Images haven't loaded yet. Please exit printing, wait for images to load, and try to print again.

Jul 29, 2016 · 19 min read

The Dark Side of Privacy: How ISIS Communications Go Undetected

A trove of communications from ISIS plots and activity in Europe reveals a mix of direct control and improvisation and shows the crucial importance of encrypted tools. "Detonate your belt in the crowds," one message declared.

By Sebastian Rotella

An airstrike on ISIS in Kobani, Syria, in October 2014. (Photo: Public Domain)

After assembling suicide bomb vests for the attacks that slaughtered 130 people in Paris last November, Najim Laachroui went underground in his native Brussels.

The 24-year-old explosives expert wasn't just hiding from the biggest manhunt in Europe's recent history. He was plotting. In a dingy apartment converted into a bomb factory, Laachroui exchanged a series of messages in French with Abu Ahmed, a shadowy commander in the Islamic State based in Syria.

If law enforcement agencies had intercepted the communications, they would have been immediately alarmed. Laachroui asked militants in Syria to test chemical mixtures so he could assemble powerful bombs. He discussed his hopes to strike France again and disrupt a soccer championship there. He reported that he and half a dozen other fugitives from the Paris attacks had split up among three safe houses, according to Belgian and French counterterror officials.

Although spy agencies in the United States and Europe were scouring the Internet for any trace of Laachroui, they failed to intercept those exchanges. The reason, U.S. and European counterterror officials say: During Laachroui's four months on the run, he and Abu Ahmed communicated through Telegram, an encrypted messaging application, and other widely available tools for secure communications.

On March 15, Belgian police raided a safe house and killed another leader of the terrorist cell in a gunfight. A worried Laachroui sent a message to Abu Ahmed reporting that the raid had cost the plotters the stash of ammunition for their AK–47 rifles, according to Belgian and French counterterror officials.

"The original plan at the airport was for them to do an attack more like Paris: shoot a lot of people first, and then set off the bombs," a Belgian counterterror official explained in an interview in April. "But they didn't have ammo because it was left behind in the safe house. Laachroui says: 'We don't have chargers for our guns. What do we do?' They were told to go ahead and attack just with bombs.'"

On March 22, they did just that. Laachroui and two other suicide bombers killed 32 people at the airport and at a subway station in Brussels. Afterward, investigators found a laptop computer that helped them re-construct Laachroui's encrypted audio and text exchanges with his commander in Syria, according to European counterterror officials.

Taken together, the voices of the Islamic State offer insights into the day-to-day workings of an organization that has carried out lethal attacks in Baghdad, Bangladesh, and Turkey in recent weeks.

The communications were described by European and U.S. counterterror officials to ProPublica, which is preparing a documentary about terrorism in Europe in collaboration with the PBS program Frontline. ProPublica interviewed counterterror officials in Europe and the U.S., some on condition of anonymity, and reviewed intercepted conversations documented in European court cases.

Taken together, the voices of the Islamic State offer insights into the day-to-day workings of an organization that has carried out lethal attacks in Baghdad, Bangladesh, and Turkey in recent weeks.

The culture of ISIS mixes the centralized control that characterized al-Qaeda with a more freewheeling approach that gives its operatives considerable latitude. The group's use of digital propaganda to inspire "self-radicalizing" terrorists has drawn attention with attacks on U.S. soil in San Bernardino and Orlando. But the communications collected in Europe show the group provides direct long-distance instructions to operatives it dispatches from its base in Syria, and they rely heavily on that guidance.

The European communications also clearly establish the importance of encryption to ISIS operations.

"We are dealing with a challenge right now: New technologies that enable encryption and allow them to be fairly confident that they are communicating in a way that can't be detected," a senior U.S. intelligence official said. "They know how to communicate securely. Often we are inhibited: We know the fact of the communications taking place without knowing the content."

In April, Italian police overheard a senior figure in Syria urging a Moroccan suspect living near Milan to carry out an attack in Italy, according to a transcript. Although the voice message had been sent through an encrypted channel, the Moroccan played it back in his car, where a hidden microphone recorded it.

In the message, the unidentified "sheik" declared: "Detonate your belt in the crowds declaring Allah Akbar! Strike! (Explode!) Like a volcano, shake the infidels, confront the throng of the enemy, roaring like lightning, declare Allah Akbar and blow yourself up, O lion!"

The suspects exchanged recorded messages over WhatsApp, an encrypted telephone application that is widely used in Europe, the Arab world and Latin America. Federal Bureau of Investigation Director James Comey and other counterterror officials have publicly expressed concern about extremists in the U.S. using such techniques to elude monitoring.

"We'll be monitoring a couple of guys in an Internet chatroom," a former FBI counterterror official said in an interview. "Then you'll see one of them says: 'OK, reach out to me on WhatsApp.' At that point, we can't do anything."

Executives at WhatsApp and Telegram defend encryption as a vital shield to privacy. Reached for comment, a spokesperson at WhatsApp said the company complies with U.S. laws requiring cooperation with law enforcement agencies. The spokesperson cited a statement by executives in April when WhatsApp implemented "end-to-end" encryption that will conceal the content of users' communications even from the company itself.

"Encryption is one of the most important tools governments, companies, and individuals have to promote safety and security in the new digital age," said Jan Koum, the company's founder, in a blog post in April. "While we recognize the important work of law enforcement in keeping people safe, efforts to weaken encryption risk exposing people's information to abuse from cybercriminals, hackers, and rogue states."

(Facebook, which owns WhatsApp, recently announced that it would add end-to-end encryption for some photo and text messages on its Messenger application.)

Telegram did not respond to a request for comment for this article. But company executives have publicly addressed concerns about encryption by saying that technology comes with an inevitable dark

side. The company says it has shut down more than 660 public channels on its application that were being used by the Islamic State.

Intelligence officials say the Islamic State's failure to launch Paris-style attacks in the U.S. reflects differences in both geography and demography. American Muslims are less radicalized and less numerous than those in Europe, and U.S. border security makes it harder for would-be terrorists to enter the country, according to Western counterterror officials.

In Europe, the Islamic State has found support in large and restive Muslim communities, especially among criminals who radicalize more rapidly today than previous generations of hoodlums-turned-jihadis. Investigators say intensified Western military pressure in Iraq and Syria has prompted the group to order European recruits to strike immediately rather than make the pilgrimage to the caliphate.

"In the context of the current strategy of the Islamic State, it's clear that their focus is causing casualties here," said Claudio Galzerano, commander of a counterterrorism unit of the Italian police.

. . .

The ISIS strategy toward the West has evolved since the Islamic State conquered a swath of territory in Syria and Iraq and declared the caliphate two years ago, causing thousands of militants to flock to Syria.

Previous generations of aspiring jihadis passed through a series of filters as they journeyed to al-Qaeda training camps in South Asia, often with a first stop at radical mosques in London. This selective, secretive approach allowed al-Qaeda to vet prospective holy warriors and detect attempts at infiltration by intelligence services.

In contrast, the flow to Syria has been larger, faster, and less security-conscious. Taking advantage of Europe's proximity and ease of travel, fighters who rushed to Syria posted photographs of themselves online brandishing guns. Their ranks included criminals and thrill-seekers with little religious knowledge, according to Marc Trevidic, a veteran French counterterror judge.

The Islamic State "has accepted for strategic reasons, because it wanted to impose itself on other groups in the region, the recruitment of anyone," Trevidic said. "Methods will be created afterwards to check that ... they are not spies, etcetera, but initially there are no filters."

> *"They know how to communicate securely. Often we are inhibited: We know the fact of the communications taking place without knowing the content."*

An Italian investigation begun in 2014 documented that hectic period. Tracking jihadis from Italy, police intercepted the cell phones of senior figures in Turkey and Syria, according to a 44-page report by a Milan investigative magistrate dated June 12, 2015. A Turkish phone was used primarily by Ahmed Abu al Harith, "a significant member of the terrorist organization with the role ... of coordinating volunteers arriving in Turkey and headed to join the Islamic State," the report says.

Monitored in late 2014 and early 2015, Ahmed Abu al Harith and fellow coordinators spoke multiple languages with callers from 22 countries including Afghanistan, Saudi Arabia, Georgia, San Marino, and Sweden.

They explained "concrete rules for joining the Islamic State already described on the Internet in a manual titled 'Hijrah [Pilgrimage] to the Islamic State—what to bring, whom to contact, where to go,'" according to the Italian report.

The coordinators didn't use encryption or coded language. But they banned recruits from traveling with "latest-generation mobile devices" in order to "avoid being located" by spy agencies. The Islamic State wanted recruits to leave behind smartphones, tablets, and other devices with existing trails of activity that make them easier to trace, and use new, disposable cell phones instead, the report says.

Some recruits were less than sophisticated about the directives.

On January 4, 2015, an exasperated coordinator repeatedly explained to a befuddled caller with a Lebanese accent that he could only bring a basic cell phone to Syria, according to a transcript.

"The important thing is that when you arrive in Turkey you have a small cell phone to contact me," the coordinator said. "Don't bring smartphones or tablets. OK, brother?"

For the fourth time, the recruit asked: "So we can't have cell phones?"

"Brother, I said smartphones: iPhone, Galaxy, laptop, tablet, etc."

Sounding a bit like a frustrated gate agent at a crowded airport, the coordinator added: "Each of you can only bring one suitcase. If you come alone, just bring one suitcase. That is, a carry-on and one suitcase."

"I didn't understand the last thing, could you explain?"

"Brother, call me when you get to Turkey."

In Syria, new arrivals were interviewed by Islamic State militants seated at computers, according to Western counterterror officials. The militants asked a checklist of questions including blood type, mother's name, level of religious education, and preference for becoming a "warrior" or a "martyr," according to copies of Islamic State intake forms obtained by ProPublica. The authenticity of the documents was confirmed by U.S. counterterror officials.

Although the culture of the Islamic State is repressive and bureaucratic, the reality on the ground can be rather anarchic. The restrictions on high-tech devices described in the Italian investigation were by no means uniformly imposed or obeyed. Militants in the self-styled caliphate have access to computers, smartphones, and social media. Some have posted a barrage of messages and images, including videos of atrocities.
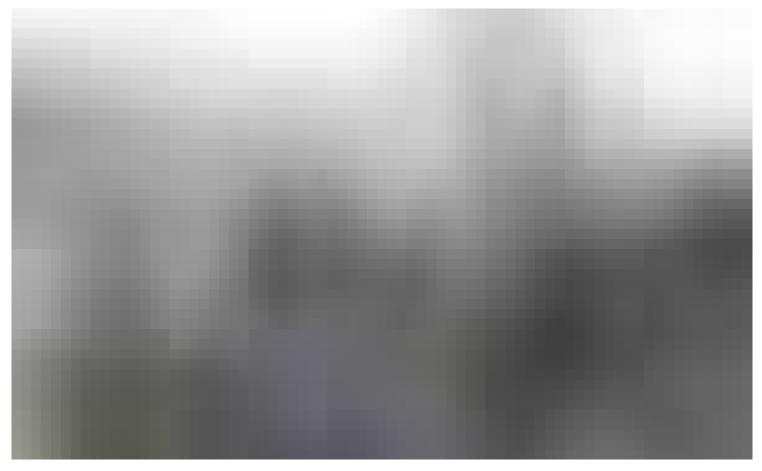
In response, leaders of the Islamic State have told foreign fighters to curtail their activity on social media because it exposes them to eventual prosecution back home or to being targeted in Syria. The use of social media has continued, however, according to European counterterror officials.

In fact, the cacophony of voices from Syria has been crucial to recruitment.

"In contrast to what has happened with other conflicts, the recruitment and the propaganda aren't just in hands of the public communications apparatus," said a counterterror chief of the Spanish police. "Each fighter has a phone and narrates his day-to-day life, his blog…. A lot of these terrorists have circles of associates in Europe because they came from there, so this is effective publicity."

Tapping into such communications, Italian police gained insight from their investigation of a family of Muslim converts from the Milanese suburb of Inzago.

Maria Giulia Sergio was 28. In September of 2014, she married an Albanian extremist she barely knew so they could join the Islamic State, according to investigators. The couple traveled with his mother to the Syrian city of Sed Forouk and met up with Albanian relatives living there, including children. The husband's brother died in combat, according to the report.

Female fighters trained by the Kurdish Workers Party to defend themselves against Islamist extremists. (Photo: Kurdishstruggle/Wikimedia Commons)

The newlyweds encountered "numerous daily obstacles" to staying in touch with people back home because of "rigid rules imposed by the Islamic State as well as the objective technical difficulties, in a country devastated by years of civil war," the report says. "This had a positive impact on the investigations because it had the practical effect of multiplying calls among relatives" in Italy and Albania when they heard from the militants.

Sergio talked via Skype because the suspects believed it was "more secure," the report says. Police intercepted the conversations nonetheless. Sergio described her husband's stint in a training camp in Iraq. She talked about child care, Koranic classes, decapitations and a stoning, and implored her family to make the "hijrah," or pilgrimage to Syria.

"I am speaking to you in the name of the Islamic State," she said. Scolding her father for remaining in his job in Italy, she said: "It

makes no sense for you to work for them. They are the ones who must be our slaves."

In April of last year, the parents announced they would join her. The father asked if he should bring his driver's license and if he could buy a car in the "Caliphate," according to the transcript.

Police arrested the suspects before they could depart.

·   ·   ·

Meanwhile, authorities across Europe struggled to intercept a smaller flow of militants traveling in the opposite direction.

Western intelligence officials estimate that the Islamic State dispatched between 60 and 180 operatives to attack targets in Europe. The strategy appears to have been to overwhelm the security forces with sheer numbers. Even if most of the strikes failed, something would eventually succeed. The results were graphically evident in France, where authorities foiled 11 attacks in 2015.

Officials say the threat has changed since the days of al-Qaeda. Osama bin Laden's group had the flexibility common to Islamist terror networks, often developing plots based on the initiative, expertise, and availability of recruits who reached its secret compounds in Afghanistan and Pakistan.

Al-Qaeda created a team to oversee attacks overseas. The chief plotters were Middle Easterners or Pakistanis, and they guided operatives to targets with instructions via phone and email. U.S. counterterror agencies identified external operations chiefs and eliminated a series of them with drone strikes and captures.

Today, the counterterror community is still mapping out the Islamic State's leadership, especially those involved in foreign plots, according to the senior U.S. intelligence official.

"They were able to elude us. But they were able to elude the Americans, too, and that shows you what a problem encryption is."

"The structure that promotes attacks is wider and deeper, but to some degree also more autonomous, than what we saw with al-Qaeda," the official said. "It isn't the case where we can home in on individuals and have a fair degree of confidence that if we neutralize them we will have had a considerable impact on the threat. That's not the situation with ISIS. We had a fairly comprehensive view of the structure of al-Qaeda…. With ISIS, we don't have an exact picture. It's an intelligence collection challenge that we are working hard to address."

The Islamic State's top echelons are dominated by Gulf Arabs, Syrians, and Iraqis, including former military and intelligence officers. Foreign fighters serve in units known as "katibas" organized by nationality and language. Large Francophone katibas field hundreds of French and Belgians, many of North African descent, and thousands of Moroccans and Tunisians. Senior foreign fighters have the resources of a quasi-state at their disposal: money, technology, identity documents, training facilities. But they are also given considerable autonomy to develop plots, officials say.

"There is … leeway to foreign fighters and operatives to choose targets and methods on turf they know best," the senior U.S. intelligence official said. "The foreign fighters know what the organization wants to see happen and they act on it."

The attacks on Paris in November briefly made Abdelhamid Abaaoud, a 28-year-old Belgian ex-convict, an internationally known leader of the external operations unit. He participated in the massacre and died in a police raid days later in the gritty suburb of Saint Denis. Yet some investigators now believe his stature within the Islamic State has been overstated.

"To me he was an average leader," said Judge Trevidic, who led investigations of plots in which Abaaoud surfaced. "Have you ever seen a general on the front in Saint Denis? That is all right for a lieutenant, a captain, but not for people above. "

Based in Syria, Abaaoud selected, trained, and deployed jihadis to Europe in 2014 and the first half of 2015. In addition to guns and grenades, he taught trainees about secure communications—

encrypted applications such as Telegram, WhatsApp, and Truecrypt—
and set up protocols to contact them when they were in place.

Secure communications technology has been a recurring feature in
recent attacks and foiled plots in France, according to French Interior
Minister Bernard Cazenueve.

"Encryption is a crucial issue," Cazeneuve told a small group of U.S.
reporters in March. "All the attacks last year used encrypted phones or
computers…. It is a difficult problem for us."

(For background on the use of encryption by terrorists, read this
article in the June issue of *The CTC Sentinel*, the monthly publication
of the Combating Terrorism Center at West Point.)

Abaaoud's operatives did not always follow security procedures,
however. In June of last year, Turkish immigration authorities
detained Tyler Vilus, a French plotter en route to Paris with someone
else's Swedish passport. Allowed to keep his cellular phone in a low-
security detention center, Vilus brazenly sent an unencrypted text
message to Abaaoud in Syria, according to a senior French
counterterror official.

"I have been detained but it doesn't seem too bad," the message said,
according to the senior official. "I will probably be released and will
be able to continue the mission."

Instead, U.S. spy agencies helped retrieve that text and French
prosecutors charged Vilus with terrorist conspiracy.

In another case linked to Abaaoud in early 2014, the National Security
Agency played a central role in helping French police track down
Ibrahim Boudinah, a plotter captured in a Cannes safe house as he
prepared an attack with explosives and guns.

Officials said the Paris plot did not involve much long-distance
direction. Instead, Abaaoud and two other field coordinators traveled
separately from Syria to Europe to prepare the attack. Abaaoud
entered via Greece in September, probably melting into a vast, chaotic
flow of illegal immigrants that the Islamic State has used to infiltrate
operatives during the past two years.

The other two leaders made their way to Budapest, where they sheltered in crowds of refugees camped out in the train station, according to Belgian prosecutors. On September 9, they were picked up at the train station by a Belgian accomplice named Saleh Abdeslam, who drove them to Belgium, prosecutors say.

The pair had different skills. Laachroui, a former electrical engineering student from Brussels, was the explosives expert. Belkaid, an Algerian petty criminal who lived in Sweden before joining the Islamic State, had more ideological preparation and religious knowledge than the others in the attack squad, officials say.

In Brussels, the duo set up a remote command post in a safe house and coordinated the Paris operation by phone. The gunmen and bombers used a number of disposable cell phones during the attacks. Although police re-constructed the activity of a phone found near the scene of the attack on the Bataclan concert hall, plotters exchanged encrypted messages before the attacks that French intelligence could not detect, according to Interior Minister Cazenueve.

Afterward, the coordinators in Brussels made calls and wired money to help Abaaoud, who was on the run, rent the shabby apartment north of Paris where police eventually killed him. Intercepted calls suggested that Laachroui and Belkaid "had some rank or influence," a senior Belgian counterterror official said.

Laachroui and Belkaid became targets of a massive manhunt along with Abdeslam, the lone surviving attacker from Paris, and several other accomplices. They were sheltered for four months in Brussels by networks based on clan, ethnicity, and criminality, and ruled by a code of silence. Police monitored at least 89 phones. An intercept picked up ominous chatter.

"It was possibly Saleh [Abdeslam] or an associate," the Belgian counterterror official said. "He's saying: 'The cops are chasing me. Things are hot here. We are going into action.' And the voice in Syria says: 'Yes, go into action.' But there wasn't intelligence of a precise plan."

That snippet of intelligence was among the leads that prompted Belgian authorities to shut down their capital for five days in

November. But the attack didn't happen for a while.

During the next four months, the bombmaker Laachroui stayed in close contact with the Islamic State using encrypted methods, principally Telegram, according to Western counterterror officials. The fugitives also communicated with Syria and each other using WhatsApp, Skype, and the mobile application Viber on devices including laptops, tablets, and phones, counterterror officials said.

Laachroui exchanged audio recordings and text messages with Abu Ahmed, a French-speaking "emir" of foreign fighters in Syria, counterterror officials said. Investigators believe Abu Ahmed was based in Raqqah, the Islamic State's headquarters, and that he also played a role in overseeing the Paris plot.

It's not clear if Western intelligence officials have identified Abu Ahmed yet. Several veteran French jihadis in Syria are suspected of overseeing external operations. They include the converts Fabien and Jean-Michel Clain, brothers from Toulouse (Fabien Clain is believed to have issued the Islamic State's claim of responsibility for the Paris attacks); Boubaker el Hakim and Salim Benghalem, Parisian veterans of a cell that first waged jihad in Iraq in 2004; and a blond convert known as Abu Sulayman al Fransi, described as a former physical education teacher and father of two.

At one point, Laachroui told Abu Ahmed there were tensions among the fugitives in Brussels, according to officials.

> *"The structure that promotes attacks is wider and deeper, but to some degree also more autonomous, than what we saw with al-Qaeda."*

"They were squabbling," the Belgian counterterror official said. "They told the emir: 'We have split up. We were arguing before. It's better now.'"

As Laachroui worked with TATP, a highly volatile explosive, in his hideout in the Schaarbeck neighborhood, he asked Abu Ahmed for technical help from bomb experts in Syria.

"He has them check different mixtures and adjusts his work based on what they tell him," the Belgian counterterror official said.

The fugitives and the emir discussed potential plans including a massive attack with 600 kilos of explosives that did not take place. The goal was to wait and strike France again in hopes of disrupting or canceling the month-long Euro 2016 soccer championship scheduled to begin in June, according to counterterror officials.

European spy agencies and their allies in the U.S. and Britain deployed the full weight of their sophisticated technology in the search for the plotters. But neither the NSA nor Britain's Government Communications Headquarters, spotted the digital footprints, officials said.

"Everyone was trying to find these guys," the senior French counterterror official said. "They were able to elude us. But they were able to elude the Americans, too, and that shows you what a problem encryption is."

Police work on the ground produced a breakthrough on March 15. A forgery investigation turned up fake identity cards used to rent apartments. Police went to what they thought was an abandoned safe house near an Audi factory in the Forest neighborhood.

The raiders used a hand-held battering ram on the door. They discovered Belkaid aiming an AK–47 at them. The firefight wounded him and several investigators, who tumbled down a flight of stairs seeking cover. A SWAT team finished off Belkaid. Police found the cache of ammunition for AK–47 rifles—and DNA traces of Abdeslam, who had fled while Belkaid held off the officers.

The bad news reached Laachrooui, who sent the urgent message to Syria. Abu Ahmed told him just to use bombs, and the fugitives decided to hit Belgium rather than France because time was running out. Once again, the Islamic State let them decide targets and timing, counterterror officials say.

On March 22, Laachroui and another suicide bomber blew up at the Brussels airport. A third bomber struck at a subway station. Thirty-five people died and more than 300 were wounded.

It could have been worse. Two other bombers lost their nerve and fled. The improvised nature of the attack raises the possibility that it might not have succeeded without the guidance from afar.

. . .

Airstrikes and battlefield losses have intensified pressure on the Islamic State. It has become more difficult for plotters to enter Europe illegally and for recruits to reach Syria, counterterror officials say.

But terror groups often accelerate attacks abroad in response to defeats at home, as reflected by a recent flurry of strikes in Turkey, Iraq, and Bangladesh.

An Italian investigation this year gives glimpses of a changing landscape. The chief suspect was Abderrahim Moutaharrik, a Moroccan immigrant living north of Milan with his wife and two children. A professional kickboxer, he was so radical that he posted a photo of himself in the ring wearing a T-shirt with the Islamic State logo, investigators say.

Moutaharrik and his associates used WhatsApp extensively, according to a 72-page Milan prosecutor's report dated April 19, 2016. The police secreted microphones in homes and cars and implanted mobile devices with spyware, the report says.

Moutaharrik idolized Mohamed and Osama Koraichi, brothers fighting for the Islamic State. His desire to emulate his friends increased after Osama died in an air strike in Iraq last year. Moutaharrik sang jihadi anthems and ranted about killing infidels in front of his four-year-old son, the report says. His wife obtained a bank loan of $7,800, allegedly to finance their imminent move to Syria.

But there were problems. Mohamed Koraichi was difficult to reach and couldn't find the family a smuggler in Turkey.

On March 15, Moutaharrik finally received an audio message from Koraichi via WhatsApp from an Indonesian phone in Syria. They discussed the kickboxer's hopes of making the pilgrimage.

On March 20, Moutaharrik received another WhatsApp message from Syria. But this time a new voice addressed him by name: a high-ranking militant who spoke flowery classical Arabic. He wanted the kickboxer to wage jihad right away.

The "sheik" said the Islamic State was under attack by "Christian" armies from "bases in your homes, European bases," according to the transcript.

"You must take revenge on them, revenge for the Muslims," the sheik said. Praising "lone-wolf" operations, he continued: "in the Christian nations, one operation gives more satisfaction than dozens of bombs…. You will be among those who do this good deed in the lands of the Christians, in Rome, in Italy…."

"We will take revenge," Moutaharrik replied, according to the transcript. "God willing here they will only know massacres and killings."

The police went on red alert. Suicide bombers struck Brussels two days later. Moutaharrik and his wife celebrated, according to transcripts. The sheik and Koraichi urged the increasingly agitated kickboxer to attack right away.

Italy "is the capital of those who carry the cross, my brother," Koraichi said. "Until now there hasn't been any operation done [in Italy], know that if you do an attack it is a great thing."

On April 8, the sheik sent a soliloquy that he titled "Bomb Poem." It evoked images of fire, suicide bomb belts, and Islamic battalions "annihilating the infidels."

Police arrested Moutaharrik and three other suspects 11 days later.

Follow Us on <u>Twitter</u> | *Like Us on* <u>Facebook</u> | *Subscribe to Our* <u>Email</u>
<u>Newsletter</u>

.   .   .

This <u>story</u> *originally appeared on* <u>ProPublica</u> *as "ISIS via WhatsApp:*
'Blow Yourself Up, O Lion'" and is re-published here under a Creative
Commons <u>license</u>.