

ISSN: 2538-9610 (on line)

TRIARIUS

Volume 4 - Issue 81



October 15, 2020



Prevention and Security Bulletin on
Terrorism and the New Threats





ISSN: **2538-9610** (en línea)
Medellín - Colombia
Volume **4** - Number **81**
October 15, **2020**

Editor

Douglas Hernández

Triarius Analysts

Ulises León Kandiko, Guadi Calvo,
Douglas Hernández.

This bulletin 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 Hernández
Medellín Colombia
Mobile: (+57) 321-6435103
director@fuerzasmilitares.org
hernandez.douglas@hotmail.com



EDITORIAL

How much do you know about strategic intelligence and its current trends? We invite you to review these issues by reading the interesting article by Argentine analyst Ulises León Kandiko, with which we opened this edition.

Next, our senior analyst, Guadi Calvo, also from Argentina, enlightens us about the situation in the Caucasus, and how what is happening there (and what could happen) affects Russia's strategic and security interests. Next, we present a brief analysis referring to the Colombian Marine Infantry and its future projection.

In his next article, Guadi Calvo enlightens us on the security situation in Central Asia, in relation to the different terrorist groups that operate there and that not only confront legitimate authorities, but also confront each other for territorial control, of the population and its resources.

We close this edition with a new contribution from Ulises León Kandiko, referring to Cyberwar. In this article, he presents us with a list of offensive-type operations, which allow negatively affecting enemies/adversaries, without the need to deploy conventional forces. The explanation is very interesting and uses real cases to exemplify.

As always, we hope that this material will be of interest and use to our kind readers. To whom we invite to make their contributions in the form of articles or analyzes on the topics that dominate. It is about making a productive exchange of information, that nourishes us intellectually and makes us be better in our functions.

Know to win!

Douglas Hernández

Editor



This newsletter has a Spanish version.

TRIARIUS 081

Content:

Strategic Intelligence. The Next Step, p.4
By Ulises León Kandiko (Argentina)

Caucasus: A little Libya on the Russian borders? p.7
By Guadi Calvo (Argentina)

The future of the Colombian Marine Corps, p.10
By Douglas Hernandez (Colombia)

A Caliphate in Khorasan, p.12
By Guadi Calvo (Argentina)

Cyber Warfare: A Decade of Learning, p.15
By Ulises León Kandiko (Argentina)



TRIARIUS

The number one issue of this magazine was published on February 1, 2017, so we are fast approaching a new anniversary. They have been years of experiences and learning, as well as growth in various ways. As an editor, it is my duty to read in detail each of the articles and analyzes that we publish, to offer our kind readers a brief review in the editorial, which guides you on what each edition offers you. Having read all that has enriched me with knowledge, but it has also made me very unhappy, because the more you know about the world situation, it is inevitable to feel overwhelmed, worried, and even hopeless. At this point, it is where I remember why we do it, what motivated us to create this specialized communication medium, and then everything makes sense again.

Triarius exists so that a group of good and useful people to society, belonging to the security, defense, intelligence, counterterrorism and cybersecurity sectors, exchange information in order to become stronger and continue doing good.

On the cover, ***Soldiers from Kenya.***
See more information at the end of the magazine.

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

Very special thanks to the international analysts who have sent us their articles for this issue free of charge.

Strategic Intelligence. The next step

By Ulises León Kandiko (Argentina)



Despite Covid19, the world continues to turn, some countries have almost resumed their usual cycle, be it good or not so good, some have once again reactivated their economies in an exceptional way, others have returned to not solving anything, but what certainly Powers and developed countries have not stopped doing is Intelligence.

Certainly, today Intelligence encompasses and operates more and more in sectors that we would never have thought of before and which we would consider completely outside its scope. Let's add to this that a particular combination of Strategic Intelligence, Geopolitics and Financial Analysis is being developed.

This is how we can visualize that there are currently three types of Intelligence transformations, namely, conceptual, technological and operational.

In the first case, it is a new and original Intelligence paradigm. It could be said that it is a mechanism based on the identification of the need for information - research - processing and analysis - dissemination - feedback, we move on to what some already call "position intelligence". In other words, we are arriving at an information mechanism that continuously perceives data and processes it, and then permanently and continuously disseminates it to those who have to use it.

Although the old Intelligence model was "positivist", that is, it was about unique objective and empirical data to be included in a decision-making process that is not determined by Intelligence, currently it is about building a continuous follow-up, not of data, but of political behaviors, perceptions of

reality by the enemy-opponent, as well as complex phenomena that constantly reach the Intelligence matrix from different parts and areas.

Although in the past Intelligence was rhapsodic and temporary, at the behest of politicians and, on occasion, even unsolicited, today it has become the stable nucleus of political, strategic, economic and industrial decisions. What obviously, generates as a result a new relationship between politicians and the Intelligence Services.

Although, in an era that we have already defined as "positivist", the facts, news and unknown novelties of the enemy-opponent counted, what matters today is the increasingly evident integration between the intelligence system and politicians.

Obviously, there is a danger that should not be overlooked, that is, the danger that, without even realizing it, the Intelligence Services assume responsibilities and roles that should belong only to elective bodies. But certainly, Intelligence plays a much more important role today than in the past.

Another key element of the conceptual transformation of Intelligence is the use not only of highly advanced and powerful information technologies, but also of scientific paradigms that we were unaware of just a few years ago. Let's think only of artificial intelligence, but also of cloud computing, algorithm theory and Markov chains, and here we limit ourselves to the mathematics that underpin current computing and technologies.

But there is also human ethology, an extraordinary evolution of Konrad Lorenz's animal ethology, as well as social psychology, sociological analysis, and

scientific depth psychology. There is no doubt that it should be used to analyze, for example, seemingly unpredictable mass behaviors, as well as the psychological reactions of both the ruling classes and the masses, and the interactions between the various group behaviors in a country.

Nothing to do with the old Kuk Evidenzbureau, which informed the Austro-Hungarian General Staff of the movements of the enemy troops or the mistresses of the different generals.

We are experiencing a substantial union between Intelligence and political decision-making or, better said, between the thought that Intelligence produces and the foundations of political decision-making.

In those old days of the Intelligence Services, we saw operations like the CIA often tried to poison Fidel Castro's beard. Today, beyond the dubious rationality of this operation, it would be a matter of using, for example, advertising, television series, Hollywood movies, the cycles of the sugar, tourism or tobacco markets, not to poison the beard of the late Fidel, but to put the Cuban economy and the decision-making system in structural crisis. This without prejudice to the ethical or moral that may result.

We can also infer that reality and facts have shown that the typical idea of the Anglo-Saxon political culture, according to which, once the "tyrant" is eliminated, everything can be fine and return to its place, has not given positive results. .

Another factor in the conceptual transformation of Intelligence is speed. We cannot be oblivious to the immediacy with which computer networks allow the collection of data in real time regarding facts and, therefore, favor wide-ranging decisions.

As far as technology is concerned, it is well known that both AI networks, new calculation structures, and networks to listen to and manipulate enemy-opponent data are such that they allow operations that were not even imaginable before. At this juncture, however, there are two problems:

- A. Everyone has the same tools available and therefore the danger of not "successfully completing" the operation is great, unlike when Intelligence Services operations were based on skills, role and dissimulation possibilities. of some operations, or in confidential and restricted technologies.
- B. The other problem is the manipulation of intelligence: a country that thinks it is a target can spread - in ad hoc networks - manipulated news, malware, data and information that are completely false, but plausible, and can modify the entire information system of the country. country under attack.

Another problem with current intelligence technologies is their distance from "traditional" political decision-making centers. A Head of State or a Minister must know what comes out of the Intelligence system. However, it is so specialized and sectoral that the distance between technical data processing and the "natural language" of policy is

likely to make the data ambiguous or unclear and of little use.

In addition, a purely conceptual factor must be pointed out: if we put together the analysis of financial cycles, technological change, public finances and political and military systems, we must connect systems that operate relatively autonomously from each other. In other words, there is no "science of the whole" that can meaningfully connect such different sectors.

Therefore, there is a danger of projecting the effects of one sector onto another that is little influenced by it, or of believing that, possibly, if the economy is doing well, public debt, for example, will also do well.

In this way, the space for political decision-making is much broader than modern intelligence analysts believe. Political decision-making is still shaped by history, political-cultural traditions, and perceptions of reality that are shaped by many years of psychological and conceptual training.

With specific reference to operability, once again we are facing radical changes. Years ago, there was the only "operative" who had to decide alone - or with very little support from "Center" - what to do on the spot and who to deal with. Today, obviously, he is still the operative individual, but he is connected to the "Center" in another way and, in any case, he imagines his role in another way.

At the level of political decision-making, Intelligence is always operative, because reality is so complex and technically subtle that it no longer allows even the most experienced statesman to "follow his nose." However, the main paradox of the problem is that Intelligence cannot assume political roles that imply a choice between equivalent options. This is inevitably the sphere of politics.

Another factor in operational transformation is the inevitable presence of intelligence operatives in finance, in the scientific world, in high-level business consulting, in advertising, communication and the media. Therefore, Intelligence has progressively demilitarized and is operating more and more in sectors that previously we would have thought were completely unrelated to the intelligence services. Instead, they are currently the central ones.

In addition, we are currently witnessing a particular combination of strategic intelligence, geopolitics, and financial analysis. Why the financial field? Because it is the most mobile and widespread economic function.

We are witnessing the birth of a new profession, monetary geopolitics. Therefore, we are also witnessing the evolution of two new types of Intelligence, namely Market Intelligence (MARKINT) and Financial Intelligence (FININT).

An old and new problem is secrecy. The greater the use of old and new intelligence, the less you will be able to keep secrecy, which is as essential now as it was in the past.

What has always been the objective of strategic intelligence? Predict phenomena from a given context. The contexts, however, change rapidly and

the interaction between sectors is such that the effect of the forecasts changes.

The formalized techniques for analysis - decision making are multiple: Intelligence data mining, "grid technologies", creation and exchange of knowledge, semantic analysis, key intelligence needs (KINS Key Intelligence Needs) and many others.

All of these operations are often necessary, but at present we must highlight two factors inherent to the culture of US intelligence that, unfortunately, also negatively affect the models used by US allies.

The first aspect is that, curiously, the same formal models are proposed for both companies and States. A state does not have to maximize profits, while a corporation does, at least on equal terms with its competitors. A State is not a "competitor" of the others and, ultimately, a State does not have a specific "comparative advantage" but, on the contrary, some of its companies do, if this happens. Therefore, the overlap between Business Intelligence, which is currently necessary, and State Intelligence is a conceptual bias, typical of those who believe that a State is, as Von Mises said, "the corporation of those who pay taxes" . For companies, it is obvious that all specific and original Intelligence operations must be

known by the State apparatus, which may or may not coordinate them, considering that they inevitably have additional data. On the other hand, some commercial operations can be very useful for Intelligence. Therefore, a structure would be needed to unite the two "lines" of operations and, above all, a new concept of Intelligence is needed.

In the past, the operations of the Intelligence Services were largely defensive: knowing something just before it happened, to prevent adverse operations of a State from affecting its own resources, but all this with often minimal time limits.

Now we need expressly offensive intelligence that can attack opponents' networks (commercial, economic and strategic) before they move and in due time.

These factual realities have an impact on all States, regardless of how large or small they may be, they are all part of the symphony of Nations and whoever knows more, will be able to proceed better, in a highly competitive, demanding world exposed to selfishness and intellectual miseries, whoever has the best Intelligence will be the one who can best position himself and give his citizens the best of a safe and prosperous world.

Image Source: <https://expresionesguerrero.com.mx/wp-content/uploads/2020/11/patrulla-1.jpg>

Ulysses Leon Kandiko

(Argentina) Degree in Security, graduated from the University Institute of the Argentine Federal Police. Professor of the IUPFA in the Security Sciences career, analyst, Director of Air Planning of the Ministry of Security of the Province of Buenos Aires. Specialist in cyberterrorism and criminal intelligence.

Caucasus: A little Libya on the Russian borders?

By Guadi Calvo (Argentina)



Fuente: Institute for the Study of War, junio de 2015.

A breath of hope had flown last Friday 9, when it became known that at the request of Russian President Vladimir Putin and after long telephone communications with Azeri President Ilham Aliyev and Armenian Prime Minister Nikol Pashinian, they had reached a high-level agreement fire, which would be effective from noon on Saturday local time or eight GMT (Greenwich Mean Time). For his part, the Russian Foreign Minister, Sergei Lavrov, met for more than ten hours in Moscow with his counterparts from Azerbaijan and Armenia, paving the way for talks on the solution of the Nagorno-Karabakh conflict, which would represent a new success of the Putin-Lavrov tandem, in international politics. The Russian minister reported that: "The fire will cease for humanitarian purposes, such as the exchange of prisoners and mediation bodies, according to the criteria of the International Committee of the Red Cross."

For Moscow, containing the escalation of the South Caucasus is essential for the relationship with both republics that have been part of the Soviet Union, since it has a security pact with Erivan and important economic and oil production agreements with Baku, in addition, during the Soviet interregnum, there were great cultural links between Russia, Azerbaijan and

Armenia, to the point that to this day the Azeri elite uses Russian as their habitual language, a practice that has also spread in Armenia. In addition, this country is dependent on Russia in the energy field, since it is not a producer of gas or oil, without becoming a relevant economic partner of Moscow, Putin continued to support the current Prime Minister Nikol Pashinian despite not have been his favorite.

On September 26, one day before the fighting began, the Russian military exercises *Kavkaz 2020* had ended, which this year had been carried out in the Russian North Caucasus in which Armenia had an active participation while Azerbaijan limited itself to observe.

The good news of the ceasefire was extremely short-lived, since, within minutes of its launch, Armenia accused Azerbaijan of bombing the areas near the city of Kapan, in the southeast of the country, with a population of around 150,000. inhabitants, where at least one civilian would have died. For their part, the Azeris rejected the complaint, which they classified as a provocation. At the same time, Baku blamed Armenia for bombing the Azerbaijani regions of Terter and Agdam during the night from Saturday to Sunday, violating the ceasefire agreement. The Azeris

said that at least nine civilians were killed and 30 others wounded, following missile attacks by the Armenian army on the city of Ganja, the city of Mingachevir, of about 110,000 inhabitants. While the pro-Armenian Nagorno-Karabakh separatist forces denied the attack on Ganja and claimed to be respecting the ceasefire. In addition to denouncing that Azerbaijani rocketry was fired at Stepanakert, the capital of the "Republic of Artsakh", a state not recognized by the United Nations, which intends to give a legal format to the disputed area, whose president Arayik Harutyunyan declared on Sunday morning that : "The situation in the region is relatively calm, with some minor fighting along the front line, but in a few minutes the situation could change."

Which takes for granted the failure of the Russian management, since a lasting ceasefire would allow the Kremlin to "elegantly" block Turkey's attempt to expand its influence in what it considers to have rights inherited from the Ottoman Empire, to which the president Turkish Recep Erdogan aspires to revive.

Erdogan's Mujahideen

The Turkish intervention in the conflict is not a secret for anyone, since not only for the assistance of arms and logistics, but also the sending of mercenaries of fundamentally Syrian origin, by Ankara to the Azeri-Armenian front.

Both Russian and Syrian intelligence sources assure that, since the beginning of the conflict, this traffic of fighters has continued to intensify, so it is a challenge for Moscow to deactivate any possibility that, in addition to the established purpose, fighting together with the Azeris against Armenia, they could generate a focus of conflict near its borders, encouraging the Chechen fundamentalists, who although they are deactivated, since most of their combatants were decimated precisely in Syria, where they went to fight as part of the anti-Bashar al-Assad Western entente. Although it is known, it is not necessary to reconfigure the old terrorist groups that are still alive in Chechnya and Dagestan. Nations that are part of the Russian Federation, with a large percentage of the *Muslim population*, which, as has already happened, could encourage those groups to once again start a war against Moscow.

It was learned that Moscow has detected several camps where Syrian mercenaries have gathered, after according to some unconfirmed information,

Russian aerospace forces fighter planes bombed those positions to prevent them from articulating as an uncontrolled force, generating in the Russian border a little Libya.

The same source insists that the Russian air strikes against the mercenary camps managed to destroy them, while hundreds of those fighters would have died.

This war will be for Russia a test of its pulse not only politically and military but also for its intelligence services, everything in the Caucasus was and to a great extent continues to be a hotbed of fundamentalist terrorism, fundamentally after the dismemberment of the Soviet Union and the disaster of Afghanistan, which gave the United States and Saudi Arabia an excellent opportunity to shake the waters of a new Russia, still anarchic and disorganized, which had not completely finished with its Soviet past. For this reason, and pushed by the *Wahhabi-North American alliance*, thousands of young people set out on the dream of building one or more *Islamic states in the Caucasus, with the Taliban Afghanistan as a model*. That cost thousands of lives and a monumental effort by Russia so that the darkest forms of *Islam* do not eat away at a fundamental part of its territory.

Nothing is known exactly about the more than fifteen hundred mercenaries that Erdogan has deposited in Azerbaijan, and how many of them may be elements linked to *al-Qaeda* or *Daesh*, so security must be raised to the maximum. Some experts in the region believe that some Chechen and Dagestani terrorist elements, including some exiles in Europe, may return to fight alongside their Azerbaijani "brothers", as happened in the 1988-1994 war between the that there was the unknown Shamil Basayev, who years later would be the head of the commando that stormed the *Dubrovka theater* in Moscow in 2002 and left 170 dead, most of whom were attending a sold-out performance of the play *Nord-O at that time*. st (Northeast) and became the supreme *emir of the group that, after his death in 2006, would become known as the Emirate of the Caucasus*, responsible for various attacks such as those on the Moscow and St. Petersburg subways.

Azerbaijan has a 400-kilometre border with Dagestan, a space wide enough for the Russian Confederation to allow a new Libya to be established on its borders.

Guadi Calvo

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



LISA Institute
Security Education

**Fórmate Online con Expertos.
Cuando quieras. Donde quieras.**



**+20%
DESCUENTO**

Código: *TRIARIUS20*

(Descuento disponible hasta fin de existencias)

CURSOS CON INSCRIPCIONES ABIERTAS

INTELIGENCIA

Curso de Experto en Análisis de Inteligencia

Curso de Analista de Inteligencia Especializado en Redacción de Informes de Inteligencia

Curso de Analista de Inteligencia Especializado en Sesgos Cognitivos y Esquemas Mentales

TERRORISMO

Curso de Gestión de Objetos Sospechosos y Explosivos

Curso de Asistencia y Tratamiento a Víctimas del Terrorismo

Curso de Análisis Interno de Procesos de Radicalización en Terroristas Yihadistas

Curso sobre Drones como Tecnología Dual: Seguridad y Defensa vs Terrorismo y Crimen Organizado

RELACIONES INTERNACIONALES

Curso-Certificado de Analista Internacional

Curso de Experto en la Unión Europea

**100%
ONLINE
INTERACTIVO
FLEXIBLE**



www.LISAINSTITUTE.com

The future of the Colombian Marine Corps

By Douglas Hernandez (Colombia)



Special Forces Unit, with Zodiac-type pneumatic boats and “submarine boats”.

The official information provided by the institution about its immediate future is as follows: “The Marine Corps of the National Navy is a highly trained and constantly evolving body, capable of adapting to current and future Colombian scenarios, seeking simplicity in its structures, the flexibility in its procedures, the improvement of its education and training, but always maintaining loyalty, the spirit of sacrifice and discipline as the fundamental pillars for the fulfillment of its constitutional mission that projects the capabilities of the National Navy in a scenario for in the year 2030 “to be a medium-sized marina with regional projection”, developing in a timely manner:

- The strengthening of amphibious capabilities for the defense of the nation and regional security focused on the coastal zone with dual tasks for the attention of strategic interests and the development of military operations with the purpose of neutralizing transnational threats. Additionally, the development of other tasks, among which are peace operations, humanitarian assistance and humanitarian demining, whose purpose is to materialize the institutional contribution to the challenges involved in the post-agreement and the consolidation of peace in Colombia.
- The defense of coasts whose obligation and commitment is the protection of strategic scenarios for the nation, such as the archipelago of San Andrés and Providencia, where the National Navy has been present since the 1960s. The institutional projection for the fulfillment of this task, is to acquire weapons systems for the defense of the coast, decisive to generate a strategic dissuasion that guarantees the integrity of the national territory.
- The fluvial capacity in the main rivers of the country and especially in the border rivers. This process will require proper planning and execution under the premise of guaranteeing the safety and control of navigation, contributing to the development of the country's maritime and river interests, in natural settings that become the sustainable strategic reserve for progress, growth and prosperity of Colombians from the regions.
- Strengthen the capacity of special operations, adapting it to meet the requirements imposed by the current situation in the country; that is to say, we are experiencing some processes of change, which require us to continue with the challenge of generating differential tactics and doctrine from the maritime scenario and grow within the requirements of the new national environment that the Armed Forces will face, particularly the National Navy and the Marine Corps. .”

PLAN 2030

The National Navy traced a strategic course, thinking about its harmonious development for the following decades. In relation to the marine infantry, the following objectives were presented. We can verify after reading this article that some of the points have already been specified, and more importantly, we can know what is to come.

At sea level

- Creation of comprehensive offshore security units.
- Creation of the Hydrocarbons Spill Emergency Response Brigade.
- Acquisition of amphibious capabilities-support of coastal populations.
- Increased participation in peacekeeping operations and international naval operations against transnational crimes.
- Strengthen international and regional cooperation in training and combating transnational crime.

at river level

- Creation of river coastguard units.
- Development of joint operations, to take the state offer to the most remote regions using the interior and border rivers.
- Creation of the national comprehensive river security system in support of the development of freight and passenger transport by river.
- Increase fluvial control in border rivers.

On land

- Creation of the Humanitarian Demining Battalion.
- Creation of the Disaster and Emergency Attention Company.
- Participation in regional and local development in support of the unified action of the State.

It is also important to note that, among the plans of the National Navy, is the acquisition of a large amphibious landing ship, to allow it the ability to project naval power to land in the execution of multinational operations, or if required by national emergency, catastrophe, or international conflict.

The Colombian National Navy, and in particular its Marine Corps, continue their evolution and development, committed to national and international security and peace.

References

<http://www.eluniversal.com.co/colombia/asi-sera-la-armada-nacional-en-2030-231543>

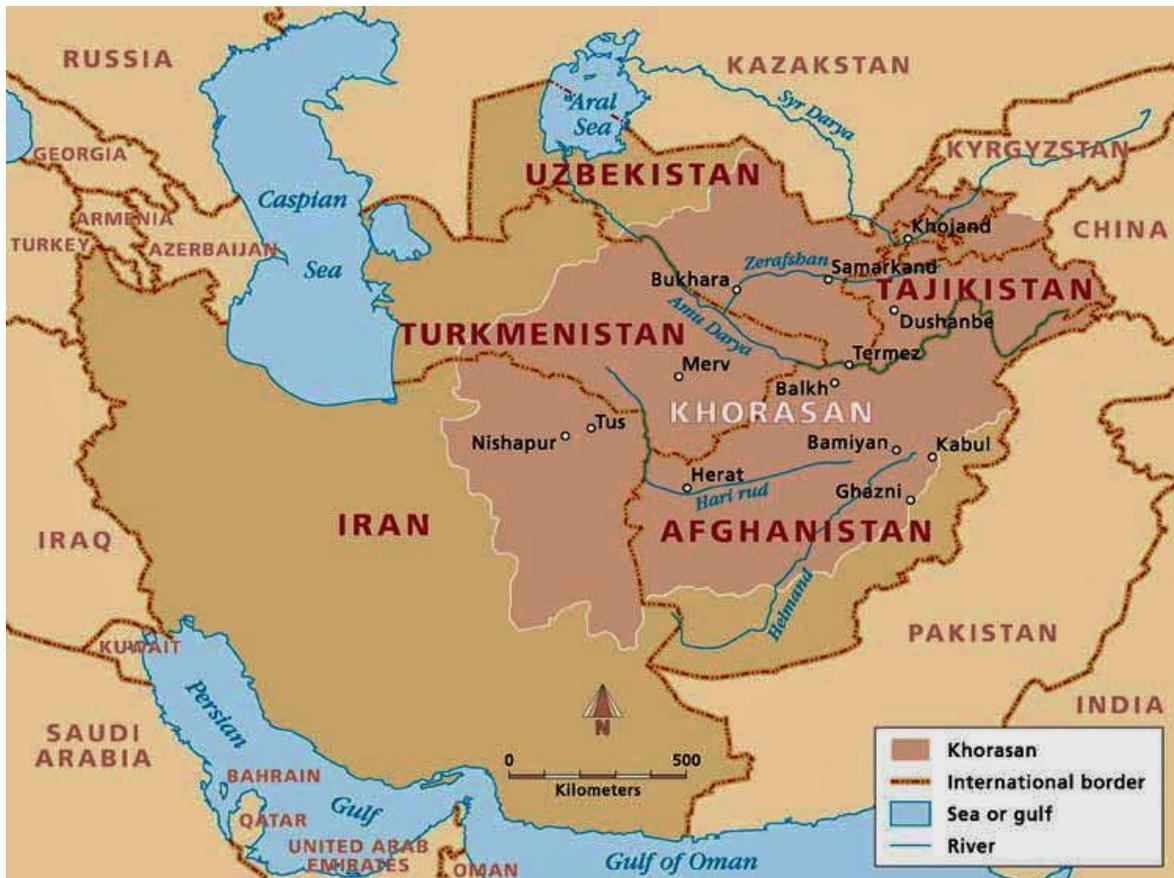
Image Source: National Navy.

Douglas Hernandez

(Colombia) Founder and director of the website www.fuerzasmilitares.org, he works as a journalist specializing in security and defense. He is a contributor to the Air and Space Power Journal -USAF's institutional magazine-, and to the Brazilian magazine *Segurança & Defesa*. He is a Sociologist and Master in Education from the University of Antioquia (Medellín, Colombia), a PhD student. He has a Diploma in International Relations.

A caliphate in Khorasan

By Guadi Calvo (Argentina)



In the face of the defeats that the *Daesh franchise* in Afghanistan is suffering after the attacks, not only by the United States and the *Afghan National Army* (ENA), but also by the *Taliban themselves*, who have never admitted other insurgent forces to their territory, with the exception of his historical *al-Qaeda allies*, the *wilāyat Daesh Khorasan*, as the group operating in Central Asia is known, is in retreat. Militiamen have stood out in its ranks, not only Afghans, but also foreigners, mostly Indians, Tajiks and Pakistanis, many of them veterans of the war in Syria and Iraq.

On April 4, the *wilāyat* suffered a devastating blow when Aslam Farooqi or Abdullah Orakzai, the *wali* (governor), was arrested. of the organization in Afghanistan since 2018, after the elimination of Abu Saeed Bajawori, by Afghan and US forces. The arrest of the high military chief, along with about twenty of his men, in an operation mounted by the *National Directorate of Security* (NDS), together with the CIA, took place in the southern province of Kandahar. According to the Farooqi *Taliban*, he was not

captured, but is under the protection of the Americans. This is not the first accusation by Afghan fundamentalists of collusion between *Daesh* and the *State Department*.

It was unknown that the organization founded by Abu Bakr al-Baghdadi was operating in Kandahar, an emblematic province for the *Taliban*, as it was considered his birthplace in 1994. What leads one to suspect that Farooqi, after being forced to abandoning his positions in the northeastern provinces of Nangarhar and Kunar, he sought safe refuge on the porous border with Pakistan, his country of origin.

Most *other Daesh emirs* or *walis Khorasan* in Afghanistan have died over the last two years, so this would have been one of the last blows to finish decapitating the group that, despite its enormous capacity for resistance, after enduring almost five years of constant siege from US bombing, Afghan army operations and ambushes by the *Taliban itself*, it would eventually have to abandon its main objective in Central Asia. What in Persian times was known as

Khorasan (land of the west or land of the sun) was made up of the current territories of Iran, Afghanistan, Tajikistan, Turkmenistan and Uzbekistan.

The defeat of the *caliphate* in Iraq and Syria has taken financial and logistical support from its various "branches" including the *wilāyat Khorasan* , to which it must be added that among the points agreed with Washington and the organization led by *mullah* Hibatullah Akhundzada, is collaborating with the fight against *Daesh* in the country, an issue in which the *Taliban* was focused from the beginning in which al-Baghdadi's group settled in the country.

The high command that accompanies the decision of the *mullah* Akhundzada knows very well that agreeing with the Americans will mean much agreeing with *Satan himself*, as they themselves have called the United States throughout these almost 20 years of war. So, it is logical to expect that some provincial middle managers will rebel against the agreements that their managers have signed in Doha last February with Donald Trump's delegates. The same thing they are doing now with the "puppets" of Kabul, as they have repeatedly called the government of President Ashraf Gani.

The *Daesh* understands that any defections from the *Taliban* could benefit them by swelling their ranks, so now more than ever resistance is key and for them and transferring their war to the former *Soviet republics* of the Afghan north is a great opportunity, because of the wide and permeable borders. With Tajikistan 1,210 kilometers, with Turkmenistan 744 and with Uzbekistan 137, countries where *Daesh* also has related groups that have been operating in those countries for years and where fundamentalism is deeply rooted after almost eight decades of "obscurantism, atheist and materialist *Soviet*".

From the war that the former Soviet Union waged against the Afghan *mujahideen* , supported by a gigantic entente in which the great Western powers participated with the United States at the head, which used the infinite economic resources of the oil monarchies of the Persian Gulf and a huge list of nations that included from Pakistan to Egypt, through Israel and a confused China.

The final outcome of that war and the dissolution of the *Soviet Union* , in most of the *Islamic* nations , from Nigeria to the Philippines, the fundamentalists financed by the Persian Gulf monarchies went all out, so the attack on the towers of New York, was not a beginning at all, but one more battle for *Allah* . The former *Soviet* republics of Central Asia have not been exempting from the phenomenon of the internationalization of the *Wahhabi* cause.

Therefore, the disbanding of *Daesh* in Afghanistan, the internal upheavals of the *Taliban* , which are beginning to show, for example with the offensive that they are developing in the province of Helmand, has set off the alarms since it could force them to interrupt not only the intra-Afghan talks, has been to further delay the US withdrawal from the country, one of the fundamental points of the agreement with the United States. For several days, areas near Lashkar Gah, the provincial capital, have been under attack, forcing the intervention of the ENA, with US air support, for which hundreds of families had to abandon everything and flee the area. Until Wednesday the 14th, *Taliban troops*, rebels at your command? they continued advancing towards Lashkar Gah, violating the commitment with Washington signed in February not to attack cities. Apparently, this operation had been decided before President Trump announced, as part of his re-election campaign, his willingness to repatriate all his troops before Christmas.

Takfirist imaginary , the fanaticism aroused by the new escalation between Azerbaijan, a *Muslim* nation , for the unredeemed territories of Nagorno-Karabakh against the Armenian "crusaders" and the state of volatility in which Kyrgyzstan finds itself, after civil unrest fueled by suspicions of electoral fraud, that have forced President Sooronbái Jeenbékov, this Thursday 15th to announce , make up an optimal scenario to activate the fundamentalist groups that operate in the region.

The Fergana Valley

With a size of 22 thousand square kilometers, as large as the Republic of El Salvador, and shared by Uzbekistan, Tajikistan and Kyrgyzstan, where the most conservative communities of those nations are rooted, organizations such as the *Islamic Movement of Uzbekistan* (MIU), *Jund al Khilafah* , the *Islamic Jihad Union* , have been established for years and having taken their oath of allegiance or *baya't* to al-Baghdadi, they would be a perfect place for *Daesh men* leaving Afghanistan to wait for a change in the situation in that country, that benefits them to return. In the Fergana Valley they have their "brothers" who will be able to supply them, give them shelter, logistics and men.

Many Uzbek, Kyrgyz and Tajik *mujahideen* participated in *Daesh* and *al-Qaeda* in Afghanistan and Pakistan, as well as in the war in Syria and Iraq. Perhaps the most relevant figure was former Tajik army colonel Gulmurod Khalimov, *the Islamic State's war minister*, who was killed in Syria in 2017.

The governments of Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan are evaluating the possibility of the return of their citizens who have survived the war in Syria and Iraq and can return to their countries to strengthen local terrorist organizations, since they have shown a high organizational level, it is estimated that some 5,500 Central Asians marched to war in the Levant, divided into some 2,000 Uzbeks, as many Tajiks, 850 Kyrgyz and 500 to 600 Kazakhs. Although most of them had been recruited outside their countries and were living in Turkey, Gulf countries and Russia.

Last April, German intelligence was able to disarm a network of Tajik *mujahideen* associated with Albanian cells, who were operating in North Rhine-Westphalia, to launch a major attack somewhere in Europe.

The *Katibat al-Imam al-Bukhari* (*Imam al-Bukhari Battalion*) by the religious born in the city of Bukhara, today Uzbekistan, in 810, mostly composed of Uzbeks. In the city of Aleppo they fought together with two Chechen organizations: *al-Muhajireen wal-Ansar* and the *Jamaat* belonging to the *Emirate of the Caucasus*, *Tawhid wal Jihad* also participated in that alliance, a group made up mostly of Kyrgyz.

All in all, the nations of Central Asia, with a spectrum of more than 70 million inhabitants, have not suffered major terrorist actions, in part due to the strict controls of the Russian advisers, what happened were sporadic almost individual actions and not part of orchestrated campaigns such as can happen in other nations where more structured organizations operate, which continues to be an incentive for dreams of a caliphate in Khorasan.

Image Source: https://en.wikishia.net/view/Greater_Khorasan



fuerzasmilitares.org
el portal militar colombiano

Cyberwar: A decade of learning

By Ulises León Kandiko (Argentina)



Cyberattacks, or Cyberwar, are not new in this environment, certainly a little over 18 years ago they are topics that I follow and try to understand and share with all of you. Back in the early 2000s, we witnessed the first global cyberattack with the release of ILOVEYOU, a computer worm that infected millions of computers around the world in an effort to steal passwords and allow its creator to access the Internet unintentionally. free. Over the next ten years, newspapers reported on China's infiltration of United States of America (USA) and United Kingdom (UK) defense networks, Russia's attacks on Estonia and Georgia, and denial-of-service attacks. of North Korea against South Korea.

But the truth is that it was not until the beginning of 2010 when cyberattacks, or "offensive cyber operations" (for the Armed Forces) really broke into the globe. The idea is to go over some offensive cybernetic operations during the last decade in order to recognize thematic objectives and see if there is something that the Armed Forces and/or Armies can obtain as a lesson learned.

While each of the case studies has its own lessons, they each share a key theme: they demonstrate that cyberspace is a central element of the battlefield, and effects launched from or occurring within cyberspace easily have an impact outside of cyberspace. of him, and from this comes, in my opinion, the importance of having a Weapon (branch) or at least a specialty in Cyberwar.

Offensive Cyberspace Operations: ESPIONAGE

Offensive Operations in Cyberspace can provide understanding by gaining access to sensitive information, bringing espionage into the digital age. This form of attack uses offensive cyber techniques to gain unauthorized access to systems and steal data for the attacker's purposes.

As with conventional espionage, many governments around the world have been implicated in some form of cyber espionage campaign. The most prolific offender, however, is almost certainly China, whose government has aggressively targeted others for the past decade and beyond. Its objectives have been twofold: first, to obtain intellectual property to pass on to domestic organizations and fuel China's economic growth, and second, to obtain sensitive information for intelligence and security purposes.

Both goals have an impact on defense: domestic economic growth allows for increases in defense spending, and information stolen by China can directly increase its threat. For example, China's stealth fighter program has benefited significantly from stolen F-35 research and development.

However, one of the examples of Offensive Cyberespionage Operations was the one known as "Cloud Hopper", it was carried out by China. Cloud Hopper was perpetrated by a group known open source as APT10 and linked to the Chinese Government Civil Security and Intelligence Agency of

the Ministry of State Security (MSS). The attack targeted managed IT service providers (MSPs - organizations contracted to provide and manage IT on behalf of others -) and exploited the legitimate access they had to their customers' systems and data. In doing so, the MSS was able to steal intellectual property from hundreds of organizations. The industries of those engaged organizations were closely aligned with China's 2016 five-year plan, and therefore the data they had was highly valuable for economic growth. This economic growth in turn made it possible to increase defense budgets: spending grew by 81% between 2010 and 2020.

In addition to demonstrating the usefulness of Offensive Cyberspace Operations in enabling espionage, the extensive theft of China's intellectual property over the past decade underscores the relevance of cyberspace to other arenas of conflict. The advantage gained in cyberspace can directly lead to an advantage in other domains; Conversely, insecurities in cyberspace (ie the failure of defensive cyber operations) can directly lead to insecurities in other domains.

Offensive Cyberspace Operations: FUNDING

The rich and interesting thing about the variety of Offensive Operations that can be carried out is that there are those that provide financing for other Offensive Operations, a kind of going out to find funds. This can be achieved in many ways, for example, by developing offensive cyber tools and licensing access to others for a fee, by holding organizations to ransom using offensive cyber tools (e.g. ransomware), or by using offensive cyber operations to carry out frauds. While these companies are typically the domain of criminal organizations, North Korea is an exception; the regime has targeted financial services institutions around the world to carry out a series of high-yield frauds over the past decade.

The largest fraud attempt or at least one of the most notorious fraud attempts from North Korea was the Bangladesh Bank robbery in 2016. In this operation, the attackers issued fraudulent instructions through the SWIFT interbank network in an attempt to steal almost a billion US dollars, of which they managed to obtain 81 million dollars. To do so, they compromised the Bank's internal network and instructed the Federal Reserve Bank of New York to transfer funds to four attacker-owned accounts in the Philippines, from where it was distributed to a network of other accounts.

FireEye, which is a cybersecurity firm, discovered that these cyber operations to generate money, linked

to the Reconnaissance General Office of North Korea, began just a year after the Security Council of the United Nations imposed sanctions that limited the access of the foreign exchange regime. Therefore, it is almost certain that these cyberattacks were planned and carried out to circumvent these restrictions.

There is no doubt that in addition to the economic return that this type of Offensive Operations represent, an added value is that they provide a real-world training ground for North Korean cyber operators, who can then attack government or defense targets with greater impact. However, the broader utility of Offensive Cyber Operations as a mechanism for providing covert funding to illicit groups and rogue states (and thereby bolstering their capacity) is evident, just as terrorist groups have historically relied on bank robberies and other forms of organized crime to finance their operations. As with China's cyber espionage, this shows how advantage in cyberspace can enable advantage in other domains.

Offensive Cyberspace Operations: INFORMATION

Offensive cyberspace can be used to support information operations and to influence populations and their decision making, I have extensively developed the topic in "DISINFORMATION: nothing new under the sun", but delving a little deeper, we see in the recent "Russia Report" by the Parliamentary Intelligence and Security Committee, Russia has used offensive cyber operations to support a broader campaign of information operations aimed at undermining Western governments and society. A high-profile example of this is his involvement with the US Democratic National Committee (DNC) and subsequent data leak in an attempt to undermine the 2016 US presidential election.

In this attack, Russian military intelligence (GRU – Main Directorate of the High General Staff of the Armed Forces of the Russian Federation) gained unauthorized access to the DNC network, compromising a large number of systems, including mail and file servers. The GRU obtained thousands of documents and copied them onto computers controlled by the GRU. Simultaneously, the GRU created the DCLeaks website to host the stolen documents, designed the personalities "DCLeaks and Guccifer 2.0" to publish them, and also passed the documents on to WikiLeaks. This operation was designed to undermine the American public's confidence in democracy and in Hillary Clinton, whom the Russian government believed would likely win the

presidency; both goals would benefit Russia's foreign policy.

It is more than clear that this type of use demonstrates how Offensive Operations in Cyberspace manage to achieve a strategic effect, both during the war (as was the Russo-Georgian war of 2008 to undermine public support for the Georgian government), as during the peace (with Russia undermining American democracy by attacking the DNC).

Offensive Cyberspace Operations: KINETIC EFFECT

Last, but not least important or plausible for that, there is a growth in Offensive Cyber Operations in which they can be used to achieve kinetic effects and to replace, although today it would be more to complement or accompany, conventional military operations. This could include the denial, interruption or destruction of property or physical harm to persons. In fact, the UK Defense Secretary stated in June 2020 that "cyberattacks are just as deadly as those faced on the physical battlefield."

The kinetic effects that have been seen may be unintentional or an indirect consequence of a broader attack. For example, the 2017 "Wannacry" cyberattack infected 1,220 UK National Health Service (NHS) medical teams; while the National Audit Office's after-action report did not identify any direct harm to individuals, the resulting cancellation of thousands of appointments likely caused indirect harm. However, the NHS's goal in this attack was likely incidental, and the North Korean attackers' motive was monetary.

There are also documented examples of Offensive Cyber Operations that have intentional kinetic effects. Security researcher Matt Wixey talked about this in his

DefCon 27 talk, citing examples including: near real-time malware manipulation with CT scans to add/remove evidence of lung cancer, attackers sending animations designed to trigger photosensitive epilepsy to web forums and hacking pacemakers to withhold or add downloads and cause heart problems.

One usually saves the best for last, like dessert, so we can say that perhaps the most notable example of a cyberattack causing a kinetic effect is Stuxnet. First discovered by security researchers in 2010, this joint US-Israeli attack likely began in 2008 and was designed to degrade Iran's nuclear enrichment program. It did so by initially infecting five Iranian companies linked to the program and moving via USB drives to eventually infect systems at Iran's Natanz nuclear power plant. Once these systems were infected, Stuxnet caused around 1,000 centrifuges (used to enrich uranium for power generation and nuclear weapons) to spin outside their designed limits and fail. The failure of these centrifuges temporarily deprived Iran of around 20% of its total uranium enrichment capacity, causing delays in the broader nuclear program, all without the use of any conventional force.

While the other examples we looked at in this article have focused primarily on Offensive Cyber Operations as an enabler, Stuxnet demonstrates how Offensive Cyber Operations can have direct kinetic impact and project power globally without deploying forces. As offensive cyber capabilities continue to develop, it is very likely that more examples of these will emerge that have a direct kinetic impact, as well as an increase in the impact of these operations.

The battlefield has not changed, but has simply increased, just as it was once extended to the air battlefield, today the cybernetic battlefield is a fact that requires Generals and Politicians with a clear and clear awareness of its existence. and imprint.

Image Source: https://cincodias.elpais.com/cincodias/2016/06/23/sentidos/1466709895_593659.html

Fuerzas Antiterroristas del Mundo

Arduentes Fortuna Iuvat



Kenyan soldiers facing a terrorist attack in Nairobi's hotel zone.

Kenya Special Operations Regiment



The Kenya Special Forces are relatively new to the Kenya Defense Forces (KDF). The largest of these units is the *Special Operations Regiment (SOR)*. The SOR is made up of three Battalion-sized units, these are the 20th Paratroopers, the 30th Special Forces, and the 40th Rangers Strike Force.

The Special Operations Regiment has been used intensively since its creation. For example, they have been active in Somalia for several years.

The SOR Special Forces operators are highly trained and equipped with the best that their Armed Forces have available. The training is taking place in Kenya, receiving advice and training from allied forces from the United States, the United Kingdom, Jordan and Belgium.

While the SOR is the best-known Special Operations unit in Kenya, it is not the only one.

- The naval force of this African country has the Kenya Special Boats Unit (KSBU), which has been trained by personnel from the United States Navy (SWCC). The KSBU goes through a full training course that includes combat medicine, navigation, ship handling, weapons proficiency, and ship boarding procedures. Part of the training takes place at Manda Bay.
- The Kenya Air Force established as of 2016, a unit intended to operate behind enemy lines, to carry out the recovery of personnel. This unit receives training from the United States Air Force and is headquartered at Nanyuki Air Base.

- The Police of this country has the so-called General Services Unit (GSU). The GSU has been in existence for many years and is heavily involved in counter-terrorism, civil disorder, and special operations.

The men who captured Badhadhe came from the KDF's Special Operations Regiment (SOR), which includes troops from a variety of Kenya's best units, whose numbers have increased since 2011.

While most of its operations remain classified, SOR operators have been used more aggressively in recent years.



Kenyan Special Forces operative

"Our revolution started with Somalia," a commanding officer of one of the elite units told the *Sunday Nation*, *speaking in confidence*. Elite soldiers train to track down a target and take it down undetected. They are highly trained, well equipped, and are experts in weapons, intelligence gathering, and battlefield medicine.

Before the start of the Somali War, the 20th Kenyan Army Paratrooper, who rushed to the rescue of besieged KDF troops during the El Adde attack, was the only known unit of Kenya's elite forces. Today, others that make up SOR are the 20 Para, the 40 Rangers Strike Force, and the 30 Special Forces.

Since October 16, 2011, the day Kenyan soldiers crossed the border into Somalia, the elite forces have grown in every conceivable way, from funding and personnel to deployment.

A senior officer, a War Studies graduate of King's College in the UK, says greater use of special forces is needed because traditional approaches to deterrence have become inadequate. "Special operators are trained to implement unorthodox alternatives to missions, especially in a war where it's extremely frustrating to tell a civilian from a combatant," he says.

According to Special Operations Regiment sources, the elite forces were initially deployed alongside almost all battalions. But in subsequent years they have been sent for specific missions in Somalia.

For example, on the morning of May 29, 2015, elite forces carried out a two-pronged assault on the Bula Hawo district.

The increasingly robust presence of special forces, including within Kenya's borders, has been fueled by a sharp rise in demand for unique expertise in unconventional warfare and counterterrorism. Nowadays, most of the special forces can reach most of the towns, cities and even villages in Kenya.



Kenyan soldiers in training.

They are the protectors of Nairobi, the people of the Boni Forests in Lamu County, and the herders of Northern Kenya. They are tasked with identifying risks and providing advice to government officials on the ground to bolster local security capabilities and reduce the likelihood of full military interventions.

The elite forces are also tasked with beefing up security for the president and other foreign dignitaries when they visit the country, including when US President Barack Obama arrived in Nairobi last year. Despite their increased presence in the country, the elites still prefer to work under the radar.

Long Range Surveillance Team

Another unit is the Long-Range Surveillance (LRS) team which is very secretive. Its men and women carry out difficult long-range secret military missions, often in small units. The objective includes gathering intelligence behind enemy lines. Missions involve tracking down and identifying enemy camps for bombing or special forces attacks. The unit can also be used to track down high value enemy operatives for elimination or intelligence gathering purposes. These are the guys who are trained to do long-range surveillance patrols in small units. Teams typically conduct missions on foot and have to perfect the art of camouflage in all types of terrain to avoid enemy patrols in a hostile area. The goal is always to get to the heart of the enemy. A logistics center, an armory, a camp of particular importance to the enemy, the residence of an enemy commander, the location of enemy units, their size and strength.

LRS missions are often physically and psychologically exhausting and only the best are deployed. Units report back to headquarters using radios, satellite phones, photographs, GPS transmitters and laser pointers for drones or helicopter gunships to locate them. The units provide accurate information for KDF rangers, special forces and long-range artillery units. These units fulfill the function of locating the Al Shabaab camps within the extensive boni forest. LRS tactics have served militaries well around the world, including Israeli, American, Russian, and UK special forces.

KDF personnel from the elite forces pride themselves on being among the best trained and equipped on the continent. During a recent joint training with the Jordanian Rapid Reaction Force, a military source said that the Jordanians were taken aback by the superior skills of the Kenyans.



Kenyan soldiers on a motorized patrol.

Most of the specialized teams were trained by Americans and British. Before the US Congress and UK Parliament pressured their governments to declare how much their countries were investing in and equipping Kenya's elite forces, the information was kept from the public eye. In 2018, the US and UK presidents have committed to military cooperation with Kenya, especially in the area of training, counter-terrorism, countering IED threats and cyber operations. The forces of the two countries conduct regular joint training exercises with the KDF.

According to several Western sources, who spoke to the *Sunday Nation* for a special report, US special operations forces have played a crucial role in infrastructure investments for Kenyan special operations teams. Military support has also included the establishment of a school for rangers.

Ranger force

In 2009, a Kenya Defense Force (KDF) captain led a six-man team to the US Army National Guard (ARNG) Combatant Training Center at Fort Benning, Georgia. His mission was so secret that not even his closest friends in the military knew about it, and his arrival on American soil on August 8, 2009, was the second time in as many years that Kenyan soldiers had gone out for specialized ranger training .

Those six members of the elite mission would, months later, pioneer the Kenya Pre-Ranger Program. "We hope to develop a specialized unit that can respond to the country's immediate threats," the Captain told the US National Guard newspaper. When they returned, the US established and supported a Ranger Strike Force (RSF), but its training and operations remain a closely guarded secret.

Around the same time, another elite unit, the Special Forces (SF), was established, forming Kenya's first Special Operations Force. The team, known as the Special Operations Regiment (SOR), is made up of the Rangers Strike Force - identified as 40RSF - and the Special Forces (SF) - known as 30S. Both RSF and SF were relatively unknown until Operation Linda Nchi was launched and they were deployed for special operations in Somalia.

Their performance on the front lines of the war was so brilliant that President Mwai Kibaki, during the Jamhuri Day celebrations, and as Commander-in-Chief of the Armed Forces, rewarded several of the outstanding fighters. Among those honored with a Silver Star (SS) was Captain Boniface Waithaka, Officer Commanding (OC) of the Ranger Company which was then headquartered in Belesc Qoocani, Somalia.



Urban patrol in anti-terrorist operation in the Kenyan capital.

Training

Gilgil Barracks, located approximately one kilometer from the city of Gilgil, is the home of the special operators. And, to join the happy little family here, you must be outstanding in the military field. Members of these elite units are selected from the best of the best after blackouts, and immediately begin to be evaluated for stamina, stress management, and resourcefulness.

The Ranger Strike Force takes 63 days to train with regular exercises after deployment, while training for Special Forces takes six months. One of the main differences between the two is that the Rangers are trained by Americans and the Special Forces by the British.

Contrary to popular belief, the Special Forces are not a rapidly deployable unit; the secret of its success is intensive preparation. They are well versed in details about power grids, water supplies, farming, economics, roads, and local politics. They plan, discuss, and rehearse combat and follow-up operations.

During training, the Rangers spend three weeks in Isiolo, three more in the high-altitude region of Mount Kenya, then move to the wet coastal military base at Manda Bay. They train alongside British Commandos, US Army Rangers and Special Forces personnel in and out of Kenya.

Some of the training activities can traumatize even the bravest. According to KDF sources, they are trained to keep fighting without retreating and remaining flexible even in the harshest conditions. Their training carries lessons of survival, exposing the men to pressure and suffering, while making them masters of disguise, deception, and sabotage.

Special operators are also specialists in the fight against terrorism; urban, desert, mountain and bush combat; and the handling of a wide range of weapons, from light infantry weapons to heavy artillery.

Several of those serving in Somalia have received training from the US 3rd Special Forces Group in weapons and tactics, first aid, hostage rescue operations, map reading and navigation, field craft, humanitarian operations, escort and VIP protection, swimming and personal defense.

Kenyan Special Forces are also being trained by British Navy Commandos in Counter Insurgency Operations (COIN), Operations in Built Up Areas (OBUA) and sniper training, including stalking, long-range marksmanship,

observation skills, camouflage and concealment, intelligence gathering from observation posts (OPs), and counter-sniper exercises.

Others are flown to various locations around the world where they conduct intelligence gathering, surveillance, target acquisition, and reconnaissance training in a jungle setting.

"Several of the recruits do not complete the training due to injuries sustained in the course of training, lack of stamina, negative attitude towards training or not following instructions," said a Special Forces member who asked not to be identified.

American Support

According to leaked diplomatic cables, the United States decided to support a new elite unit after concerns were raised in the US Congress about the development of the parent unit at the time, the 20th Parachute Battalion. The Kenyan unit was alleged to have committed human rights violations during Operation Okoa Maisha on Mt Elgon. The same unit was also accused of further violations during the deployment to Mandera.

"In 2003, at the request of the Kenyan Ministry of Defense, the United States began assisting in the development of military units capable of responding to cross-border security challenges," read a cable sent from Nairobi to Washington.

"The development of the land force has focused on two types of units; conventional army infantry and an elite Kenya Army Special Operations Force/Strike Force Rangers."

The United States is using permanently attached personnel from its Special Operations Command Africa (SOCAF) to train RSF. In 2005, US Special Forces conducted basic infantry training through various joint combined exercise training events with approximately 99 RSF soldiers.

Initial plans called for the establishment of a 900-man KSOF battalion in Gilgil by September 2011, but not everything has gone according to plan due to the Somali incursion.

According to the plans, the unit was supposed to consist of 450 front-line soldiers organized into three companies, with an additional supporting company, the battalion, a headquarters company, a heavy mortar platoon, a reconnaissance platoon, and a platoon. antitank.

Kenya also intends to expand training to the Air Mobile (helicopter) and Air Assault battalion. His predecessor was the Kenya Paratroopers. Within the army, the unit is known as the "green berets" or the "paras". Your work and activities are classified.

Along with the Recce Company of the General Service Unit, they played a major role in putting down the 1982 coup plot when they escorted Moi back to Nairobi from his home in Kabarnet. The "paras" have a secret division known as the D 20th Company Paratrooper Commandos.

This unit is said to be a replica of the famous elite British unit, the SAS. The 20th Parachute Battalion had a Ranger Strike Company, and it is this unit that became the current Rangers. The 20 Para and Special Operations Regiments are considered as the army commanders' reserve and therefore can only be deployed with their consent.

Each Special Forces soldier, a highly skilled operator, is taught to train, advise, and assist the host nation's military. Traditional Special Operations Force unit missions include Unconventional Warfare (UW), Direct Action (DA) and Close Target Reconnaissance (CTR).

Operations

Unconventional warfare is a broad spectrum of military and paramilitary operations carried out in politically and socially fragile areas, and its activities include guerrilla warfare, evasion and escape, subversion, sabotage, and covert or clandestine operations. low visibility.

Direct action involves capturing, damaging, or destroying a target, while close target reconnaissance involves operations behind enemy lines, to provide the theater commander with intelligence on the enemy, or gather information about their terrain and population.

In general, these elite forces are equipped with advanced equipment such as tactical satellite communications, high-frequency radios, global positioning systems, and medical kits. Its operations are aimed at interdiction, survival, evasion, resistance and escape and water infiltration.

In Somalia, the Special Forces were deployed in the cities of Kolbio, Baadade, Kismayu and Burgabo, while the Rangers were deployed in the port cities of Kismayu, Baadade and Beles Coqaani.

Kolbio is said to be on the shortest route to Kenya from Kismayu, while Baadade is a strategic deployment to stop raids from behind. The FS has been primarily involved in reconnaissance and infiltration missions, while the Rangers are used as an elite quick reaction strike force. In the battle for Kismayu, units were positioned on the objective before the rest of the battle group using inflatable boats.

In addition to weapons and close combat skills, the commandos are trained to parachute from aircraft at 800 feet both day and night, using night vision goggles with little or no assistance.

All the female soldiers who have tried their luck in the Special Forces have retired after failing to withstand the rigorous training.

Only 25% of those who volunteer to join the Special Forces graduate after two years of training.





TRIARIUS

Por un mundo más seguro, estable y en paz