorities to the confrontation between criminal groups(Restrepo 2018). According to hypothesis of the Metropolitan Police and the Mayor, recent violent homicides, which were characterized as cases of people tortured and dumped in plastic bags, due to the capture of Juan Carlos Mesa Vallejo, alias' Tom, or Carlos flat ', one of the most bloodthirsty leaders of the' Envigado office '.

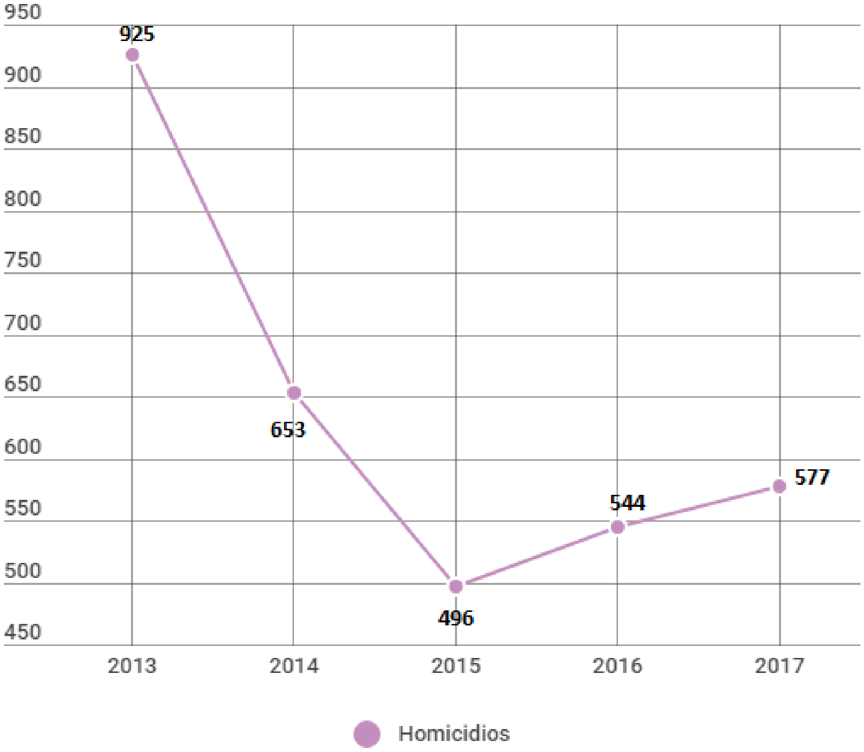


Figure 1. Historical development homicide. Adapted from: Restrepo, V. (2018, January 1). Medellin closed the year with 577 homicides.

According to the latest report of the Citizen Council for Public Safety and Criminal Justice, a Mexican civil organization that annually draws up a list of the 50 most violent cities in the world, Latin America is the region that hosts the largest number of violent cities: 17 are in Brazil, 12 in Mexico, Venezuela 5, 3 and 2 in Honduras Colombia (BBC, 2018). While Medellin presents an increase in the number of homicides in the last two years, for the third consecutive year was out the list of the most violent cities in the world, when for over 15 years topped this list. Colombian cities included in the ranking are Cali, Palmira and Cucuta with positions 28, 37 and 50 respectively.

On the other hand, the Citizen Perception Survey 2017 Medellín Cómo Vamos program, evidence that the perceived safety of citizens decreased by 4 percentage points compared to the previous year, 69% say they feel safe. Among the most serious problems regarding security is headed by drug addiction 33% are mentioned, gangs or combos 25% (led mainly from the Envigado Office and Clan Gulf facing for control organized crime in the city), street robberies 16%, 9% drug trafficking, among others(Medellín Cómo Vamos, 2017).

In this sense, the city of eternal spring presents an ambivalent reality on the one hand, it's a big world leader in urban planning, and on the other, remains the epicenter of crime and violence despite not being on the list of most violent cities in the world.

> The city grows demographically, economically and politically as an example of a successful city, while continuing to establishing itself as an epicenter of crime and violence, reaching figures that have located in the most violent cities in the world due to the development of various criminal activities, ranging from microextorsión to trafficking in drugs, weapons and other own activities of transnational organized crime (Patiño Villa et al., 2015, p. 14).

Carlos Patiño states that, despite being one of the few cities that has committed so many public resources for social development planning and implementation of integral projects, violence and crime persist. The paradox continues: while there are ambitious plans for public policies to combat social problems, crime rates and collective violence are still high(2015, pp. 177-178).

Currently they operate responsible for killings, micro-trafficking, extortion, displacement and other criminal activities that disrupt illegal security structures. According to figures from the Directorate of Criminal Investigation and Interpol for the period from 01 January to 30 April 2018, there have been 180 cases of homicide(National Police of Colombia, 2018)For its part, the Information System for Security and Coexistence -SISC- the Mayor of Medellin, recorded 199 people killed, 39 more than in the same period last year. The trend so far is upward: 9 of the 16 municipalities and two of the 5 districts have increased that statistic(Restrepo 2018).

Precisely the Comuna 13 has been the scene of an ongoing criminal siege shootings, deaths, injuries, burning buses and empty by the actions of criminal organizations schools, which generated an institutional response to the presence of 320 police and military to control situation in Altavista has also been given to safety reinforcement. According to Secretary of Security, Andres Tobon, Comuna 13, Robledo and Altavista are of great interest to criminal organizations because they constitute a strategic corridor for transporting weapons and drugs(El Tiempo, 2018).

In addition to the offensive between combos and criminal groups that territorial control is disputed, this situation has a background and is the confrontation between organizations and local government, this because of the war said Mayor Federico Gutiérrez, against such criminal structures.

In the last accountability of the mayor last March, capturing 10 leaders of criminal organizations Integrated Drug Trafficking -Odin- in 15 months it stood out: alias' Jumbo ',' Soto ',' Camellete ',' Cheese '' Abelito '' Matthew ',' El Chivo ',' Camilito '' Tom 'and' Elkin Triana '(Mayor of Medellin, 2018). Gutiérrez has called these catch as an accomplishment of the city as they were the result of joint action by the police, prosecutor, army and administration.

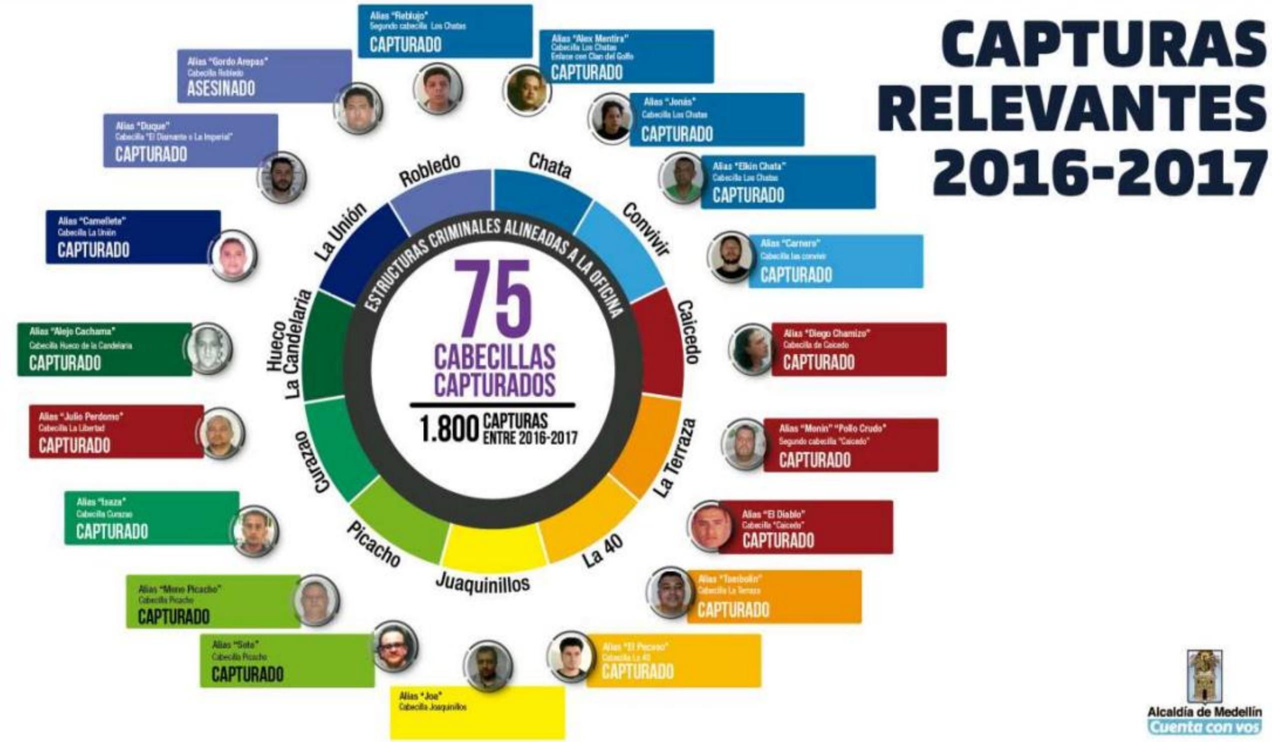

CAPTURAS RELEVANTES 2016-2017
Alias "Rebiujo" Segundo cabecilla Los Chatas CAPTURADO
Alias "Alex Mentira" Cabecilla Los Chatas Enlace con Clan del Golfo CAPTURADO
Alias "Gordo Arepas" Cabecilla Robledo ASESINADO
Alias "Jonás" Cabecilla Los Chatas CAPTURADO
Alias "Duque" Cabecilla "El Diamante y La Imperial" CAPTURADO
Alias "Elkin Chata" Cabecilla Los Chatas CAPTURADO
Alias "Camellete" Cabecilla La Unión CAPTURADO
Alias "Carnero" Cabecilla las convivir CAPTURADO
Alias "Alejo Cachama" Cabecilla Hueco de la Candelaria CAPTURADO
Alias "Diego Chamizo" Cabecilla de Caicedo CAPTURADO
Alias "Julio Perdomo" Cabecilla La Libertad CAPTURADO
Alias "Monin" "Pollo Crudo" Segundo cabecilla "Caicedo" CAPTURADO
Alias "Isaza" Cabecilla Curazao CAPTURADO
Alias "El Diablo" Cabecilla "Caicedo" CAPTURADO
Alias "Mono Picacho" Cabecilla Picacho CAPTURADO
Alias "Tombolín" Cabecilla La Terraza CAPTURADO
Alias "Seto" Cabecilla Picacho CAPTURADO
Alias "El Pecoso" Cabecilla La 40 CAPTURADO
Alias "Joe" Cabecilla Joaquinillos
Robledo
Chata
Convivir
Caicedo
La Terraza
La 40
Juaquinillos
Picacho
Curazao
Hueco La Candelaria
La Unión
ESTRUCTURAS CRIMINALES ALINEADAS A LA OFICINA
75 CABECILLAS CAPTURADOS
1.800 CAPTURAS ENTRE 2016-2017
Alcaldía de Medellín
Cuenta con vos

Figure 2. relevant catches 2016-2017. Adapted from: Medellin's town hall. (2018). 2016-2019 Second annual report. Public Hearing on Accountability.

As a result of the increase in violence, it should also contemplate wear 'Pact rifle' July 2013, which was given as a non-aggression agreement, cooperation in illicit activities and establishment of division of territories the city between the Office of Envigado and Clan Gulf, calling itself the Autodefensas Gaitanistas of Colombia. So the relative stability of criminal structures thanks to the truce, may be coming to an end because catches as they are generating significant gaps of power that are reactivating an urban war that deepens the destabilization of the city.

Still, it seems not enough that the mayor is attributed as a personal combat criminal organizations. The setback suffered by the administration with the then security secretary and confidant, Gustavo Villegas, who was captured in July 2017 for his alleged connection with the Office of Envigado, and conversations between alias Pichi, ringleader Terrace, and Carlos Pesebre Pesebre leader of the organization, who from prison promoting Cómbita would set a plan to destabilize Medellin(Week, 2018)They are proof of the obstacles that have arisen in the management of the mayor, who must stop the crime wave and show strong results to face the challenge imposed by the illegal and criminal organizations.

Officials say recent violent events do not obey the expansion of criminal groups, but a reaction of these because they are desperate to catches of the ringleaders. The Ombudsman's Office also ensures that the phenomenon has generated account changes and reconfiguration of alliances between illegal structures and a dispute between two organizations by the monopoly of illicit economies.

> On one side the illegal group posdesmovilización AUC: AUC Gaitanistas of Colombia, seeks to maintain control over mobility corridors of illegal economies, ensuring the loyalty of local armed groups operating in the territory, through the imposition of foreign managers and intimidation of the civilian population; and other criminal organizations with limited territorial impact, but articulated structures more armed and economic capacity of the so-called Office of Envigado, intended to dispute the control of such mobility corridors.(Ombudsman Colombia, 2018)

At this point it is clear that the dynamics evidence that criminal organizations have the ability to reinvent themselves in order to evade institutional controls, which means for the state to be to the front to prevent strengthening and transcend time.

The situation is complex and not solved only traditional measures of public safety, since the population there is a feeling of uncertainty that calls into question the state's ability to control criminal organizations and the legitimacy of the institutions of security and justice are sometimes co-opted by corruption, must make decisions and implement structural measures covering the entire territory, in order to have a visible parity between innovation and safety.

References

Medellin's town hall. (2018). 2016-2019 Second annual report. Public Hearing on Accountability. Recovered from https://www.medellin.gov.co/irj/go/km/docs/pccdesign/medellin/Temas/PlanDesarrollo/rendicion/Shared%20Content/2018/RENDICION%20DE%20CUENTAS%202017.pdf

Navy, A. (2013). "Cities will be more important than the states." Recovered from http://www.abc.es/20120612/sociedad/abci-ciudades-importantes-estados-201206112005.html

BBC World. (2018, March 7). These are the 50 most violent cities in the world (and 42 are in Latin America). Recovered from http://www.bbc.com/mundo/noticias-america-latina-43318108

Ombudsman Colombia. (2018, April 24). Early alterta Imminence No. 041-18. Recovered from https://verdadabierta.com/wp-content/uploads/2018/04/AT-N%C2%B0-041-18-ANT-Medelli%CC%81n.pdf

Time. (2018, April 30). Violence persists in Robledo, second commune more killings. Retrieved May 24, 2018, from http://www.eltiempo.com/colombia/medellin/persiste-la-violencia-en-robledo-segunda-comuna-con-mas-homicidios-211808

Time. (2017, February 28). Medellin receives new recognition as an innovative city. Time. Recovered from http://www.eltiempo.com/colombia/medellin/medellin-recibe-nuevo-reconocimiento-como-ciudad-innovadora-62420

Medellín Cómo Vamos. (2017, November 1). Presentation: Public perception Survey, 2017. Recovered Medellin May 24, 2018, from https://www.medellincomovamos.org/download/presentacion-encuesta-de-percepcion-ciudadana-medellin-2017/

Patiño Villa, CA, Zambrano Pantoja, FR, Montenegro Lizarralde, F., Viviescas Monsalve, JF Gonzalez Borrero, JI, Montoya Pino, AP, ... Romero Quiñones, MC (2015). Medellin: territory, conflict and state. Urban geostrategic analysis. Bogotá, Colombia: Editorial Planeta SA Colombina

Colombia National Police. (2018). Recovered 2018. Homicides May 24, 2018, from https://www.policia.gov.co/observatorio/estudio_criminologia

Restrepo, V. (2018, May 3). How he has gone to the mayor of Medellin with security? Retrieved May 24, 2018, from http://www.elcolombiano.com/antioquia/seguridad/seguridad-en-medellin-balance-del-alcalde-EX8642789

Restrepo, V. (2018, January 1). Medellin closed the year with 577 homicides. Retrieved May 23, 2018, from http://www.elcolombiano.com/antioquia/seguridad/homicidios-en-medellin-durante-2017-FD7948557

Week. (2018, April 27). Under the criminal siege, what is happening in Medellin? Retrieved May 24, 2018, from https://www.semana.com/nacion/articulo/crisis-criminal-en-medellin-y-la-comuna-13/565134

AIG

American Intelligence Group

In the Kingdom of the Warlords

By Alfredo Campos (Spain)

"Abandon all hope who enter!"
(From Hell Canto III, Judgment 7-9, Divine Comedy, Dante Alighieri)

In the heart of the continent, Africa has a wound that is bleeding for more than 5 years, and that wound is called Central African Republic. The precarious security situation in the fledgling nation favors permanent instability, which is a major challenge facing any initiative that seeks to consolidate state structures beyond the capital Bangui and for their own economic development. But the Central African conflict also constitutes a bad regional endemic: the central geographical position of the Republic, which shares borders with countries facing serious security problems: Chad, Sudan, South Sudan, Democratic Republic of Congo and Cameroon; They make it a strategic territory for the region, key fighters and mercenaries corridor.

The Central African Republic has the dubious honor of starting the fastest "hell" descent to become the poorest country in the world, it is certainly one of the most unstable at the mercy of countless warlords who have made the conflict permanent and lucrative criminal activity their way of life. Criminal groups roam freely, bands that have developed in the heat of predation successive political elites and an almost total absence of the state apparatus in most of the country. Leaders of armed groups in order to legitimize their actions have fueled an artificial religious conflict between Christians and Muslims, and disputes between communities who even ethnic cleansing. Meanwhile,

From the humanitarian point of view, this situation creates an unprecedented catastrophe at the end of 2017 had already led to the flight of 1.1 million people; a quarter of the total population. The crisis threatens to spread throughout the region and become chronic over time. With this article I try to unravel the keys of such a complex and dynamic, unpredictable conflict.

Historical background

The territory occupied by the current Central African Republic historically housed the slave Sultanate of Dar al-Kuti already in the nineteenth century was replaced by French domination. The new colonial administrators favored some ethnic groups over others: as with the coastal communities south as Ngbaka (Mbaka), the Yakoma and Ubangi, from which formed the ruling elites in the country, to the detriment of other communities north who have felt discriminated against since.

Central African Republic, known as Ubangi-Shari during colonization, gained independence from the

French metropolis in 1960. However, it has never ceased to remain in the orbit of the diffuse space of the African continent special geostrategic interest to the Gallic country called Françafrique . The country is in a key position on the continent and extending along two dividing lines on the continent: one that separates the Arab world with African and other delimiting zones spread of Christianity and other Animist religions Islam. If we draw an imaginary line between territories majority population of these religions mentioned, would follow a route from West Africa through Nigeria, through northern Central African Republic, South Sudan extreme, Ethiopia bordering its southern end to end in Somalia. Therefore, not surprising that along this line deploy its activity many armed groups like Boko Haram and Al Shabah and some others who use the religious element as an identity factor and motivating their armed struggle.

The first president of the young nation was David Dacko, who came to power through a coup backed by France. Later, in 1965 Dacko was overthrown by his cousin; Colonel Jean Bedel Bokassa-who ruled dictatorially, even proclaiming himself emperor and converting to Islam to gain the favor of Libyan leader Muammar Gaddafi. The mandate of the infamous dictator Bokassa was characterized by serious abuses and violations of human rights and in 1979, France had already lowered enough support to the dictator, which materialized in a coup against him, replacing in power Dacko again. In 1981, General André Kolingba rises to power through another coup. Again, France mentored the transitional process from President Kolingba to Ange-Félix Patassé.

In May 2001, Patasse put down an attempted coup supported by fighters of the rebel leader of Democratic Republic of Congo Jean-Pierre Bemba and Libyan militiamen. The subsequent repression was such as to be classified as a war crime. The subsequent government of military François Bozizé was supported by the former French colony and coincided with a period of instability, favored by the complicated regional situation in the neighboring countries of Chad, Sudan and Republic of Congo, until the signing of the peace agreement in Birao 13 April 2007. Bozizé is elected again in elections that are rated pantomime by the opposition.

In 2013, the umpteenth coup occurs. A group of rebels had joined since 2012 in a coalition called Seleka ("alliance" in the local language Sangho) with the Muslim religion and etiquette minority oppressed by the Christian majority as an identity factor. Seleka was formed by Muslim fighters with strong cross-border links with Chad and Sudan (Chadian and Sudanese mercenaries, the latter led by General Moussa Asimeh, accused of genocide crimes in Darfur) in the border region of northeastern Central African Republic. From the outset, however, it was revealed that slightly more than the lust for power and wealth and a strong desire for revenge motivated the unity of the leaders of this group. In fact, later this group will experience numerous divisions in the years 2013-14.

The performance of the Seleka coalition received widespread condemnation from the international community. In addition, the new administration was raised revise mining contracts signed by the previous president with Chinese and South African companies. In response to the insurgence of Seleka, the antibalaka militias ("-" anti-balles-AK "in local languages" anti Cutlass "or booletproof AK 4) are formed. They have the widespread belief that amulets and objects carrying protect them from bullets to fight the first and Muslim communities in general. In the beginning, these militias are organized in the capital Bangui, in 2013 around groups of Christian militiamen and motivated by the agitation of the popular historical imaginary response to the slave expeditions Muslims Northeast and frustration because of its prevalence in the areas of trade and mining animists. Agitation of religious identity factor reaches its peak under the rule of ousted President Bozize, who led an evangelical church during his tenure and later was one of the main sponsors of the anti-Balaka movement from exile. Although the religious element does not appear to be at the root of the Central African conflict, a direct consequence of these tensions have been high levels of sectarian violence that have occurred during the war.

The conflict leads to anarchy

The current conflict that has ravaged the Central African Republic has contours that reflect the competition for access to natural resources, control of trade and financial networks and national and ethnic identity. Before the conflict, the Central African population was distributed approximately 85% of Christian and animist population and 15% Muslim population.

ethnic division of the Central African Republic.

As indicated above, François Bozizé was overthrown in 2013 by the Seleka alliance, which controls the country reaching the gates of Bangui. Bozize is forced to sign a peace agreement whose duration is minimal since the March 24, 2013, Seleka aúpa Michel Djotodia military power. The government of Bangui was unable to maintain order beyond the capital and attacks on the Christian population and churches succeeded, prompting the president Djotodia to order the dissolution of the Seleka armed group, although many commanders of the militia ignored the extent demonstrating the lack of authority of the leader of the coalition on them since operated with considerable autonomy because of their Sudanese origin or Chadian. On the other hand, both Djotodia as Seleka coalition led, since coming to power,

As is known, this situation causes the reaction of the antibalaka, originally born in the 90s to protect the population from bandits and criminals, and the outbreak of violence between the two groups, who see in this situation a unique opportunity to instrumentalize religious differences to their advantage. Sectarian violence caused thousands of deaths and causes the displacement of more than one million people throughout the country. As a backdrop to this fratricidal conflict is the exploitation of mineral resources rich areas, what is the real reason for the conflict is revealed more intense in these regions.

The Seleka are forced to leave Bangui with the thrust of the antibalaka militias in January 2014. Instead, take their strongholds in the north and northeast of the country where they obtain resources from exploitation of gold and diamond mines. For its part, the antibalaka settle in the southwest region where major diamond mines. Both groups use ethnic cleansing against members of the rival community, leading to massacres of Christians or Muslims according to the territory and which group controls.

International pressure forces Djotodia to resign in January 2014 and is replaced by the ruling Catherine Samba-Panza who holds the position of president temporarily. However the outlook is bleak: a Armed Forces whose members also ineffective in many cases have ties with irregular armed groups. Amid the anarchy, the security of the population is in the hands of different international missions mentioned later.

which has resulted in violence and displacement for members of the latter group at the hands of antibalaka; which in turn has caused some are finished joining the ranks of ex-Seleka groups.

The role of international missions and regional actors

With the coming to power of Djotodia the starting point of the international missions is marked, due to the lack of control over this territory and the enormous dimensions was reaching humanitarian crisis. On 5 December 2013, the United Nations approved Resolution 2127/2013, authorizing the deployment of the International Support Mission in the Central African Republic (MISCA), supported by a French military force. This support mission was named Operation sangaris.

Beside, the EUFOR RCA mission is temporarily on 10 February 2014 to provide temporary support to missions already mentioned, stabilize some of the most dangerous areas of the capital and handing the deployment of United Nations (MINUSCA). In this mission, army units and the Civil Guard of Spain played a prominent role.

Some 9,000 soldiers approximately were revealed clearly insufficient to maintain order in a country the size of France and widely dispersed population. Consciousness quickly took by all stakeholders; Central African Republic, African Union and United Nations, the need for a comprehensive approach to peacekeeping in the protection of civilians was the main priority. Resolution 2149/2014 of the Security Council enabled the launch of the Multidimensional Integrated Stabilization Mission United Nations in the Central African Republic MINUSCA, authorizing the deployment of up to 12,000. For experts in the region as Lt. Col. Jesús Díez Mayor, the mission was born in 2014 marked from the outset as insufficient to curb the chaos and violence that had already spread throughout the whole country; with the serious threat of cronificar the situation of the country's division for sectarian reasons and the rule of armed groups and warlords.

Almost four years later, the situation is not very encouraging and the task of MINUSCA can be described by a cinematic simile of "Mission Impossible". The Mission has been renewed by Resolution 2387 (2017) of the Security Council, extending the mandate of the same until 15 November 2018. Although during 2017 there have been modest progress in the deployment of authority state throughout the country, violence persists widely. The blame for this is largely attributable to the use of inflammatory rhetoric, ethnic stigma and religious manipulation by politicians and the media, creating a propitious environment for the revival of the conflict. While violence has decreased among communities, clashes between armed groups and self-defense militias have increased in recent times, especially in areas where seasonal migrations occur. Clearly, the race to dominate territory and access to natural resources is the main cause of violence between different armed groups factor.

West of the country, coinciding with the reopening of transhumance corridors, the antibalaka forces have faced pastoralist groups ethnic Fulani in the prefecture of Mambéré-Kadéï after members of this group ransacked towns near Gamboula killing civilians . The MINUSCA has succeeded in ending the presence of armed groups such as 3R in Bocaranga and the Patriotic Movement for Centroáfrica MPC Bang (later I will discuss in more detail these groups), making the first sign an agreement with local antibalaka militias in Bouar, to end the spiral of violence in the region.

On the downside, new groups like cleavages existing as the National Movement for the Liberation of Central Africa (CLN), emerged from the MPC, competing with other groups to gain control of territory and trade routes in the emerging west corner of the country. In other prefectures of Ouham as further east, fighting between antibalaka militias and ex-Seleka groups they caused the destruction of towns and important movements of displaced persons. There are few groups that still today sabotaging the timid attempts to restore state authority. In addition, in the eastern corner they operate other armed groups from neighboring Uganda as militia Lord's Resistance Army (LRA), which constitute a serious threat to civilians.

Paradoxically, the situation in the capital Bangui is relatively stable despite rumors that it might be brewing an armed insurrection. 2017 has also been the most dismal year for members of the missions of peacekeeping with 13 people killed in different circumstances.

In parallel, a European military training operation called EUTM RCA to support the Armed Forces of the Central African Republic develops. Spain has participated deployed 30 military members of the European army.

At the same time, US special forces landed in the country in December 2011, establishing a base at the southeastern end as part of a mission to neutralize the rebel Ugandan origin Joseph Kony, leader of the "Lord's Resistance Army". The Central African Republic is included in a group of 10 countries in the Central Africa region whose area is included in the performance of the African Command (AFRICOM) based in Stuttgart (Germany). The troops were established in the city of Obo with support from local military and armed forces of Uganda. Although the mission was declared ended unsuccessfully, it is unknown today if it continues to present a contingent of US troops in the region.

Against the deployment of Europe and the United States, Russia and China are struggling for room in such a complicated and coveted for its abundant mineral resources region. In 2017 the UN authorized an exception to Russia to provide weapons and military personnel to the government of Bangui, primarily to assist in sustaining the beleaguered weak central government and its armed forces. This privileged position has allowed Putin to sign bilateral agreements with the government currently in charge a contingent of Russian troops from the security of the current president Touadera. Russia exhibits muscle which is the first African mission with boots on the ground in the region, thus accessing influential positions in the administration of the central African country. China, meanwhile, no slouch and has been present in the region with its "checkbook diplomacy" in recent months reaching important economic agreements on military matters, bilateral debt forgiveness and training of officials. The readiness of Russia and China to "help" the weak Central administration has not done more than raise suspicions for France and other European countries about the true intentions of this support, with the suspicion that it may be in return for obtaining concessions mining or privileged trade relations. The MINUSCA itself has not been without controversy as there have been allegations of sexual abuse and other human rights violations committed by members of the mission. arriving in recent months important economic agreements on military matters, bilateral debt forgiveness and training of officials. The readiness of Russia and China to "help" the weak Central administration has not done more than raise suspicions for France and other European countries about the true intentions of this support, with the suspicion that it may be in return for obtaining concessions mining or privileged trade relations. The MINUSCA itself has not been without controversy as there have been allegations of sexual abuse and other human rights violations committed by members of the mission. arriving in recent months important economic agreements on military matters, bilateral debt forgiveness and training of officials. The readiness of Russia and China to "help" the weak Central administration has not done more than raise suspicions for France and other European countries about the true intentions of this support, with the suspicion that it may be in return for obtaining concessions mining or privileged trade relations. The MINUSCA itself has not been without controversy as there have been allegations of sexual abuse and other human rights violations committed by members of the mission. The readiness of Russia and China to "help" the weak Central administration has not done more than raise suspicions for France and other European countries about the true intentions of this support, with the suspicion that it may be in return for obtaining concessions mining or privileged trade relations. The MINUSCA itself has not been without controversy as there have been allegations of sexual abuse and other human rights violations committed by members of the mission. The readiness of Russia and China to "help" the weak Central administration has not done more than raise suspicions for France and other European countries about the true intentions of this support, with the suspicion that it may be in return for obtaining concessions mining or privileged trade relations. The MINUSCA itself has not been without controversy as there have been allegations of sexual abuse and other human rights violations committed by members of the mission.

Finally, we should not lose sight of the role played by regional players and in this sense we can not fail to mention Chad, northern giant that played a key role in the fall of Bozizé. Shares a 1,200 km border with the Central African Republic, through which a large volume of trade occurs. Factors such as the main groups opposed to Chadian President Idriss Deby came from northern Central African Republic and the advance of desertification, which causes the nomadic cattle across the border (second source of income in importance for Chad), increasingly have to travel further south conditioning relations between the two countries and are generating conflicts. Additionally, It has been reported occasionally some "sympathy" from the Chadian side to the Seleka and ex-Seleka groups, making it difficult mediating role it can play in the region. What is certain is that Central African Republic is a major concern for Chad, as the country depends almost exclusively on oil revenues generated in the wells that are located along the border between the two countries, taking into deposits that extend into the territory of the Central African country.

A look at the armed groups and warlords

I indicated earlier that the military dynamics of the conflict in Central African Republic is much more complex and overcome the rivalry between Seleka and anti-Balaka groups. For some years, the country has seen the proliferation of armed groups and their division into smaller groups to perform at a more local level, and thus have effective control over the resources of the area. This fragmentation and dispersion of armed groups further hinders a possible solution to the conflict because even traditionally antagonistic groups, have established strategic alliances surpassing the old dividing line between Seleka and anti-Balaka.

Hinterland of armed groups.

According freelance journalist Philip Kleinfeld, the main groups are:

- Renaissance Popular Front for the Central African Republic (FPRC) group from the "hard" line ex-Seleka, led by Nourredine Adam and former leader Michel Djotodia coalition. They have established alliances with some elements of the antibalaka militias.
- Union for Peace in the Central African Republic (UPC), ex-Seleka group led by Ali Darassa whose former headquarters was located in Bambari. They claim to represent the interests of the Fulani / Peuhl community in the country. Throughout the year 2017, they fought against FPRC.
- General Ali Darassa of the Union for Peace in the Central African Republic.
- Patriotic Meeting for the Renewal of Central Africa (RPRC), ex-Seleka group formed in the diamond region of Bria in 2014. Led by the former commander Zacharia Damane Seleka and former parliamentarian Gotran Djono Ahaba. The group has a significant presence and influence the Gula ethnic group.
- Patriotic Movement of Central Africa (MPC), another ex-Seleka faction formed in 2015 as a dissident FPRC. The group fractionates turn in mid-2017, being born a new group called MPC Siriri.
- Revolution and Justice (RJ), formed in late 2015 in the northwest under the leadership of Armel Ningatoloum Sayo. The group has recently held fights with the National Movement for the Liberation of the Central African Republic (CLN) around the town of Paoua, which has caused significant displacement of refugees into Chad. The CLN is led by the general proclaimed Ahamat Bahar; ex-Seleka, ex-FPRC and former MPC. It is suspected that the CLN receives significant support from the Fulani nomadic communities from Chad.
- Return, Reclamation, Rehabilitation (3R), led by General Sidiki Abas, based in the northwestern region of the country near the border with Cameroon. This group is practically dominated by fighters Fulani / Peuhl group.
- Anti-Balaka Christian militia group and animists with local structures scattered throughout the country. The main factions are led by Patrice-Edouard and Maxime Ngaissona Mokom, whose group is supported President Francois Bozize earlier and allied himself with former Seleka FPRC since 2015.
- Self-defense groups, a new generation of militias arose during the year 2017 under this

name in the Southeastern region. Distantly connected with anti-Balaka groups have launched attacks on both Muslim communities and members of United Nations missions.

Violence is renewed in 2017

More recently, in early 2016 in the Central African Republic elections they were held and the transition was verified from an interim government that had ruled the country since 2014. Faustin Archange Touadera was elected president, in a context of heavy reliance on international funds and a state authority that blends the more we move away from the capital Bangui. That state structure is still very fragile and few steps have been taken in the direction of achieving the desired stability. As we saw earlier, the Seleka movement has split into factions that fight even including attacking civilians belonging to ethnic communities of rival groups. All parties, including the armed forces, have ties to organized crime and extortion use in their areas of control.

This cocktail of weak administration, sectarian violence and competition for natural resources among different warlords had already caused more than 600,000 internally displaced and over 500,000 refugees in neighboring countries by UNHCR in late 2017. In addition, more than half of the total population is in need of humanitarian aid. These figures are shocking if we put them in perspective with the total population of Central African Republic: approximately 4,600,000 people, which gives us some idea of suffering to which the civilian population is subjected.

The focus of the new outbreak of violence would be the town of Bangassou, a coastal city in southeastern, about 30,000 inhabitants on the banks of river Bomu. It would not be for lack of alert since early 2017 recruitments of young people and the presence of members of the UPC (ex-Seleka militia led by Ali Darassa) began to occur, taking advantage of the withdrawal of American and Ugandan troops from the eastern region. In parallel, a new generation of Christians and animists groups called "self-defense" began to proliferate in the city, to the persistent rumors of the presence of the UPC group in the region. It did not help too much animosity toward these self-defense groups MINUSCA troops deployed in the area, Moroccan Muslim, the belief that there were abetted by the former Seleka militias and particularly with the UPC. The conflict was served.

In the background of the arrival of war Bangassou, previously relatively peaceful region, they hide complex dynamics. On one hand, the split into two factions of one of the larger groups Seleka: FPRC (led by Nourredin Adam and Michel Djotodia) and UPC; formed by nomadic Fulani fighters community. Both groups controlling the country's mineral resources vied; in an attempt to wrest the mining areas controlled by the UPC, the FPRC allied with some antibalaka factions, causing the eruption of a strong anti-Fulani sentiment in local populations. UN decides to evict the UPC leader, Ali Darassa, its stronghold of Bambari in February 2017 to avoid a bloodbath, as FPRC troops were advancing. This decision caused all that is shifting the problem further south, where local populations were already sensitized against the presence of UPC fighters in the region. Violence erupted between the militia of the UPC and self-defense groups a "hunt" of Muslims in the area taking place.

In the midst of all this horror, episodes hope that invite occur. Bishop of Bangassou, the Spanish Juan Jose Aguirre, offered as a human shield to thousands of Muslims who had taken refuge in a mosque, protecting the antibalaka violence. A mosque that had been displaced neighbors of Tokoyo, mainly Muslim recommended by the UN contingent. Previously, about 1500 antibalaka militants had orchestrated a plot to kill anyone suspected of being Muslim. The attack and subsequent siege to the mosque ended with hundreds dead, until all internal refugees were evacuated. Despite the heroic gesture, he could not prevent many Muslims have had to flee to northern regions of the country.

When the war is a profitable business

The Central African Republic is one of the world's poorest countries. All this despite its abundant mineral and forest reserves. Forced displacement due to the conflict has severely affected agricultural and livestock production in the country, leading to a food crisis unprecedented. An estimated three million people live in extreme poverty. South-north of the battered Muslim communities, which formerly controlled the commercial networks throughout the territory, exodus has contributed to the economic collapse of the country.

In this context, an entire industry has flourished network of illicit economies that can be termed "economy of the warlords." Armed groups obtain huge profits from extortion and taxes illegal trade in gold and diamonds. Looting and theft is not uncommon for the militias. Some groups like the LRA, have profited from illegal hunting of elephants for ivory trafficking in the Asian market.

Despite being a major world producer of diamonds in 2013 he was banned its sale under the Kimberley Process; international certification that seek to regulate trade in this precious mineral to prevent so-called "conflict diamonds" end up in the international market. Such a ban was partially lifted in 2016. Despite the good intentions of this initiative, there is another area where more visible than the serious and systematic violation of human rights can come from large multinationals rather than the state itself. In this regard, the recent article by Professor Tania García Sedano for the Institute for Strategic Studies is instructive.

The diamondiferous regions are highly sought after by armed groups, often determining the course of their strategic movements and military actions. This can easily check whether superimpose maps scope of armed groups and the distribution of natural resources in the country, throwing amazing coincidences.

natural resources of the Central African Republic.

The Central African Republic does not seem to have oil reserves, although the former President Bozizé granted some exploration licenses in the north, on the border with Chad, Chinese companies. The Seleka revolt led to the revision of these contracts.

Another important source of mineral wealth is the country's uranium reserves. Recently, in France a case of corruption promoted by the French giant uranium, Areva, through a Canadian subsidiary, Uramin, to mediate with former President Bozizé a benchmark conflict to a mining license in Bakouma is investigated . Uranium mines the Central is equally coveted by other countries like UK and South Africa.

In more recent times, China has shown great interest in the exploitation of natural resources in the region, which could lead to a competition between great powers to serve as feedback from the conflict itself.

conclusions

The conflict in Central African Republic, despite having entered a phase of lower intensity, does not seem to completion peeped medium term. In the center of conflict converge several powerful dynamics for continuity.

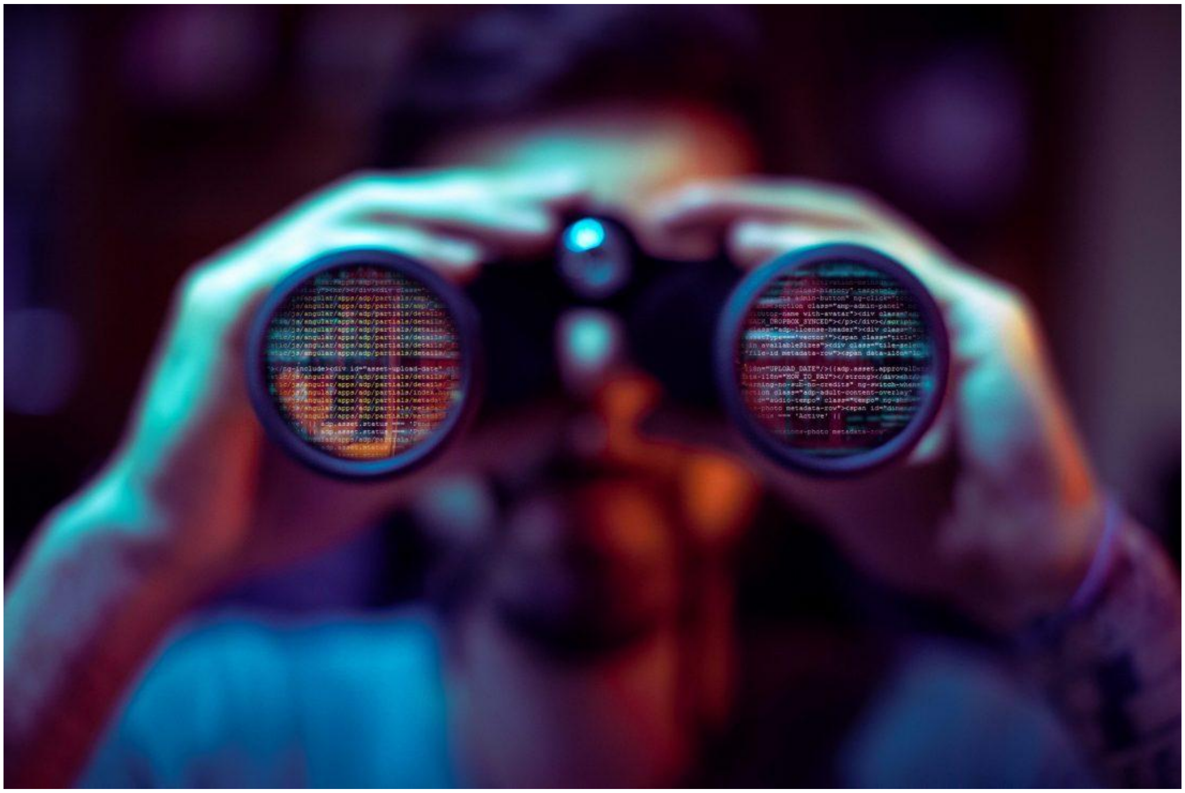
Nathalia analyst for Dukhan, the country apart from being one of the poorest in the world is one of the most volatile. This situation has been reached partly due to predation by successive political elites who have ruled the country and the "ghost state" which has facilitated the proliferation of large criminal groups have become violence certainly a profitable business syndrome.

As cover for their criminal activity, these groups have raised the specter of religious and ethnic differences, fueling tensions between communities, to the point of ethnic cleansing. Trinidad and journalist Deiros indicated back in 2014 in an article published by the Institute of Strategic Studies, that what was happening in that country was a religious conflict "invented". The true origin of the conflict can be found in the struggle of different groups to seize control of resources, taking advantage of pre-existing tensions, struggle that becomes fiercer if possible to natural circumstances such as the advance of desertification, causing conflict between sedentary and nomadic groups as we saw farmers.

The recent arrival on the scene of international powers with interests and agendas found, does not appear to be a factor that would help stabilize the country as it could be exploited by different warring parties to seek their own survival and achieve higher levels of power . The current situation of chaos and violence will take years to reverse it and have to take many steps in the right direction. It seems that this is not the case in the present context.

Cyber Intelligence: Reinventing the wheel

Ulises Leon Kandiko (Argentina)



As I have said many times, today every technological component will usually precede the term Ciber then followed by the topic of interest, in this case the Cyber Intelligence. However, and like other notions related to cyberspace, there is no definition Crystallized "Cyber Intelligence", not even enough focused on how it prepares studies, although you will find several articles on the subject, there is still a doctrine fully accepted .

By supporting the idea that organizations must pass security reactive to proactive, postures management and oppose the attitude of interpreting cybersecurity mainly as "Measures taken after the event" and "static perimeter defense", various representatives of the cybersecurity community are now sponsoring the adoption of concepts, tools and practices for the development and exchange of global intelligence on cyber threats. This intelligence should enable consumers to understand the operation, tactical, and strategic threats contexts (agents, capabilities, motivations, objectives, impact and consequences not only from a technical perspective); provide their developments short, medium and long term; and take preventive decisions.

If integrated into their decision-making related to security, should enable organizations to take action "predictive and proactive instead of facing the past" in a format "dynamic rather than static" and "agile and adaptable vs . and shaped rigid postures "toward cyber-related hazards. Intelligence described above often labeled as "Cyber Intelligence" (CYBINT). Overall, CYBINT is used to convey the idea of a broad and qualified better understanding of actual or potential related to cyberspace that can threaten an organization events.

If you look relevant policies or mechanisms that have been recently implemented (especially Europe) and other documentation issued by private or public and academic order organizations, the Cyber Intelligence is not always defined exhaustively and definitions vary [i]. Despite the increasing use of this or similar expressions by academics, the media and professionals, the current thinking on the subject is limited and not well developed. Further investigation of the issue, both either from a theoretical and practical point of view, is missing.

On the contrary, both academics and professionals in the field of Homeland Security United States (USA), have reflections on the relatively more advanced Cyber Intelligence. This could be the result of the earlier adoption of concepts, practices and technological solutions related to CYBINT based on US government agencies, similar situation can be seen in Russia and China.

Looking for a definition, terminology or notion.

Sadly in everyday language CYBINT commonly used primarily as a wrapper or expression. What is CYBINT more accurately? It should be understood as a product and process, it is intelligence "from", "inside", "or" to "cyberspace or some combination thereof? What are the main sources of CYBINT? How is this done? The cycle "traditional" intelligence is applicable to the CYBINT? What are the problems associated with the creation and sharing of CYBINT use? Trying to answer some of these questions might lead us to understand the CYBINT.

For example, the lack of a uniform understanding of the term "cyber" makes any attempt to propose a comprehensive and uniform CYBINT notion. In fact, while it is more or less indisputable to establish what intelligence (as product and process) is to define it in relation to the cyber domain is a challenge. One may wonder, however, how these concepts apply to a domain that differs from the traditionally known domains. Cyber is, in fact, man-made, a not completely evolutionary highly tangible, technologically configured and that, perhaps, needs to be interpreted by different paradigms. Their interactions with the physical / actual domain is not yet fully understood.

In addition, the CYBINT is a relatively new practice, which is far from being fully tested, evaluated and developed. There is not enough shared experience about how it works and on best capabilities to carry it out effectively. This hinders any attempt to come up with a comprehensive interpretive model for CYBINT.

Depending on the scope of activities of gathering information, the means used to carry them out and the final purpose they serve, there are really two ways to look at or interpret CYBINT. One way is to think of the CYBINT as intelligence "" cyber; ie the knowledge produced through the analysis of any valuable information collected "in" or "through" cyberspace. This is the CYBINT sensu stricto. From this perspective, "cyber" refers to the domain where data as in other words, that vast digital repository of information that can be retrieved and processed are obtained both; and / techniques / media tools through which this data is collected (for example, through technologies and techniques operating computer networks). According to this interpretation, CYBINT can, in principle, support decision-making in any domain, not just to counter cyberthreats. It can support a wide variety of missions in government, industry and academia, including policy development, strategic planning, international negotiations, risk management and strategic communication in areas beyond cybersecurity. In other words, the CYBINT can operate "independently and not necessarily to support mission cyber". However, since the CYBINT often discussed in relation to cybersecurity or prevention and response to cyber threats, these are the primary targets, but again,

Another way to interpret it is considered as CYBINT intelligence "to" cybernetics; that is, vision that is derived from an intelligence activity complete source that occurs within and outside cyberspace. Sensu lato is the CYBINT. In this sense, intelligence "to" cybernetic also may include (or based on) intelligence "from" cybernetics. You can draw from any discipline of intelligence that provide crucial knowledge, regardless of the source, method or means used to produce it. As such, CYBINT may result from the combination of open source intelligence (OSINT), signal intelligence (SIGINT), geospatial intelligence (GEOINT), Social Media Intelligence (SOCMINT) and human intelligence (HUMINT). From this point of view, the CYBINT is less a discipline in itself an analytic practice based on information / intelligence gathered also through other disciplines and designed to inform decision-makers on issues related to activities in the domain of cyberspace. What qualifies this kind of intelligence as "cyber" it is the purpose for which it is made: to support decision-making on issues related to cyberspace.

The two discussed perspectives on CYBINT "from" and "to" are often condensed into a single integrated concept. This is also due to the fact that intelligence "to" actually incorporates cyber cyber "" one. The result is a broader notion of CYBINT including the collection, processing, evaluation, analysis, integration and interpretation of the information that is available "inside", "through" and / or "external" cyberspace to improve decisions about threats related to cyberspace.

As for the information to create CYBINT, this may vary from network technical data (eg, data, hardware and software), data on hostile organizations and their capabilities, cyber ongoing activities potentially relevant information about geopolitical events. The data type and their classification are not functional to the definition of CYBINT. The data may be raw data or already processed; They can be legally obtained by illegal actions or intrusion / exploitation open source, proprietary or other ordered sources. As suggested by the literature, multiple sources of information are needed to develop a more holistic understanding of the threat environment and produce a comprehensive CYBINT. The most important aspect of the data is to be validated in some way. When analyzed, the information should enable those responsible for making decisions identifying, tracking and forecasting capabilities, intentions and activities cybernetic offering courses of action. This is the main feature of the CYBINT; ie the enabling goal of providing consumers with knowledge of potentially hostile activities that may occur in the cyber domain or may be perpetrated by or against cyberspace, allowing them to design counter (proactive) preventive measures or (reactive). cybernetic intentions and activities offering courses of action. This is the main feature of the CYBINT; ie the enabling goal of providing consumers with knowledge of potentially hostile activities that may occur in the cyber domain or may be perpetrated by or against cyberspace, allowing them to design counter (proactive) preventive measures or (reactive). cybernetic intentions and activities offering courses of action. This is the main feature of the CYBINT; ie the enabling goal of providing consumers with knowledge of potentially hostile activities that may occur in the cyber domain or may be perpetrated by or against cyberspace, allowing them to design counter (proactive) preventive measures or (reactive).

Depending on its scope or level of action, CYBINT can be strategic, tactical, or operational. There is no uniform what the different levels of CYBINT must be interpretation. According to the literature, strategic CYBINT focuses on the long term. Generally, reviews trends in current and emerging threats and examines opportunities to contain these threats. It serves processes applicable to decisions aimed at achieving the mission of an organization and determine its direction and goals. CYBINT covers strategic threat landscape, brand trends (political, social and economic) affecting the organization and identifies threatened actors, their goals and how they can try to achieve them; It is rich in contextual information. CYBINT tactic refers to what happens on the network. It also examines the strength and vulnerabilities of an organization, and tactics, techniques and procedures (TTP) used by actors of the threat. Because of its nature and scope, tactically CYBINT generally corresponds to the intelligence of cyberthreats. Usually more technical in nature, reports the steps and actions focused on the network that the organization can take to protect assets, maintain continuity and restore operations. As regards operational CYBINT, is the knowledge of imminent or direct threats to an organization. It allows and maintains operations and daily departures. At this level, the CYBINT look at the organization and vulnerabilities in their internal processes. It also examines the strength and vulnerabilities of an organization, and tactics, techniques and procedures (TTP) used by actors of the threat. Because of its nature and scope, tactically CYBINT generally corresponds to the intelligence of cyberthreats. Usually more technical in nature, reports the steps and actions focused on the network that the organization can take to protect assets, maintain continuity and restore operations. As regards operational CYBINT, is the knowledge of imminent or direct threats to an organization. It allows and maintains operations and daily departures. At this level, the CYBINT look at the organization and vulnerabilities in their internal processes. It also examines the strength and vulnerabilities of an organization, and tactics, techniques and procedures (TTP) used by actors of the threat. Because of its nature and scope, tactically CYBINT generally corresponds to the intelligence of cyberthreats. Usually more technical in nature, reports the steps and actions focused on the network that the organization can take to protect assets, maintain continuity and restore operations. As regards operational CYBINT, is the knowledge of imminent or direct threats to an organization. It allows and maintains operations and daily departures. At this level, the CYBINT look at the organization and vulnerabilities in their internal processes. techniques and procedures (TTP) used by actors of the threat. Because of its nature and scope, tactically CYBINT generally corresponds to the intelligence of cyberthreats. Usually more technical in nature, reports the steps and actions focused on the network that the organization can take to protect assets, maintain continuity and restore operations. As regards operational CYBINT, is the knowledge of imminent or direct threats to an organization. It allows and maintains operations and daily departures. At this level, the CYBINT look at the organization and vulnerabilities in their internal processes. techniques and procedures (TTP) used by actors of the threat. Because of its nature and scope, tactically CYBINT generally corresponds to the intelligence of cyberthreats. Usually more technical in nature, reports the steps and actions focused on the network that the organization can take to protect assets, maintain continuity and restore operations. As regards operational CYBINT, is the knowledge of imminent or direct threats to an organization. It allows and maintains operations and daily departures. At this level, the CYBINT look at the organization and vulnerabilities in their internal processes. informs the steps and actions focused on the network that the organization can take to protect assets, maintain continuity and restore operations. As regards operational CYBINT, is the knowledge of imminent or direct threats to an organization. It allows and maintains operations and daily departures. At this level, the CYBINT look at the organization and vulnerabilities in their internal processes. informs the steps and actions focused on the network that the organization can take to protect assets, maintain continuity and restore operations. As regards operational CYBINT, is the knowledge of imminent or direct threats to an organization. It allows and maintains operations and daily departures. At this level, the CYBINT look at the organization and vulnerabilities in their internal processes.

It is worth to make it clear that the distinction between the levels described CYBINT is mostly academic. In practice, there is no clear demarcation from a level of intelligence to another; often they overlap or combine. In addition, the meaning of strategic, tactical and operational is likely to vary among organizations because of their size, complexity, mission and related attributes. Regardless of any clear demarcation between levels, the ability of an organization to consider all these levels and the art of intelligence that allows you to understand the challenges and opportunities that are likely to encounter in the short, medium and long term is very important.

The process of Cyber Intelligence: Alternative models vs. traditional

The process to which all refer is none other than the famous "Intelligence Cycle" [ii], which has been studied and questioned several times by professionals and academics to the point that have been proposed and discussed alternative models. The "validity / applicability" traditional intelligence cycle also at issue in the context of CYBINT. As an eminent expert noted, "as intelligence grows increasingly digitized and cybernetics form (in their field, its methods and its forms), a clearer understanding of intelligence and its cycle is actually a heuristic device rather dated, rather than a constructive dimension of intelligence as such can release the stakeholders to think about intelligence in more innovative ways "[iii]. This view is shared by other academics and experts, who consider the cycle as linear and repetitive, since it does not emphasize the natural interrelation of activities (planning, collection, processing, etc.) while the process is CYBINT their mutual relevance; in other words, not capture their interdependencies and mutual influences.

Indeed, those who criticize the cycle, based on arguments that are inadequate to describe the representativeness of the intelligence cycle in general, regardless of CYBINT. Therefore, one can question more deeply if an ad hoc interpretive model is needed to explain the process CYBINT; or, in other words, why CYBINT process is so peculiar and different processes embedded in other fields requiring intelligence be described through an alternative and particular model for CYBINT. Provide concrete answers to the above questions would require a clear thorough and complete understanding of CYBINT as a concept and as a practice even more. Such an understanding is elusive because of the lack of sufficient reflection and experience in CYBINT. Therefore, at the present stage, the definition of interpretative model represents primarily an intellectual exercise or a test whose results must be validated progressively. However, some arguments seem to support either the definition of an ad hoc model to explain the CYBINT process.

Tautologically speaking, the main feature of the CYBINT lies in the fact that it is "cyber"; ie it is knowledge on issues related to cybernetics. CYB INT involves analyzing the information gathered cyberspace and other sources to achieve purposes related to cyberspace. At the very basic level, the "cyber" adjective refers to a domain by man, highly evolving with technological form and not entirely tangible created. In this domain, information is generated, processed, disseminated, shared, stored, altered, is consumed and destroyed by a multitude of actors at an incredible speed. The impact of specific decisions on issues related to cyberspace and its effects on both the virtual and physical domains so are difficult to predict. This affects how the CYBINT is produced and consumed. Defy the basic functions of the intelligence process when the collection, evaluation, analysis, integration, interpretation and dissemination of intelligence information applies to Cybersphere, namely.

With respect to the collection and evaluation, CYBINT also based on the information provided by uncontrolled sources such as the Internet. This information must be filtered, evaluated and (somehow) validated. The filtrate is essential to select only significant information elements cyberspace. Evaluation is often a challenge due to the high volatility and uncertainty anonymity of the data available in cyberspace and heterogeneous data sources. To validate the data, it becomes essential to corroborate the information derived from a source with that from other sources, and it is better if at least one of the first controlled. Filtering, evaluation and validation aims to alleviate the "anarchy of information" generated by the high volume of data available along with the lack of control over them. Since the process of CYBINT may also use the information / intelligence produced through other disciplines, the integration of all relevant knowledge in a single consistent product can be challenging. This is due to the different formats, nature and degree of uncertainty of information and intelligence obtained cyberspace (eg information or other technical data from social networks, web forums, etc.) confronted with other "non-virtual" sources . The uncertainty also affects the interpretation of the processed information; ie, judgment and deductions based on it, which is usually added in the final cybernetic product.

Another important aspect to consider when defining any interpretative model for CYBINT process is the time frame set that is often required to perform intelligence functions. This requires that the functions occur simultaneously or shortcuts taken in its implementation. In other words, the functions do not run in a circle, but establishing a "network channel" between them.

Apparently, we could be faced with the need to have an own intelligence cycle for CYBINT, or at least revitalized. Looking at the literature, a team of experts and academics working in the Software and Engineering Institute (SEI) of Carnegie Mellon University proposed its own model a couple of years ago. The SEI model differs from the cycle of traditional intelligence due to the adopted terminology is not linear and logically strict or consequential functions that is the process, the breakdown of analysis functions into two specialized functions (technical or functional analysis and strategic) analysis and the ability to combine technical cybersecurity "narrow" and prevention purposes "broader" cyberthreats to which the CYBINT can serve within an organization. As illustrated, the proposed model fits the interpretation of the CYBINT as an analytical practice that relies on information / intelligence also collected through other disciplines and is intended to inform decision-makers on issues related to activities in cyber domain. The SEI model consists of five functions:

1. Determining the "environment" that establishes the scope of the effort CYBINT and influences the information needed to achieve this;
2. The "data collection" or exploring data sources and data collection and information filtering tools through intensive use of labor;
3. The "functional analysis" which is the performance of technical and customized analysis (usually in support of a mission cybersecurity) for deriving the "what" and "how" of threats;
4. The "strategic analysis" involving the review, integration with contextual information, and further elaboration of functional CYBINT in order to answer the questions "who" and "why"; Y
5. The "Report and comments"; ie the spread of CYBINT to decision makers and gathering feedback.

The main dependencies and mutual influences between the functions described are: data collection should be based on the determination of the environment, which is influenced by decisions made by the organization on the basis of CYBINT consumed. The resulting intelligence of functional analysis can inform decisions about actions to be taken at the level of the technical network of an organization that, in turn, impact the determination of the internal environment; the same goes for intelligence resulting from the strategic role, affecting both the internal and external environment. The strategic role also represents the resulting intelligence of functional analysis, which is consumable by those responsible for making decisions that may not have a technical background. From this perspective, It is a kind of supplement that helps to bridge the communication gap between analysts and key decision makers. The latter provide feedback on intelligence received in order to give analytically, adjust the direction of the organization and, therefore, influence the environment. Question the "validity" of the SEI model is beyond the scope of this article. The model was designed and proposed as a result of empirical work that mapped and assessed current practices in the US CYBINT. Also it has a regulatory scope; It suggests how the process should work to be effective. The latter provide feedback on intelligence received in order to give analytically, adjust the direction of the organization and, therefore, influence the environment. Question the "validity" of the SEI model is beyond the scope of this article. The model was designed and proposed as a result of empirical work that mapped and assessed current practices in the US CYBINT. Also it has a regulatory scope; It suggests how the process should work to be effective. The latter provide feedback on intelligence received in order to give analytically, adjust the direction of the organization and, therefore, influence the environment. Question the "validity" of the SEI model is beyond the scope of this article. The model was designed and proposed as a result of empirical work that mapped and assessed current practices in the US

CYBINT. Also it has a regulatory scope; It suggests how the process should work to be effective. Also it has a regulatory scope; It suggests how the process should work to be effective. Also it has a regulatory scope; It suggests how the process should work to be effective.

1D34S F1N4L3S

Having a clear understanding of CYBINT is important. It can help to relevant stakeholders to be consistent when they promote programs or take actions related to CYBINT political, legal, operational and other level. Such an understanding must be premise on the definition of a solid conceptual framework CYBINT. The adoption of this framework would also represent a basis for developing the CYBINT as a discipline element; ie a specific area of study or work in intelligence. Although most of the literature considers the CYBINT is an established or soon established discipline, it does not seem to be the case.

In other words, CYBINT not be considered a discipline that has not yet been sufficiently defined theoretically nor implemented in depth. In addition, as described throughout this article, the nature of the CYBINT and its manufacturing process makes it less a discipline that an analytical practice, which is based on information / intelligence gathered also through other disciplines. Of course, nothing prevents the CYBINT is established as a discipline that uses specific technical or human resources through the different functions of your process.

Personally I think the CYBINT end up being a discipline long before what is believed to use its own cycle due more to the peculiarity of cyberspace in which immediacy and interconnection coexist symbiotically making the classic cycle remains somewhat outdated conceptually. Cyberspace as mentioned here, is man-made, a not completely tangible highly evolving environment, technologically configured and that perhaps needs to be interpreted through different paradigms, it is for this reason that since the military field is known as the 5th domain, a new battle scenario where virtual also often live with the physical and therefore in my opinion require special attention,

Notes and References

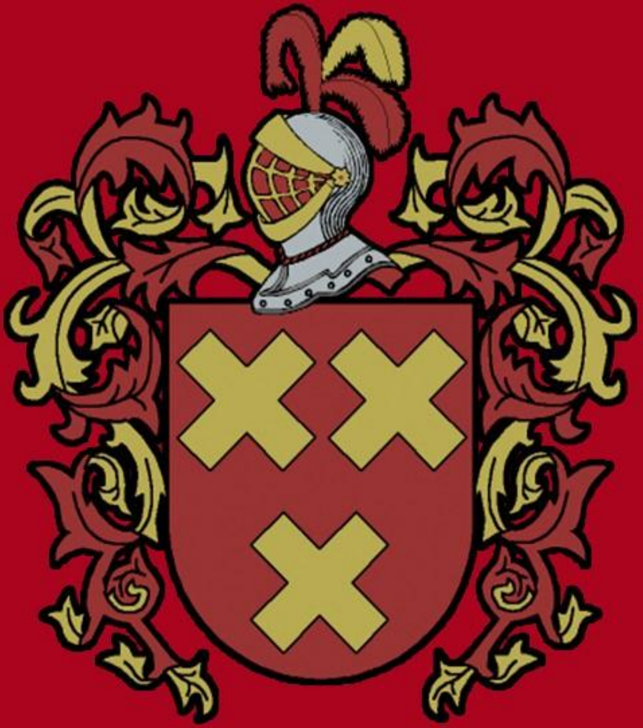
[I] Here are some of the documents that account for it. See, for example, Mario Caligiuri, Cyber Intelligence. Tra libertà e sicurezza (Roma: Donzelli, 2016); Mario Caligiuri, "Cyber Intelligence, the Sfida dei Data Scientist," June 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/ approfondimenti / cyber cyber intelligence-la-sfida-dei-data-scientist. html; Antonio Teti, "Ciber Intelligence" and Cyber Espionage.

[Ii] While there are different representations of the intelligence cycle, the most common include five distinct functions: planning and direction, collection, processing, analysis and dissemination. In the intelligence cycle, see Mark Phythian, ed. Understand the intelligence cycle (London and New York: Routledge, 2013). In particular, see Philip HJ Davies, Kristian Gustafson and Ian Rigden, "The intelligence cycle is dead, long live the intelligence cycle," to understand the intelligence cycle, p. 56.

[Iii] Michael Warner, "The past and the future of the intelligence cycle" in Understanding the Intelligence Cycle, p. 19.

Image source:
https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/10/iStock-610855316-1100x733.jpg

ANIVERSARIO NÚMERO 15



www.fuerzasmilitares.org

2003-2018

15

¡Siempre en Vanguardia!

Strategic Intellectual Capital Management

By Douglas Hernández (Colombia)

In this paper it aims to reflect on the possibilities offered by the strategic management of intellectual capital, and how they can contribute to this modern administrative and managerial techniques such as coaching, empowerment, Organizational DNA and benchmarking. Of course, we are thinking about how to translate these elements of the business sector, security sector and defense, using all the qualities and successful experiences that have been achieved in the first, to enhance the second and make it more efficient. As a preliminary step, it is appropriate to establish some definitions on which to base reflection.

Intellectual capital is its own intangible of all organizations, it consists of structural capital, which has to do with issues such as patents, goodwill, and other similar intangible assets; human capital, which has to do with the knowledge and skills of employees, and relational capital, which refers to how the organization relates internally with their environment and the market.

On the other hand, a definition that seems pretty accurate about the management, is provided by Chirinos, cited by Hernandez and Gomez (2010):

> Management is the art and science of working with and through a team towards achieving the objectives of an organization. This involves building a body of knowledge about such activity, and that activity involves managing relationships with others to achieve organizational goals. (P.628)

A manager is in general terms, responsible for directing and managing the affairs of a company or organization, as well as coordinating internal resources, represent the company against third parties and monitor goals and objectives. Specifically, you must fulfill four functions simultaneously:

- Plan: provides courses of action to achieve organizational objectives, taking into account available resources.
- Organize: the duty to provide time and space in human material and financial resources required to achieve the objectives.
- Direct: mainly refers to his leadership, and his capacity for decision-making, constantly influencing the progress of the process.
- Control: refers to qualitative and quantitative processes and implementation of plans that have been drawn measurements.

These four functions are common to managers, directors or commanders of military, police, intelligence and anti-terrorist units worldwide. In that vein, provide elements to help improve the performance of these actors will help the personnel and resources under his command are used more efficiently, and better results are achieved in the fight against crime, terrorism and new threats.

Strategic management, is one that is based on a holistic thinking, covering multiple aspects of the organization themselves, the environment and the market, and also projected into the future. There are levels of management focused on fulfilling quality objectives and / or quantitative short-term or low impact it is everyday affairs of the company or organization. The manager must ensure the manufacture of a certain number of units, within a specified period, with a specific quality, and using for this machinery, a personal and specific raw materials. And so over and over again. It's not competition this manager if the produce is sold or not, and what are the characteristics of the market or competition, let alone what will happen within 5 years with all these variables. This person does not meet strategic management functions.

On the contrary, in a management meeting, the general manager receives reports from production managers, finance, logistics and administration, and accordingly, and its market valuation, prospectively makes decisions that affect the whole company, today and in the future, in order to achieve objectives in the short, medium and long term. Other managers must implement the strategic guidelines from general management. In the context of security and defense, strategic decisions are taken by high levels of command, being clearer establish responsibility, because the organizational structure is eminently upright

Under the intellectual capital, it should be clear about that unlike other assets, its quantification is very difficult, given that it is intangible. But despite being intangible exist and affect one way or another the progress of the organization and the possibility of achieving or not achieving organizational objectives. Therefore, intellectual capital must also be gerenciado.

It has established itself as the intellectual capital consists of structural capital, human capital and relational capital. It is necessary to note that human capital seems to be the determinant of the other two, and therefore improvement in that variable will influence almost certainly in others, and these as a whole will allow an improvement throughout the organization.

In this vein, in this paper we will focus on human capital, and how to manage it strategically.

Human capital is then the set of knowledge, skills and talents possessed by a person and make it suitable to develop specific activities in the organization.

Logically, for each position knowledge, skills and talents are required. But there is also a body of knowledge, skills and talents that everyone should possess and that help create, sustain and improve interpersonal relationships. Roughly speaking, we can establish that it is necessary to define job descriptions for each worker, where specified what is expected of him / her in performing their specific functions -aquello so you pagan-, but also need a description generally what should be the profile of an employee of that company or organization. Thus, to properly manage must have:

- Compendium of job descriptions.
- Profile of an employee of the company or organization, which is made based on, and in turn strengthens:
    - Institutional philosophy.
    - Institutional values.
    - desired relationships.
    - Social values / Family.
    - Attitudes towards issues of concern to the organization, for example, the environment.

There are two main areas of action for the strategic management of intellectual capital:

- Knowledge, skills and talents that workers already have, which are aimed at fulfilling their daily tasks, and can be increased and improved.
- The attitude with which the worker deals with all matters related to its labor dimension, which is absolutely crucial in terms of results it will bring to the organization.

It is clear that a person with a high IQ, perfectly trained in the best universities in the world, with postgraduate studies, and an exemplary family life, may prove to be even harmful to the company or organization an unproductive employee, if you have the right attitude, on the other hand, an average person, with regular studies, and even attached to a dysfunctional family, can become an exemplary employee, if your attitude leads to it. According to this reflection a priori, it is essential to improve staff attitude as a basis strategy for achieving willing to give the best of their abilities, the best of themselves.

To achieve a change of thought, and therefore a change in attitude, aligning the personal objectives of employees with organizational goals, some modern management tools can be used.

In this vein, here are some items to consider:

1. Working with people is always long-term, it is processes.
2. The strategic planning process also.
3. Benchmarking, Empowerment, Coaching and Organizational DNA, are strategic for the important changes that are generated from them.
4. Improvements in Knowledge Management can be approached from Knowledge Management.
5. From Knowledge Management, one could try to create a learning community in the organization, while successively applied, the four strategies.
6. Outlined the strategic objectives of the organization, 5, 10 or 15 years in the context of philosophy and corporate values, strategies can be applied in this order: (a) DNA Organizational - forming and strengthening management, (b) Coaching - led by managers who accompany and grow human capital, (c) Empowerment - empowered teams of its mission and functions, and (d) Benchmarking - The organization take on new challenges with enthusiasm, efficiency and flexibility.
7. According to the above, you can take full advantage of each of these strategies, applying them in succession, and not advancing to the next, until the previous stage be consolidated.
8. I think an organization avoque to continuous improvement of its human capital, and plan at the strategic level, has multiple and more likely to survive and thrive than those who do not.

These are just some ideas for discussion. In the management area all is said and what works in one organization may not work in others. In that vein flexibility is a feature that must have a modern manager, to operate in the complex environment of transmodernity.

Precisely to bring more elements, it is important to make some clarifications on the management tools that we referred to a few paragraphs back.

Organizational DNA

In this interesting managerial strategy, an analogy of the company or organization, with (really gifted DNA) is living. The genetic material allows living things to evolve, react to their environment and adapt to change. Lozano, O., Gomez, H., and buttered, I. (s / f). said elements "DNA" that the company needs to evolve and react to opportunities in the environment, these are: culture and leadership, organizational skills, organizational structure and management. Noting further that these four elements are interdependent, and therefore must be mutually consistent. These authors note:

> We begin by analyzing the organization from the perspective of each of these elements. This allows us to know in depth the current situation of the company, ask where you want to reach, understand what needs to change, design how it will achieve change, and establish a management method to do so in a sustainable way through weather.
>
> Each DNA element contributes to the process of change in an organization, from first contact to the internalization change completely.
>
> These elements are implemented through an action plan that allows the organization to merge by involving the organization of what management understands and wishes (communication), integrating and engaging people in the same case (involvement), developing skills for build a fitness (training) and build a whole (Inclusion).

The structure as understood Lozano et al (s / f), is the functional division of labor in different roles and an associated positions, including horizontal and vertical interactions are presented authority. On the other hand, it refers to management decision making in a company. These decisions also have a hierarchy (consonant with our initial thesis statement). It is necessary to determine who makes what decisions trying to get what results. According to these authors, the variable that differentiates decisions is time. In this regard, a strategic decision is projected to a longer time (maybe years), whereas an operational decision, has to do with the outcome of the day, with the short term.

Knowledge and skills possessed by the staff is what is understood as competence, whereas culture and leadership behaviors of people of a company shall mean inside and outside.

Management draws a northern strategy, then the organization follows strategy. When the strategy and organization are not aligned, confusion and failed results occurs. Management decisions must pursue this alignment, taking into account four factors of organizational DNA.

In culture and leadership should prioritize effective communication and transparency and availability of information, thus facilitating teamwork. Regarding organizational skills, it is important to clearly define job profiles, roles and functions, and empowering people to better fulfill the roles and functions assigned, working harmoniously with peers and forming teams. As for organizational structure, the precise definition of the structure supporting role and assignment of direct responsibility for each process and function is necessary. Finally, in terms of management, managers should be trained to make timely, accurate and translate into results leading to the achievement of organizational objectives decisions.

Coaching

Coaching has been defined over time in many ways, but in this diversity there are some essential elements to consider. According to the International Coaching Community (s / f), this tool aims:

> Help a person change in the way you want and help you go in the direction you want to go, (...) supports a person at every level to become who wants to be (...) promotes awareness, whom He wants to be and allows the change. Unlock the potential of a person to maximize their performance. Coaching helps them learn rather than teaching.
>
> The coach helps the client to achieve its best version of itself and to produce the results you want in your personal and professional life. Coaching ensures that the customer can give the best, learn and develop in the way you want. (S / p)

Additionally, the same source states conceptual differences between coaching and other tools, which bear some relationship, but they are definitely not the same. These differences are set with tutoring, counseling, therapy, training, consulting and teaching.

Specifically and as García-Allen (s / f), coaching is:

> (...) a methodology that gets the highest professional and personal development of people and influences in transforming them, generating changes in perspective, increasing motivation, commitment and responsibility. Therefore, coaching is a systematic process that facilitates learning and promotes cognitive, emotional and behavioral changes that expand the capacity of action in terms of achieving the goals.

This author also points out that there are different types of coaching, establishing the following types:

- Personal Coaching (also called Life Coach).
- Organizational Coaching, which is subdivided into Business and Executive, and
- Sports Coaching.

Personal coaching refers to the development of skills for daily living. In these processes, it is working from life projects and to achieve the necessary changes to achieve the objectives that people have charted strategies.

Executive coaching is aimed at senior executives of the organization. Seeks to develop leadership, management skills and interpersonal communication.

Business coaching is aimed at companies and organizations globally and not just executives. Developmental issues such as interpersonal relationships among workers, teamwork, productivity, customer satisfaction, and particularly the empowerment (Empowerment) are included.

These are the three types of coaching that are worth noting in this paper, because as will have been appreciated, certainly possible to influence the human capital of organizations.

Finally, according to the method used to advance the coaching (individual or group), we have the following types:

- Ontological Coaching: aims to improve the way individuals express themselves.
- Systemic Coaching: considers the person as part of a system. Identifies the impact of acts of the person in their environment.
- Coaching with Emotional Intelligence: Pursues autoregulation of emotions through self-knowledge.
- Coercive Coaching: It aims to motivate the individual and foster their sense of belonging to a group. It has created controversy by using radical and aggressive strategies. It is also known as "Healing Your Life", "Coaching inside", "Transformational Leadership", "Samurai game" or "Engineering the Impossible".
- Coaching NLP (Neuro Linguistic Programming): It helps modify behavior through the analysis of how the person interprets and faces reality (visual, auditory and kinesthetic it).
- Cognitive Coaching: looking for effective knowledge transfer.

Empowerment

We can see that the English names of some management techniques are conserved untranslated, this is the case Empowerment. Perhaps it is deemed commercially and psychological impact will be greater, or that the technique will have more credibility to be something "imported". Johnson (s / f), tells us about that:

> Empowerment means empowerment or empowerment that is the fact of delegating power and authority to subordinates and give them the feeling that they are masters of their own work.
>
> English "empowerment" and its derivatives are used in various meanings and contexts, but in Spanish the word is in conflict with a number of expressions that approach without achieving the fullness of the noun. "Empowerment" homologated

> with "empowerment" and "to empower" with "strengthen" while falling into disuse oldest expressions as "empowering" and "enable". (S / p)

This tool, which is considered strategically provides elements to strengthen the various processes within companies, allowing them to develop better conditions. Surge of Total Quality, and applied on models of continuous improvement and reengineering. In addition to making sense of teamwork and strengthen leadership, "allows the overall quality is no longer a motivational philosophy, from the human perspective and become a radically functional system." (Johnson, s / f: s / p).

In the process of training to promote the emergence and development of Empowerment in the organization, you should pay attention to the ability to:

- Support their peers.
- Participate in meetings.
- Get organized.
- Communicate ideas.
- Help in decision making.
- Evaluate differences.
- Control conflicts.
- Solve problems.

These skills to solve problems, contribute decisively to the formation of self-directed teams, which provide the following benefits:

- Better communication between employees and managers.
- Greater employee commitment.
- Positive change of attitude, from "having to do" one thing "wanting to do it."
- more efficient decision-making process.
- Increased satisfaction.
- Improved quality.
- Reduced operating costs.
- more profitable organization.

Benchmarking

This tool, also called Referential comparison, is quite popular not only practical but also effective. Business is to compare itself with competing companies, as well as other companies even other sectors, in order to detect and analyze their winning strategies, and if possible, apply them to the business itself. Obviously, the same applies to military, police, intelligence or counterterrorism organizations.

David T. Kearns, quoted by Entrepreneur (2012), who was director of Xerox Corporation, was one of the initiators of this concept and defined it as "the continuous process of measuring products, services and practices against competitors or those tougher companies recognized as leaders in the industry. "

There are five basic steps to efficiently implement this tool:

1. Know yourself. The organization should perform a SWOT analysis along with performance analysis. At this point you should make a planning about what is really expected from the benchmarking process, and what method will be to gather as much information as own the other companies, in addition to determining a budget and timetable. In a previous number of this magazine an example of how to prepare a DOFA matrix occurs.
2. Know your competition. It is very important to understand what works and what sector the leading companies in this sector are. further can select companies or individuals that advance good business practices that serve as an example.
3. Find your strengths. Once chosen the other companies in which the research will focus, it uses multiple pathways for information on these organizations, trying to detect what their strengths are and what their weaknesses. Focusing on the practices that make them industry leaders.
4. Apply it to your company. The information gathered in the previous points, should be analyzed, evaluating practices which can be effectively incorporated into the organization, even with accommodations. Organizational changes will be executed, should be extensively socialized with employees.
5. APPRAISAL. It is essential to constantly evaluate the result of organizational processes, particularly when new practices or strategies are implemented.

These five points must be repeated is steady, it is necessary estarse renovated to adapt to changes in the context and the market.

In conclusion

It happens that absorbs us everyday and everyday emergencies not allow us to spend much time on what is important. Roughly speaking, we can say that in terms of organizational activities necessary for the operation would merely tactical, and thought about or planned for the long term would be strategic.

In this vein, a manager can "manage" the day and be good at it, until internal circumstances, the environment, or market, become unwieldy or adverse organizational interests, and then he will miss not having managed thinking about the future. Of course no one can predict the future, but there are methods that allow scenarios such as the prospective project, through which we can prepare for the change in circumstances, or we can act proactively to changing circumstances.

Thus, in the context of intellectual capital (structural, human and relational), we must have policies, plans and goals, both tactical and strategic order. Tools such as benchmarking, Empowerment, Coaching and Organizational DNA allow us to improve the brainpower from the human, with an impact on the structural and relational. Clearly these tools are applicable to the security sector, defense and intelligence.

References

Entrepeneur (2012). What is benchmarking. I online resource, accessed 11 July 2018. Available at: https://www.entrepreneur.com/article/265507

Garcia-Allen, J. (s / f). 6 types of Coaching: the different coaches and their functions. Psychology and Mind. I online resource, accessed 20 July 2018. Available at: https://psicologiaymente.com/coach/tipos-de-coaching

Hernandez, J. and Gomez, D. (2010). An approach to the concept of management and administration applied to the discipline of nursing. I online resource, accessed 13 July 2018. Available at: http://www.redalyc.org/pdf/1277/127715324027.pdf

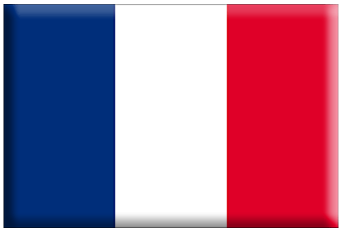
International Coaching Community (s / f). What is Coaching ?. I online resource, accessed 18 July 2018. Available at: https://internationalcoachingcommunity.com/es/que-es-coaching/

Johnson, Y. (s / f). Empowerment concept. I online resource, accessed 15 July 2018. Available at: https://www.gestiopolis.com/concepto-de-empowerment/

Lozano, O., Gomez, H., and buttered, I. (s / f). What is the organizational DNA? Online resource accessed 10 July 2018. Available at: https://www.forbes.com.mx/brand-voice/que-es-el-adn-organizacional/

France

13 Dragoons Parachutists



The 13th Parachute Dragoon Regiment (French: 13 Dragons Regiment Parachutistes, 13 and RDP) is a special reconnaissance unit of the French army. It is one of three regiments belonging to the Special Forces Command of the French Army, which in turn is under the command of the COS (Special Operations Command). It is based in Martignas-sur-Jalle.

Historical review

It is a unit of great tradition, the oldest in France. It was created by the Marquis of Barbezières Languedoc in 1676 as Dragoons (mounted cavalry). Then in 1791 he was appointed as the 13th Regiment of Dragoons. In 1936 the regiment became an armored body, then in 1952 become a recognition unit with airborne capability.
In 1956 the regiment was made up to the 25th Paratroopers Division, created in that year. In 1957 to the 10th Airborne Division he was transferred during the Algerian war. He was later part of the 11th Division Light Intervention. 13 and RDP became a recognition unit reaching. During the Cold War, the main mission of 13 and RDP it was to provide intelligence to the 1st Army, while each company of the 1st Parachute Regiment 1st Marine RPIMa provide intelligence for the Army Corps.
In April 1960, the French army in Germany decided to form an experimental intelligence company long range, the 7th Company Command, based on earlier work in Indochina and Algeria. The seventh company developed survival and recognition procedures to operate behind enemy lines. These methods and procedures and personnel are absorbed by the 13 e RDP. This led to 13 and RDP from 1963 formally to the task with current missions 'Patrol long range recognition'.

Finally, in 1968, the French army presented a plan for conversion of the regiment completely to his new task. Pending the creation of the new 1st Army in 1972, EMA decided to implement this plan, restructuring the regiment. 13 and RDP is available to the host to be used in Germany in case of war. The regiment was initially subordinate to BGRE (Brigade military intelligence and electronic warfare of the French army). Today, 13 e RDP is part of French Special Operations Command.

Since the end of the Cold War, the 1st Parachute Regiment Marine 1 e RPIMa became a direct action unit, while 13 and RDP specialized in reconnaissance / surveillance in hostile environments, gathering intelligence special operations. In a way, they are similar to the role of the Surveillance Long Range US Army. UU.

13 and RDP participated in the Gulf War. This was highlighted when three operators were captured by Iraqis in late 1990. On 13 and RDP was, along with other French units, heavily involved in the Kosovo War and used tactics and technology to force the Serb armored combat Army Kosovo Liberation allied forces and other outdoor, which facilitated its destruction by allied bombing, particularly by the United States air Force and the Royal air Force. 13 and RDP also contributed to the capture of Momčilo Krajišnik in 2001.

Mission

The mission of the regiment is to acquire human intelligence at any time and in any hostile environment (water, high mountains, equatorial forest, desert), behind enemy lines, using small autonomous and discreet, capable of positioning units close to acquire intelligence and transmit it to the allied forces. The troops are trained to use in their missions improvised means, but also the highest technology.

High-level skills and 13 RDP is special recognition, often makes it requested its support by other forces. The National Gendarmerie Intervention Group maintains a close relationship with 13 and RDP to train their gendarmes in advanced recognition and hostage rescue operations in hostile environments. The Équipes d'Observation in Profondeur (EOP, advanced control equipment) of the French artillery regiments used the standard operating procedures of 13 and RDP. The Regiment also works with the Direction générale de la sécurité extérieure (DGSE, French intelligence service).

Organization

The Regiment is currently comprised of seven squads, including three squads "search" or intelligence teams providing reconnaissance regiment. Two squadrons of long-range communications, providing a link insurance between teams deployed recognition and higher headquarters communications, and two squadrons of training, which are responsible for providing house training courses and certify new members of the unit.

13 and RDP is equipped with standard material of the French army, but has access to weapons and specialized equipment when necessary.

GESTIÓN DE RIESGOS
WWW.MASTERSECURITYCONSULTING.COM

MITIGA RIESGOS EN TU ORGANIZACIÓN

ANTES, DURANTE Y DESPÚES

IMPLEMENTA CONTROLES QUE REDUZCAN LOS RIESGOS

Auditorias e implementación de estándares en seguridad física, electrónica, de la información, realización de visitas domiciliarias, verificación de antecedentes, pruebas de lealtad, poligrafía pre-empleo y específica. Investigaciones.

MAS QUE CONSULTORES, SOMOS TUS ASESORES DE CONFIANZA

PREGUNTA POR LOS PAQUETES EMPRESARIALES Y KIT PYME TOTAL

contáctanos info@mastersecurityconsulting.com
+57 3165479295