INVISIBLE DOG
INVESTIGATIVE JOURNALISM
ISSUE # 51 MARCH 2016
www.invisible-dog.com invisibledog@email.com

SYRIA: THE SAUDI GAMBLE

The Syrian battleground is so crowded that it is difficult to understand who is fighting who. On one side, Russians and Iranians are supporting Bashar al Assad's troops, alongside with Lebanese and Iraqi Shia volunteers and the Hezbollah. On the opposite front, there are a myriad of group that include the Free Syrian Army and Salafi formations like Jabhat al Nusra, Jaish al Sham, Jaish al Suri al Hurr, Suqur al Jabal, Ansar al Sharia, Ansar el Din, Ahrar al Sham and so forth.

Are they all united against Assad? Not necessarily. Some of them fight on behalf of their sponsors, be they Saudi Arabia, Turkey or Western powers. Others instead, like Jabhat al Nusra, are affiliated with Al Qaeda and are on a collision course with the ISIS. The Syrian kurds from the YPG, the military wing of the Democratic Union Party, don't fight Assad, but do against the ISIS. There are then the Iraqi Peshmerga, who also fight against the ISIS but are not in good terms with the YPG. Syria is the typical scenario of everyone against everyone. What happens on the ground is similar to what happens in the skies. The Syrian airspace is currently occupied by the Russians, Syrians, US and other nations.

In such a chaos, there was really no need for Saudi Arabia to announce its intention to send ground troops into Syria to fight terrorism. The initiative, still lacking details, will either see a direct Saudi commitment or the deployment of units from the so-called “Islamic NATO”. In the latter case, the risk of a sectarian struggle between a predominantly Sunni coalition and the Shia could become a reality. In fact, it is unclear whether the Saudis intend to actually fight terrorism, or prevent Iranian expansionism.

The fear of Iran

Saudi Arabia fears the rise of Iranian influence and Teheran stretching its tentacles from Baghdad to Damascus and all the way to Beirut. It all began with the agreement on Iran's nuclear program and the green light for the Ayatollah's regime to return on the international scene in the role of regional power. The fact that the deal was brokered by the United States has pushed the Saudis to get involved in Syrian affairs. Riyadh feels it has lost the uncritical support of the United States. Furthermore, US President Barack Obama has made it clear that he does not intend to send any troops to quell the unrest in the Middle East. This has put Saudi Arabia in a vulnerable position. In the light of these circumstances, the reign of the Saud, known for its quiet diplomacy and prudent foreign policy stances, has become interventionist and militaristic.

It is unclear whether such a bellicose attitude can be solely attributed to the King's son and Minister of Defense, Mohammed bin Salman. He is definitely trying to gain the spotlight in a crowded royal court and attempting to be perceived as the man for the future. Doubts remain whether such an attitude is borne out of fear or unscrupulousness. King Salman's Saudi Arabia is already involved in the conflict in Yemen, it is ambiguous when it comes to fighting Islamic terrorism and the support given by Saudi Wahabi organization to Salafi groups and is affected by an encirclement syndrome that consciously mistakes theocratic aspirations for hegemonic ones.

The Syrian gamble

The decision to deploy troops in Syria is definitely both a political and military gamble. Saudi Arabia is like a poker player. They sit at the table and keep on raising the stakes although they don't have a good hand. But bluffs don't always succeed in the Middle East. If what they intend to do is to counter the Iranian military support to the Assad regime – and thus expect to dictate the conditions during the talks in Geneva – they definitely have to think twice about putting their boots on the ground, either directly or together with a coalition.

Despite the statements from the Saudi Minister of Foreign Affairs, Adel al Jubeir, on the future of Assad, little will change for the Saudis if the new ruler in Damascus is supported by both Russians and Iranians. Furthermore, the Saudi initiative adds more international players to an already crowded conflict zone; it creates the conditions for a war that could spill over the geographical boundaries of Syria and involve the entire region. The Russian Prime Minister Dimitri Medvedev has already spoken about the risk of a “total war”.

If the Saudis lead the way, it will be interesting to see who will follow them in their adventure. Of the 35 countries member of the “Islamic NATO”, quite a few will turn the offer down. If Riyadh will possibly rely on the countries of the Gulf Cooperation Council, with the exception of Oman, Egypt will quite surely keep away from the Syrian quagmire. Cairo opposes the intervention in Yemen, does not have a good relationship with Turkey and is already fighting terrorism at home, both in the Sinai and in the areas bordering Libya and the Gaza Strip.

A premeditated escalation

The tensions with Teheran date back to 1979 when the secular monarchy of the Shah was overturned by a theocratic regime similar to the one already existing in Saudi Arabia, where the Saud dynasty relies on the support of the Wahabi clergy. Since then, the bilateral relationship has been a struggle for the leadership in the region, both political and religious. Proxy wars were fought, like during Saddam Hussein's war against Iran with Saudi funding or, more recently, in Bahrein and Yemen. The conflict might now evolve into a direct confrontation.

The escalation was not a coincidence. The execution of Saudi Shia cleric Nimr al Nimr was a deliberate and carefully considered decision. Over the past weeks, 32 people, in majority Shias, were put on trial in Saudi Arabia for espionage in favor of Iran. This is an unprecedented decision that puts more strain on the bilateral relationship between the two countries, presently suspended following the attack on the Saudi embassy in Teheran. The last piece of the puzzle is the designation of the Hezbollah as a terrorist group by both the countries in the Gulf and the Arab League. After having cut its financing to Lebanon, the Saudis have already chosen which terrorists they intend to fight in Syria.

In the light of such a chain of events, any commentator should ponder where the advantages and disadvantages lie and evaluate the risks. Are the Saudis using a bellicose strategy to attain a strategic objective? What if they are just showing their muscles for the sake of internal and international propaganda? If so, why announce the deployment of troops within two months? Such a timetable is incompatible with the ongoing military and political developments in Syria. Hence, even announcing the intention to deploy could amount to sheer carelessness.

Out of time

In concrete terms, putting together and deploying a military coalition would require at least twice the amount of time estimated by the Saudis. An operation abroad requires thorough planning, logistics and, given the participation of other countries, the definition of procedures, operational integration, a common command and control system, rules of engagement and so forth. Furthermore, several countries are presently involved in Syria. Some may be considered “friendly”, others “hostile”. You need to coordinate your actions with your friends and avoid clashing with your enemies. And this is not easy to do.

The prelude to what may happen took place from February 14 to March 10 during the joint military exercise in the north east of Saudi Arabia. Boasting the name “Thunder of the North”, it saw the participation of 150 thousand troops, over two thousand airplanes and 20 thousand tanks coming from about 20 Arab or Islamic countries. Units from Pakistan, Turkey, Egypt, Sudan, Jordan, Kuwait, Tunisia, Malaysia and Morocco carried out the dress rehearsal of the hypothetical intervention in Syria. At the same time, Saudi airplanes are being deployed at the Incirlik airbase in Turkey.

Chances are the Saudi gamble could be part of a strategic plan being carried out together with Turkey. Both countries oppose Assad, both fear Russian and Iranian expansionism, both want to dictate the conditions on the future of Syria. There are only two ways into Syria: from Turkey or from Jordan. However, as several analysts have underlined, the issue is not getting into Syria, but getting out.

ESPIONAGE KNOWS NEITHER FRIEND NOR FOE

It is certainly wrong to perceive as foul play the intelligence activity carried out by an Agency against a friendly counterpart. It is in the nature of intelligence agencies to obtain information on anything that can be considered newsworthy to their national security. Such an activity does not foresee any limits, does not distinguish between friends or foes and is carried out by all means necessary. If this were not the case, policing would be sufficient. Apart from national security, there is another parameter at play in the world of intelligence: It's not ethics, but self-interest. That is, Agencies can collaborate if their interests collide, but they could also be on opposing sides if they don't.

Such a circumstance postulates that the idea of a unique European intelligence agency is, to say the least, extravagant. What the European Union can do is incentivize a stricter collaboration between Agencies on specific topics, knowing that national interests will prevail over the ones of the community of States. It is in this context that Europe is possibly thinking about the creation of a coordination mechanism to tackle terrorism. The point is that States will share only what they want. There will be no automatism. So, apart from Europol and its police coordination activities, little will be done in the intelligence sector.

This premise helps explain why we should not be surprised or angered to hear the United States tapped the communications of Chancellor Angela Merkel, UN Secretary General Ban Ki Moon, Brazilian President Dilma Roussef, alongside side with Japanese politicians, the governor of the Central Bank, Haruhiko Kuroda, and corporations such as Mitsubishi. On the Italian front, former Prime Minister Silvio Berlusconi was intercepted together with his closest aides. The National Security Agency (NSA) has a representative in Rome, it has two listening posts managed by the Special Collection Service: one in its embassy in the Italian capital and another one in its Consulate in Milan. Both are well known to Italian security services. To seem surprised, seek explanations or recall the ambassador is just part of the comedy.

It should also not come as a surprise that a former Bundesnachrichtendienst (BND), the German Federal Intelligence Service, agent is on trial in Monaco for selling secrets to the CIA. The same happened to Israeli spy Jonathan Pollard that worked for the Mossad. He spent 30 years or so behind bars in the US before being freed in November 2015. Despite Israel's insistence, he is still not allowed to leave the United States because the Americans feel “betrayed” by a friendly Agency.

They are such good friends that, since the year 2000 and from the island of Cyprus, British and Americans were spying on Israeli drones and airplanes. Their communications were tapped from a base in the middle of the Mediterranean. The interception program came in handy when Tel Aviv pondered whether to strike Iran to sabotage the talks on its nuclear program. When the news came out, Israel said it was “disappointed”, but not surprised, as we all know the US listens to just about everyone.

The bottom line is: we may not like our friends spying on us, but ethics and sovereignty miss the point. And we always have to keep in mind that this is an open competition: sometimes you're the victim, sometimes the aggressor. Once you spy on, the next you're spied upon.

No one can claim to be innocent. German resentment against the NSA was short-lived. A report from the Der Spiegel magazine exposed how the Germans were listening on the communications of foreign embassies on their soil from Sweden, Italy, the Vatican, Switzerland, the United States, Portugal and France. NGOs such as Oxfam and the International Red Cross were also targeted, along with the US, Polish, Austrian, Danish and Croatian Ministries of Interior. Everyone was under the spell of the BND. In other words, what the CIA and NSA did to Merkel, the Germans did to their friends. An NSAgate followed by a BNDgate.

This entire sequence of events illustrates how global intelligence networks work. The NSA used the Bad Aibling base given to them by the Germans for its electronic espionage. From Bavaria, the radars intercepted communications to Syria, Iraq, Libya or Afghanistan. At the same time, the NSA used the same facilities to tap German politicians. Yet, the BND was using that same base to acquire the conversations of a succession of French Presidents, including Jaques Chirac, Nicolas Sarkozy and François Hollande. And who has shown the Germans how to decrypt communications? The French.

In the name of the Franco-German cooperation, the Direction Générale de la Sécurité Extérieure (DGSE) taught their colleagues from the BND how to penetrate codified communications and, unknowingly, helped them listen to their President. The irony is that no one put an end to the foul play. Since at least 2008, the BND had told political authorities that it knew the Americans were violating the deal. But someone decided it was more convenient not to interfere.

France has said it is “unacceptable to spy on allies”. The same statement came from Merkel, who claims “spying friends: we shouldn't do it”. Are the US then the only ones to blame? Every time a politician complains about being tapped, he or she often forgets that any international activity, and especially diplomacy, requires the knowledge of what your friends or foes think. Authorities often omit to say that they are the ones that task intelligence agencies with finding out information on people, economic deals and so forth. Do they wonder how these infos are gathered? Did Angela Merkel complain when she read the diplomatic correspondence of friendly countries or the Red Cross? Would have she objected to reading the transcripts of the phone calls from French presidents as the CIA and NSA did? We doubt it.

In this entire affair the NSA has “officially” been named the culprit. But they didn't act alone. Other nations were part of the program. The British General Communications Headquarters (GCHQ) works closely with its US counterparts in monitoring communications. As Edward Snowden pointed out, they can control any flow via radio, telephone or the internet, all over the world through the Echelon and Prism programs.

There are also other English speaking intelligence agencies that collaborate with both the NSA and the GCHQ: the Australian Signals Directorate, the Canadian Communications Security Establishment, the Government Communications Security Bureau from New Zealand. Since interceptions require the maximum degree of secrecy on who is the target and how the tapping is carried out, whoever is part of the system also has access to the information that's acquired. And no dispatch is ever handed out unless there is a specific reason to do so. Other Agencies are granted information on a case by case basis or on the basis of bilateral deals.

In other words, whatever the NSA gathered on Merkel, Hollande, Berlusconi or Roussef was shared among these five agencies. No one had the slightest moral or professional dilemma when it came to acquiring this information. On the other hand, these five countries know how interception is carried out. They hence also know what the weak points of the system are and how to defend themselves from intrusions.

One could object that it could have been more useful to dedicate these efforts to intercepting the terrorists that attacked Paris on November 13, 2015. After all, Europol has a list of 3 to 5 thousand foreign fighters that have returned form Syria and Iraq. But this is a misleading question: intelligence agencies are perfectly capable of handling both. Nonetheless, we know everything about Merkel's phone calls and nothing about the ones by Salah Abdeslam and Abdelhamid Abaaoud in Paris, or the Kouachi brothers prior to Charlie Hebdo.

The point is: anything can be intercepted, but not everything is of interest. Selection is an unsolved issue. However, the most interesting conversations are generally encrypted. This is what embassies or security forces employ when dispatching their communications. Telephones also have their encryption systems, the most effective ones being the point-to-point ones that utilize the same program. Politicians have the need to communicate, often by cellphone, and thus they don't always use encrypted means of communication.

On February 25, 2016, US President Barack Obama signed a law that grants foreign citizens from friendly countries the same privacy as US citizens. Despite the political scope of the initiative, it is self-evident that if US national security is at stake, no one will be safe from interceptions. And there is no doubt that the mass surveillance programs will not be dismantled.

The one mistake done by both the NSA and the BND deserves a final consideration. Any intelligence agency is more efficient the more secretive it is. The US agency was exposed first by Wikileaks and Julian Assange and then by Edward Snowden. The BND was put in the spotlight by a German weekly magazine. In both cases the systems failed to monitor and protect from leaks. This is the one aspect we should stigmatize: it is not what they were doing, but that they got caught doing it.

THE CYBER-WAR IN THE MIDDLE EAST: ISRAEL, IRAN AND OTHERS

There us a war being fought in the Middle East which is seldom spoken about. It is a silent, sneaky war, but an important one because it endangers the security of many States and organizations. It is the Cyber-war, a non-conventional kind of war that is fought online.

It is an offensive war, when it is used to penetrate the servers of the opponent and a defensive war when it is used to prevent one's own servers from being hacked.

This war's importance is given by the fact that the internet has become global; a highway where everything moves and where everything can be intercepted, manipulated or damaged. One just needs to know the right technique.

The cyber-warfare is not fought solely in the Middle East but across the globe (cyber crime, the criminal aspect of the internet, has risen by 30% in the past year). However, in the Middle East, where wars are ongoing and terrorism and instability are endemic, the importance of cyber-warfare is increased.

Suffice to say that last January, when the consumption of electrical energy was essential to keep the Israeli population warm during a wave of low temperatures, a cyber attack against the country's electrical company forced the caused the country to shiver for two entire days. A virus had managed to block the company's computers, thus causing a halt to the company's activity as well.

In April last year a Palestinian hacker violated the Israeli servers, breaching the systems of the Prime Minister, Defense and Education ministries, the domestic intelligence service Shin bet, the Tel Aviv police and the local stock market. Two days later the Israelis retaliated by attacking the Palestinian office of vital statistics, where the information concerning 4 million individuals is kept. The data pertaining to roughly 700 Palestinian public employees, ministers and journalists were then uploaded to the web.

If we look further back, there is the cyber-war fought by Israel against the Iranian nuclear program by means of the “Stuxnet” malware and the “Flame” spyware. (vedasi “L'Iran e la guerra segreta” - Invisible dog del giugno 2012).

The cyber-war is not aimed solely at penetrating servers and databases, but also at dis-informing, recruiting and spreading propaganda. This is why many countries have built their own, internal, structures to fight the threat and to exploit its offensive potential.

Israel

Isrealis were the first to foresee the potential threat posed by the cyber-sector when they created – over a decade ago – a structure called “Directorate C4i” (Command, Control, Communications and Computers). The Directorate operated within the army's General Staff.

In September 2014 Netanyahu announced the constitution of a new agency, the “National Authority for Cyber Defense” whose defensive role was that of protecting the State's structures from cyber-attacks. This agency presides and coordinates all operative aspects of the cyber-war. The agency should operate in full efficiency within three year's time. It falls under the jurisdiction of the Prime Minister's office and coordinates its activity with the National Cyber Office (which exists from 2012), also in the hands of the Prime Minister.

The offensive activity is developed by the army, in part by the Directorate of Military Intelligence, where the famous 8200 unit operates, and in part by the Military Signal Corps. The former is in charge of clandestine operations and is in close operative contact with the Shin Bet and the Mossad (which, in turn, have their own cyber-facilities). It is thought to be the more qualified of the two.
The latter operates almost exclusively in the interest of the army; its activity is comprised of communications, encryption and decryption (in substance, it is the more 'defensive' branch).

But the Israeli army also has a Brigade for Cyber Defense which answers directly to the army's Chief of Staff. This structure forms its own Corp and is headed by an army General. The Brigade has its own structures and operative rooms. The structure's inauguration has recently been the object of a military drill. All foreign operations planned by the army see a representative of the cyber-branch sitting around the strategy table. The tendency, as far as Israel is concerned, is that of unifying the offensive and defensive activity and, within the former, to do away with the dualism between military intelligence and Signal Corps.

There are, however, other civil agencies that dedicate themselves to the sector within the Israeli State:
- the aforementioned National Cyber Office, which expresses the guidelines for the development of cyber technologies (offensive/defensive), monitors the technological development in the industrial sector and encourages the cooperation between the various agencies (private/public). The National Cyber Office is also a consultant of the Prime Minister on all levels, including the legislative one. Within the agency there operates an 'early warning' room to spot cyber-threats.
- the Authority for National Information Security, whose duty is to regulate and give advice to infrastructures that are vulnerable to cyber-attacks.
- the various departments within the Police and the Shin Bet.

The plethora of agencies and structures give away the importance that Israel assigns to this kind of warfare, however, since it is a 'young', constantly evolving sector, there are still some unsolved problems, such as the lack of integration between the various structures. Nevertheless, at least with regards to the cyber-security sector, Israel is considered today one of the most advanced countries in the world.

Iran

Iranians, whom have experienced the danger of cyber-warfare against their own nuclear program, also have a series of structures, both civil and military, dedicated to the development of strategies to face the threat.

In 2010 Iran created the “Commando for Cyber Defense” (a military agency whose duty is to defend the State's structures from cyber-attacks), which operates under the supervision of the “Organization for passive civil Defense” (a civil structure with military head – active since 2003) which, in turn, lies under the jurisdiction of the army's Chief of Staff. All of these agencies are formed to answer to specific threats by operating though a “permanent commission” comprised of both military and government representatives. The hierarchy is military (until March 2011 they were administered by the President). These structures were created after Israeli/US hackers managed to block/damage the Iranian nuclear program with malicious software.
In March 2012 Iran founded the “Supreme Council of Cyber Space” (Shoray Aali Fazaye Majazi), which expresses the directives in this specific sector to the various government agencies. The Council is headed by General Abul Hassan Firouzabadi, who acts as its secretary, and is comprised of the heads of the judicial system, of the Parliament, the head of the State television, the Commander of the Revolutionary Guards, the head of Police and various government ministers (Intelligence, Culture, Interior, Information, etc.)
The duty of this agency is mostly that of control and censure, as we saw during the latest Parliamentary elections. Within the Supreme Council there is a commission that examines broadcasts and news from the mass media. The commission is comprised of representatives from the intelligence agencies, from the Interior ministry, ministry of Culture and Cyber Police, a special branch of the Police which fights cyber-crime and, of course, the opposition to the regime.

Half of Iran's population owns a smartphone, there are over 1500 websites and the use of social media, networks and messages is widely spread. In the past, such instruments were used in protests and demonstrations. Among the initiatives considered by the regime aimed at limiting the “negative” use of the internet there was that of creating a 'closed' web and a 'national' search engine.
In July 2009 Iran created yet another structure, the “Commission for the identification of non-authorized internet websites”. This commission is headed by Khamenei, sided by the country's highest institutional figures.
The offensive activity is administered by intelligence and military structures, especially within the Command of the Revolutionary Guards, where there exists a cyber-unit. The numbers of its members are not known, but their specialty is: the unit is comprised of hackers who carry out their offensive activity abroad. The technical capabilities of this unit are regarded – by friends and foes alike – very highly. There are allegedly two cyber Commands in Tehran where operative activity is carried out. The paramilitary Corp of the Basiji (part of the Iranian army) also has its own structure, but it is considered to be professionally inadequate. It is nonetheless also supervised by the pasdaran.

Due to the military campaign in Syria it is currently difficult for Iran to focus on cyber-attacks against other enemies, but in the future cyber-warfare will surely be an option against Iran's historic enemies such as Saudi Arabia.

The building blocks are already in place. In August 2012 (during Ramadan) a 'spam' e-mail managed to shut down over 35.000 computers belonging to the oil company ARAMCO. The attack was carried out by the self-proclaimed commando “sharp sword of Justice”, which was found to be operating out of Iran. The experiment was then successfully replicated in the following years against companies in Kuwait, Qatar and United Arab Emirates. In June 2015, at the start of Saudi Arabia's military engagement in Yemen, another group called the “Yemen Cyber Army” managed to make public about half a million documents stolen from the Saudi foreign ministry's servers. All of this happened despite the promise by US president Obama to assist the Gulf Cooperation Council in keeping their cyber-security up to date.

That Iran is – just like Israel – particularly active in cyber-warfare is confirmed by the fact that over 50 agencies/companies in 16 countries were attacked from Tehran in the years going from 2012 to 2014 as a part of cyber-operation “Cleaver”.

The Hezbollah

Lebanon's Hezbollah, who are directly assisted by Iran, have built a center for electronic warfare in the outskirts of Beirut, in the Shiite neighborhood of Dahya. The center is run by Wafiq Safa, a relative of the movement's leader Hassan Nasrallah. The structure is mainly dedicated to offensive actions against Israel. Hackers and other experts are trained by Iranians in cyber-warfare. In the Summer of 2014, during the Israeli operations in Gaza, there were a number of hacking attempts against Israel originating in Lebanon, from a company/group called “Volatile Cedar”. It must be noted that in December 2013 the head of Hezbollah's cyber activity, Hassan Laqees, was killed in Beirut, probably by members of the Mossad.

The Islamic Palestinian Jihad and Hamas

The Islamic Palestinian Jihad operating in Gaza is accredited with the capability for cyber attacks. The organization has managed to hack the Israeli telephone system and send messages to the population. Again, it seems that the training of the Palestinian hackers was carried out at the hands of the Lebanese Hezbollah thus, by virtue of the transitive rule, by the Iranians.
Hamas, which also benefits from the same source of training, also has its own cyber guerrillas, both offensive and defensive. In 2014 their unit managed to hack the Shin Bet servers, thus unveiling the identity of Palestinian spies operating in Gaza.
It is striking that such high hacking efficiency is not attained by the National Palestinian Authority and its agencies.

Syria

The Syrian army has its own structure called “Syrian Electronic Army”, to which sources attribute an attack against various journalistic structures (Reuters, Washington Post) and against the official website of the US Army.

ISIS

Al Baghdadi's group allegedly carried out a cyber attack against the website of the Syrian Observatory for Human Rights in July 2015. The hackers named themselves “Cyber Army of the Caliph”.
In January 2015, Caliph hackers hijacked the USCENTCOM's Youtube and Twitter accounts.
From July 2015, in order to oppose the ISIS propaganda, recruitment and their transmission of operative directives over the internet, the European Union created a specialized unit that monitors internet traffic and the social networks. Suffice to say that there are over 40-50 thousand accounts operated by figures with ties to Islamic terrorism which dish out roughly 100.000 tweets on a daily basis.

The potential of the cyber war

The goals of cyber-warfare are diverse: they range from espionage (by penetrating the servers of adversaries or by monitoring the various social networks) to dis-information, propaganda, psychological warfare, recruitment of sources, blocking of critical infrastructures, up to the identification of individuals for their apprehension or elimination. The case of Hamzi Abu Haija, an important member of Hamas' Izzidin al Qassem brigade, falls in the latter category. Hamzi was killed in an Israeli raid on March 22, 2014. His location was found while he was busy chatting on facebook in the refugee camp of Jenin. By using cyber techniques, Israel also managed to monitor the negotiations on the Iranian nuclear program through a hole in the computers of a Moscow hotel where the delegations were staying. Cyber attacks can block the activities of hospitals (with dire consequences in terms of victims), hinder the supply of energy or water, crash a city's network (even freeze traffic lights), interfere with electronic missile systems. Block a country's telecommunications (radio, telephone, TV) and their army's system of command and control, interfere and paralyze radars, blind the control towers of an airport with its airplane traffic… this list could carry on forever.

In the near future, because of its offensive potential, this non-conventional kind of warfare will develop greatly in the Middle East and the main players, in virtue of their specific capabilities, will be Israel and Iran.