Volume 10, Issue 9

The Cybercoaching of Terrorists: Cause for Alarm?

By John Mueller

A few Islamic State operatives have been contacting sympathetic prospective jihadis abroad via the internet to supply them with instruction and practical advice for carrying out terrorist acts. Some analysts have called this a "game-changer." However, the cybercoaching enterprise is fraught with difficulties. Above all, cybercoaches have little or no control over their charges who are very often naïve, voluble, incautious, gullible, incapable, and/or troubled. Moreover, the advice of the cybercoaches has often been anything but sagacious, and law enforcement operatives have often been able to enter the plot to undermine the effort entirely.

As the Islamic State retreats in the Middle East, it has been become exceedingly difficult for the group to attract foreign fighters to travel to join its ranks in Iraq or Syria.[1] Moreover, infiltrating trained fighters back home to do damage—once a top concern—has proven to be difficult as well, though not impossible.

In consequence, a few Islamic State operatives have been contacting sympathetic prospective jihadis abroad via the internet. The primary goal of this process is not simply to inspire them or to urge them on—that, after all, has been going on for a long time, in particular in response to the influential online speeches and sermons of the late Anwar al-Awlaki of the al-Qa`ida branch in Yemen.[2] Rather, cybercoaches are different in that they not only urge their contacts on, but supply them with instruction and specific practical advice.

The most common take on cybercoaching is to envision it as a new threat, or "a critical terrorist innovation."[3] In this, cybercoaches are seen to "offer would-be terrorists all the services once provided by physical networks."[4] They "draw from and advise a population of supporters abroad who have expressed an interest in carrying out attacks, but who may lack the technical or operational knowledge to do so."[5] In an examination of the phenomenon in this publication, Seamus Hughes and Alexander Meleagrou-Hitchens conclude that it constitutes "a game changer" that poses "a complex challenge to counterterrorism authorities."[6]

Concern and watchfulness are certainly justified, but, as will be suggested in this article, the experience thus far suggests that the cybercoaching enterprise is fraught with difficulties. Above all, cybercoaches have little or no control over their charges who are very often naïve, voluble, incautious, gullible, incapable, and/or troubled—qualities that are often underappreciated, and sometimes even unacknowledged, in official, journalistic, and academic accounts.[7] It is not at all clear how distant coaches can make up for, or even fully appreciate the extent of, these inadequacies. Moreover, their advice has often proved to be anything but sagacious, and it is entirely possible—and in many cases, not particularly difficult—for law enforcement operatives to uncover and enter the plot, not only to further complicate the task of their devious counterparts abroad, but to undermine their efforts entirely.

The Cybercoaching Record

In its Sunday, February 5, 2017, edition, *The New York Times* presented on its front page a lengthy article, "Not 'Lone Wolves' After All" by Rukmini Callimachi that seeks to demonstrate "How ISIS Guides World's Terror Plots From Afar."[8] Callimachi argues that "in several, a pattern has emerged." In this, a supporter "initially tries to reach Syria, but is either blocked by the authorities in the home country or else turned back from the border. Under the instructions of a handler in Syria or Iraq, the person then begins planning an attack at home."

Callimachi does an excellent job discussing the cybercoaching phenomenon, which she reported had become a critical focus of counterterrorism officials on both sides of the Atlantic. However, the evidence in the article also suggests that the effort thus far has been an abject, even almost comedic, failure. The article is centered on an effort by Islamic State cybercoaches over no less than 17 months to get the apparent leader of a small band of sympathizers in India to commit some violence in its name. Apparently working with a congenial criminal network in India, one of the coaches was able to supply the distant conspirators with two rusty pistols and 20 bullets that were accordingly unusable.

The *New York Times* piece later reveals that police, through wiretaps, were able to close down the whole scheme shortly after the conspirators found they could not fabricate bombs—out of materials surreptitiously supplied by their handler—by following the YouTube instructional video sent to them by their handler. "We could not succeed in making powder, as it became jellylike paste," one lamented. The plotters proved to be anything but dedicated jihadis. Once arrested, they cooperatively told the authorities all they knew about their plans and connections.

The article is peppered with similar tales of failure and inadequacy. One of the coached accidentally shot himself in the leg. Another was supposed to drive over people but attacked with an ax instead because he did not have a driving permit. A third detonated a bomb, prematurely killing only himself. The explosive in another's suicide vest proved insufficiently lethal even to smash a nearby flowerpot.

About the only "success" for the cybercoaches seems to have been

John Mueller is a senior fellow at the Cato Institute and a political scientist at Ohio State University. Among his books are Overblown, Atomic Obsession, *and with Mark Stewart,* Terror, Security and Money, Chasing Ghosts, *and* Are We Safe Enough?

the slitting of the throat by two teenagers of an 85-year-old priest in northern France.[9]

The only example of cybercoach work in the United States that is dealt with in detail in the Callimachi article is a case in Rochester, New York, in which 25-year-old Emanuel Lutchman, looking for ways to get to Syria, was encouraged by his Islamic State handler to conduct a local terrorist attack to demonstrate his devotion to the cause. Their idea was to launch a machete attack in a bar on New Year's Eve, somehow killing, in the extravagant words of his distant coach, "1000000s of *kuffar* [infidels]."[10]

Additional information available on the case strongly suggests that Lutchman was rather inadequate for the mission.[11] He had spent most of the previous 10 years in prison for various offenses, the first of which was robbing a man of such items as his cell phone, baseball hat, bus pass, library card, and cigarettes. He was also mentally ill and was apparently no longer taking his prescribed medication. He had tried to commit suicide several times, most recently by stabbing himself in the stomach. He had no money, job, or resources, and he was given to picking up cigarette butts outside the targeted bar from which he had repeatedly been shooed away by its irritated owner who described him as an "aggressive panhandler."

Lutchman attracted the attention of the FBI when he posted favorable commentary about violent jihad and about the Islamic State on the web—rather foolish because he soon found himself—first on the internet and, then in physical reality—at the center of what he believed to be a terrorist cell of four. The other three members were all what the FBI calls "confidential sources." As part of their sting operation, they provided $40 Lutchman didn't have to buy a machete and other items from a local Walmart. Any terrorist "threat" presented by the hapless Lutchman and his remote cybercoach, then, was pretty modest.

In their article in this publication on the cybercoaching phenomenon, Hughes and Meleagrou-Hitchens assess the American cases relying substantially on court documents—which are, of course, mostly materials put out by the police and prosecutors. The article is well constructed and informative. But it, too, supplies quite a bit of information that can be taken to highlight the inadequacies both of the coaches and the coached.

Although their discussion includes efforts to get Americans to go abroad to fight with the Islamic State in the Middle East, they particularly focus on terrorist plots to do damage within the United States in which cybercoaches were involved. They find six of these in 2015 and only one in 2016—a positive trend, but one, they warn, that "may change."[12]

In the United States at least, the available evidence suggests that counterterrorism authorities have thus far met any challenge presented by the cybercoached quite well and that any value added to a plot by the coaches has been modest at best.

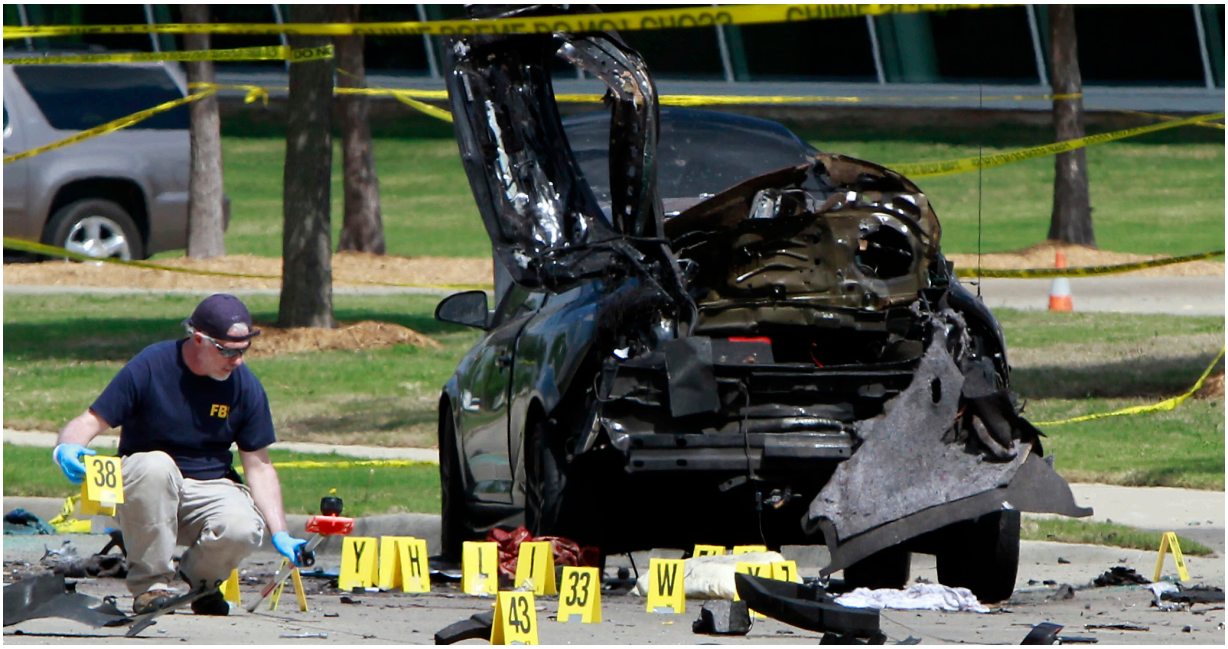
Among the six 2015 cases, there is, of course, Lutchman. Another is from Cincinnati where 21-year-old Munir Abdulkater, yearning to join the Islamic State in Syria, connected with an Islamic State cybercoach—a displaced British national named Junaid Hussain—who aided him in putting together a plot that was wildly improbable, if "chilling" in the characterization of the sentencing memorandum.[13] In this, the eager young man would raid a local soldier's home, behead him, record the deed, and send the recording to the Islamic State. Then Abdulkater would dress in the soldier's uniform (a specific suggestion of his cybercoach) and go to a police station where he would throw pipe bombs and engage the police in a shootout until death. In preparation, he visited a shooting range and handled a gun apparently for the first time in his life, which he described as a "whole new experience … I love it!"[14]

Additional information in the sentencing memorandum indicates that Abdulkater had attracted the attention of the FBI by tweeting nearly daily about his admiration for the Islamic State and his enthusiasm for beheadings. An FBI confidential source communicated with Abdulkater and the distant cybercoach about a plot to carry out an attack, in which he (the source) would participate. He also accompanied Abdulkater when he shopped for a suitably sharp knife at Walmart, planning to return to buy it after he had shaved his beard so he would look less "suspicious." Abdulkater was under full FBI surveillance at the shooting range, and he was arrested after purchasing an AK-47 rifle in a sting operation.[15] It apparently never occurred to cybercoach Hussain that the other participant in the plot might be an FBI informant.

Another case involves two men who drove from Arizona to Garland, Texas, to shoot up an anti-Muhammed cartoon contest that they presumably knew would have special security. They were rather well prepared: they had six guns and were wearing body armor. But when they opened fire, they were dispatched in 15 seconds by a traffic cop armed only with a pistol. The only other casualty was an unarmed security officer who was wounded in the ankle. The perpetrators seem to have had some encouragement from afar, and they exchanged over 100 encrypted messages on the morning of the attack—messages that may have urged them on, but did not, it certainly seems, improve their effectiveness.[16] As it happens, what could be interpreted as encouragement came from an undercover FBI special agent. Court documents revealed in mid-2016, a year after the Garland attack, that the agent had been communicating with at least one of the Arizona terrorists and, a few days before the attack, had urged them to "Tear up Texas." The operative, based in Ohio, even drove to Garland and took a picture of the event. The U.S. government argued the communication did not amount to incitement.[17]

There is also the case of a three-man conspiracy in New England to behead the woman who had organized the offensive cartoon contest. As Hughes and Meleagrou-Hitchens note, it was, in part, their contact with distant cybercoach Hussain that alerted the police. They also consider the plot to have been in the "advanced stages," and indeed the conspirators had purchased some knives through Amazon.[18] Beyond this, however, about all they had done was to talk and conduct some internet searches about, for example, firearms, flammable chemicals, what tranquilizer puts humans to sleep instantly, and how to start a secret militia. And any input from Hussain was soon abandoned when one of them, saying he couldn't wait any longer, decided to "go after" the "boys in blue" instead.[19] When he was approached in a parking lot by a group consisting of a Boston police officer and no less than five FBI agents who had been surveilling him, he moved toward them brandishing his knives and was shot dead.[20]

A somewhat similar pattern was found in a case in New York. Some Islamic State-inspired men were in various early stages of plotting some terrorist attacks, and the FBI received a tip about their efforts from a "confidential human source" who had talked to one of the loose-lipped conspirators.[21] The FBI then launched a search, and one of its agents was repeatedly stabbed by one of them with a large kitchen knife that failed to penetrate his agent's body armor. As Hughes and Meleagrou-Hitchens note, there seems to



A member of the FBI Evidence Response Team investigates the crime scene outside of the Curtis Culwell Center after a shooting occurred the day before, on May 4, 2015, in Garland, Texas. (Ben Torres/Getty Images)

have been little or no cybercoaching in this case, except that Hussain gave his blessing to the endeavors from afar and asked for a martyrdom video when the conspirators were ready to spring into action.[22]

Then there is the case of the shy and socially awkward 18-year-old Justin Sullivan in North Carolina who spent his time alone in his room with his computer and phone. It was there that he discovered the Islamic State at a time when it seemed to be very much on the rise, and that led him to Islam. "I liked IS from the beginning then I started thinking about death and stuff so I became a Muslim."[23] He was especially drawn to Islamic State videos featuring immolations and beheadings.[24] When his parents were away, Sullivan murdered a disabled 74-year-old recluse in the neighborhood, possibly to get money.[25] Later, his father alerted the police when his son began destroying "Buddhas, and figurines, and stuff," sometimes by pouring gasoline on them. Sullivan was soon being watched by the FBI online. As part of the investigation, an FBI undercover employee posing as a potential recruit to the cause got in touch with him electronically and worked his way into the young man's confidence. Sullivan was also in contact with encouraging and supportive Islamic State cybercoaches abroad, in particular Hussain.[26]

Harboring a grandiose scheme to set up "The Islamic State of North America," Sullivan discussed various plans for committing a terrorist attack in the United States with what he thought were his two cyber accomplices. He soon settled on shooting up a nightclub or a concert with an assault rifle, and reckoned he would need about 20 bullets, possibly coating them with cyanide, to kill off his estimated 25 to 50 victims.[27 a] When a package arrived from the FBI undercover employee containing a silencer for the yet-to-be-purchased rifle, his parents demanded an explanation. Sullivan became "aggressive" and later contacted the FBI undercover employee, urging the FBI agent to kill his (Sullivan's) parents—or as he called them, "the people I live with."[28] At some point, Sullivan also texted Hussain in Syria, saying he would "very soon" be "carrying out 1st operation of Islamic State of North America." Hussain responded, "Can u make a video first?" Sullivan said he would not do the video because this was not a suicide mission, but only the opening salvo in his planned campaign to halt "satanic" American airstrikes on his beloved Islamic State. "For major attack we will film, not this."[29] Judging from the information available, this may be just about the only 'coaching' Sullivan's distant cyber contact ever did. Triggered by Sullivan's death threats against his parents as communicated to his other cyber collaborator, the FBI arrested him. Some two months later, Junaid Hussain was killed in an airstrike in Syria.[30] It seems that Sullivan and the FBI undercover employee never actually met face-to-face.[31]

Finally, in the lone case from 2016, the cybercoach unwittingly connected an extremist with an agent working for the other side—any value he added to the plot was, therefore, negative. A former national guardsman in his mid-20s from Virginia, Mohamed Bailor Jalloh ventured to Africa with the notion of joining the Islamic State in Libya. He decided he was not ready to fight yet, but connected with an Islamic State cybercoach willing to help him conduct ji-

a Hughes and Meleagrou-Hitchens note that Sullivan once said it was his desire to kill up to 1,000 people. Seamus Hughes and Alexander Meleagrou-Hitchens, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," *CTC Sentinel* 10:3 (2017), p. 3. His plan, far-fetched like those of so many other prospective jihadis in the United States, was to carry out this attack and "then leave" to carry out further mayhem later on until, presumably, he had reached his extravagant goal. United States of America v. Justin Nojan Sullivan, Factual Basis, p. 8.

had back in the United States. Unaware that he was doing so, note Hughes and Meleagrou-Hitchens, the coach connected Jalloh with a contact who happened to be an FBI informant.[32] Eager to be led, the ex-guardsman said, "I will support with whatever you need from me, I need the reward from Allah and my sins to be forgiven." He was arrested in a sting orchestrated by the FBI after he purchased an assault rifle in a gun shop for the planned deed.[33]

There appears to have been more Islamic State cybercoaching in Europe than in the United States. Petter Nesser and his colleagues tally 38 "well-documented" planned or launched plots there between 2014 and November 1, 2016, that "involve some kind of IS-link." Of these, they say that 19 "involve online instruction," though three of these involve people with foreign fighter experience.[34] The cybercoaching cases are not clearly laid out in the article, but in its appendix, some 13 plots are described with the words "instructed online" or "instruction online" or "likely instructed online" or "online contacts in Syria, possible instruction" or "had online IS contacts, possible instruction?" or "told friend she had received instruction from higher-ups in IS."[35] (These cases overlap with the ones discussed by Callimachi, of course.)

In contrast to the seven American cases in which no one perished (except, in some instances, the terrorists), casualties were inflicted in some of these European plots. However, with the exception of the murder of the elderly French priest, it is less than clear that cybercoaching, in the sense of providing key information and direction, played a substantial role in fatal attacks.

There are two other cases in the set in which fatalities were inflicted. One was a knifing at the home of a Paris policeman in which two were killed by a man who was suspected of being influenced by a cybercoach.[36] And the other was the violence inflicted by Amedy Coulibaly who killed a French policewoman and then four hostages in a Jewish supermarket in early 2015. The degree to which Coulibaly was a neophyte in need of instruction is questionable, however. As Nesser and his colleagues point out, he had been part of a jihadi network in France that went back to 2003.[37]

Beyond these cases, there is the truck attack at a Christmas market in Berlin that killed 11 in December 2016 (after the article by Nesser, Stenersen, and Oftendal was published). The culprit, a high school dropout with an attraction to drugs and alcohol, had been part of a network in contact with Islamic State operatives for some time, and he also had jihadi mentors and friends in Germany. The degree to which cybercoaching may have played a role in this case is, to say the least, unclear. According to Georg Heil's study in this publication, there is "the possible presence of external attack plotters" in the case, and "remote control guidance" was "possibly a feature" of the attack due to "suspected communication with Islamic State operatives in Libya."[38]Another account indicates that the truck attacker had been thinking about carrying out a "project" in Germany for a year or more, had searched for information on the internet concerning the construction of bombs, and had been in contact with members of Islamic State in Libya (possibly with relatives who had joined the group there).[39] However, as with the Heil article, there is no specific information that cybercoaching played a role in the specific planning for the eventual attack that took place.

In contrast, as Nesser and his colleagues point out, the vast majority of the deaths perpetrated by terrorists in Europe in the 2014-2016 period were accomplished in three attacks that were carried out in two instances by cells trained and dispatched by the Islamic State and in one instance (the Nice attack) in which no evidence has yet publicly come to light about communications with terrorists overseas.[40] That is, no cybercoaching was apparently involved.[b]

There seems to be little indication that cybercoaching, or even much connection to the Islamic State, was involved in any of the three lethal terrorist attacks in England in 2017 or in the several plots disrupted there over the same period. The largest of the attacks killed 22 with a bomb—the first to be successfully set off in Britain by terrorists since 2005—and the attacker may have had some training on visits to his native Libya.[41] Although there are suspicions about an Islamic State connection to attacks in Catalonia in August 2017, there is little evidence of this thus far, and none at all about cybercoaching.[42]

However, cybercoaching, or a form of it, does seem to have played a role in terrorism plotting in Australia in 2017. Information about the case is still limited and subject to sometimes contradictory statements by Australian and Lebanese officials, but it centers on four Lebanese-Australian brothers. One of them had been in Syria for years and had become an Islamic State commander, and consequently, the Lebanese intelligence services began monitoring the telephones of all four men in 2016, according to the version of events provided by Lebanese officials.[43] In April 2017, as the Islamic State was increasingly under siege, the Islamic State brother contacted the others and urged them to conduct some diversionary terrorism in Australia. When they agreed, they were put in touch with an Islamic State cybercoach in Syria, and explosive materials, disassembled bomb components, and instructions were sent to them by the Islamic State from Turkey.[44]

On July 15, one of the brothers, say Australian police, was set to board an airliner to the Middle East with one assembled bomb in his luggage.[45] However, the Lebanese interior minister said there were two bombs—one of them in a meat grinder and the other in a large Barbie doll.[c] The intent, he alleged, was to detonate one or both of them 20 minutes into the flight when the plane was still over Australia. However, he said, the luggage was well over the weight limit allowed on the airline—a rather elemental consideration the scheming brothers and their distant handlers had apparently not pondered earlier.[46] [d] Whatever the reason, the plot was aborted, and the brother boarded the flight unencumbered while one of the others took the bomb (or bombs) back and disassembled them.[47] According to Lebanese authorities, the traveling brother told authorities he was going to Lebanon to have a wedding at the family home there. Because he had used the same reason in several earlier trips, he was pulled aside for questioning when he arrived in Beirut, and he soon spilled information about the plot.[48] In their press

b It should also be pointed out that however terrible the outrages committed in Europe in the period, far more people on that continent perished yearly at the hands of terrorists in most years in the 1970s and 1980s. Chris York, "Islamic State Terrorism Is Serious But We've Faced Even Deadlier Threats In The Past," Huffington Post, November 29, 2015. See also Daniel Byman, "Trump and Counterterrorism," *National Interest*, January/February 2017, p. 67 and Jeremy Shapiro, "Why we think terrorism is scarier that it really is (and we probably always will)," vox.com, March 28, 2016.

c The use of the meat grinder seems to make little sense. Unlike a pressure cooker, it is open at one end, allowing the blast pressure to be released. Author correspondence, Mark Stewart, academic, September 2017.

d Australian police stated they were looking into whether the plot was aborted because the luggage was too heavy. Australian Federal Police, Press Conference, Sydney, August 3, 2017, available at https://twitter.com/AusFedPolice/status/893244987315331072

conferences soon after the plot became public, Australian police, however, said they did not believe he knew about the plot.[49]

Intelligence information forwarded to Australian authorities was enough not only for them to surveil and then to arrest the brothers, but also to put together a mock-up version of the explosive. They concluded that, although the brothers had built a "fully functioning IED" (improvised explosive device), the explosive would never have made it through security. "We had a 100-percent success rate in terms of our mock IED being picked up"[50] … and "we are extremely confident that … that IED would have been picked up by security."[51] However, since the bombs had been disassembled, the police presumably were not in a good position to evaluate the would-be terrorists' handiwork.[52]

The brothers were arrested as they, urged on by their handlers, turned their attention for some reason from bombs to fabricating a device to disperse the poison gas hydrogen sulfide. But, the Australian police stress, they were a very long way from completion.[53]

The Australian case differs from the others in that the cybercoaches did not pick up their distant collaborators more or less randomly on the internet but connected because they were personally known by (and related to) a senior Islamic State operative. But there were, nonetheless, many blunders in carrying out the mission. Most important was that the brothers, following instructions and using materials supplied by the coaches, fabricated a bomb that was apparently too heavy to go onboard, and that, according to Australian police, had a 100-percent chance of being detected even if it had been put through airline security.

Impact, Difficulties, and Perils of Cybercoaching

Overall, it certainly seems that Brian Michael Jenkins' summary assessment of Islamist terrorists in the United States applies as well to the cybercoached both there and in Europe: "Their numbers remain small, their determination limp, and their competence poor."[54] Cybercoaching scarcely seems to be much of a game changer or a critical terrorist innovation.

Cybercoaches can urge their charges on and stress glorious reward in this life or in one after. But that scarcely differentiates them from a wide array of Islamic State propagandists on the web or from instances in the past when some local jihadis managed to get in direct contact with supportive terrorists abroad (or with FBI informants and agents pretending to be so). Any effort by cybercoaches to go beyond this, to actually supply their charges with information and resources that are materially helpful—to guide the "world's terror plots from afar," in the words of the *New York Times* headline—is fraught with difficulties.

The distant cybercoaches obviously do not really know the territory, and the lack of face-to-face contact impedes efforts to assess the dedication, and particularly the capabilities, of the coached. Daveed Gartenstein-Ross and Madeleine Blackman do acknowledge that "the lack of in-person training is a disadvantage."[55] However, this seems to be a considerable understatement. Although even the hopelessly inadequate can sometimes get lucky, Michael Kenney finds that would-be terrorists characteristically are operationally unsophisticated, short on know-how, prone to make mistakes, poor at planning, and limited in their capacity to learn.[56] Accordingly, he suggests, there is no substitute for direct, on-the-ground training and experience.[57]

Moreover, the advice and assistance tendered by the cybercoaches has often been of questionable value. If an apparent authority figure tells his confidante to "go out and stab somebody," that may provide a degree of motivation in some cases. But it scarcely seems like a substantive contribution. And, as noted, the cyber assistance in the Australian case generated bombs that likely would have been detected by airline security even if they had not been too heavy to take on board.

In addition, there is a great danger that the plot will come to the attention of the police. Although communications can be encrypted as the plot develops, they cannot be at the outset if there is not already a connection. For the most part, coaches must find their charges, and the charges must find their coaches, out in the cyber-open. This effect is amplified by the widespread tendency of American jihadis to advertise their passions and often their violent fantasies on open social media like Twitter and Facebook. There have been many cases in which the would-be perpetrator used chat rooms or Facebook or Twitter to seek out like-minded individuals and potential collaborators, and usually they simply connected to the FBI.[58] Indeed, as Daniel Byman and Jeremy Shapiro and others have pointed out, the foolish willingness of would-be terrorists to spill their aspirations and their often far-fetched fantasies on social media has been, on balance, much to the advantage of the police seeking to track them.[59] The internet, it can be argued, has facilitated the counterterrorists far more than the terrorists.

Interestingly, in five of the seven cybercoach cases in the United States identified by Hughes and Meleagrou-Hitchens, the would-be jihadis attracted not only the attention of a cybercoach from "afar," but also one—or, in the case of Lutchman, three—informant(s) or undercover agent(s) from the FBI. Indeed, police and intelligence operatives have sometimes even been able to connect with the distant Islamist cybercoaches directly. And in each case, the cybercoach naively assumed, because his charge was also duped, that the FBI interloper was actually a legitimate co-conspirator. In fact, in one case, as noted, the Islamic State coach actually put his charge in contact with an FBI informant in the United States who the coach thought was on the Islamic State's side.

And people working for the FBI on such cases have tremendous advantages over their distant rivals. They can actually materialize if necessary, and they are likely to know the local territory in detail—or can find it out by contacting local police.

It also appears that being a cybercoach is a perilous occupation. As Hughes and Meleagrou-Hitchens note, four of the most influential cybercoaches were killed in 2015 and 2016, and a fifth was arrested.[60]

Back in the summer of 2016, Harry Sarfo, a German criminal who had joined the Islamic State in Syria, told *The New York Times* in a prison interview that "they have loads of people … hundreds definitely" who were "living in European countries and waiting for commands to attack the European people."[61]

Sarfo suggested, however, that it was more difficult to get operatives into North America. Therefore, for that venue, the group was going to rely on cybercoaching: "For America and Canada, it's much easier for them to get them over the social network, because they say the Americans are dumb—they have open gun policies … they say we can radicalize them easily, and if they have no prior record, they can buy guns, so we don't need to have no contact man who has to provide guns for them."[62]

It has not been that easy. CTC

Citations

1 Thomas Gibbons-Neff, "Number of foreign fighters entering Iraq and Syria drops by 90 percent, Pentagon says," *Washington Post*, April 26, 2016; Griff Witte, Sundarsan Raghavan, and James McAuley, "Flow of foreign fighters plummets as Islamic State loses its edge," *Washington Post*, September 9, 2016. On the decline, see John Mueller and Mark Stewart, "Misoverestimating ISIS: Comparisons with Al-Qaeda," *Perspectives on Terrorism* 10:4 (2016); Jacob Shapiro, "A Predictable Failure: The Political Economy of the Islamic State," *CTC Sentinel* 9:9 (2016).
2 Scott Shane, *Objective Troy: A Terrorist, A President, and the Rise of the Drone* (New York: Tim Duggan Books, 2015); Daveed Gartenstein-Ross and Madeleine Blackman," "ISIL's Virtual Planners: A Critical Terrorist Innovation," War on the Rocks, January 4, 2017.
3 Gartenstein-Ross and Blackman.
4 Daveed Gartenstein-Ross, "Lone Wolves No More: The Decline of a Myth," *Foreign Affairs*, March 27, 2017.
5 Bridget Moreng, "ISIS' Virtual Puppeteers: How They Recruit and Train 'Lone Wolves,'" *Foreign Affairs*, September 21, 2016.
6 Seamus Hughes and Alexander Meleagrou-Hitchens, "The Threat to the United States from the Islamic State's Virtual Entrepreneurs," *CTC Sentinel* 10:3 (2017), pp. 1, 8.
7 For an extended discussion of such terrorist qualities and the degree to which they are under-appreciated, see John Mueller and Mark G. Stewart, *Chasing Ghosts: The Policing of Terrorism* (New York: Oxford University Press, 2017), chapters 1, 3-4, and pp. 257-66.
8 Rukmini Callimachi, "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar," *New York Times*, February 5, 2017.
9 On this case, see Moreng. See also Jason Burke, "The myth of the 'lone wolf' terrorist," *Guardian*, March 30, 2017.
10 United States of America v. Emanuel L. Lutchman, Criminal Complaint, December 30, 2015, p. 5.
11 John Mueller ed., *Terrorism Since 9/11: The American Cases* (Columbus, OH: Mershon Center, Ohio State University, 2017), case 78 by Cassandra Dula, introduction by John Mueller from which the case description in the text is drawn; available at politicalscience.osu.edu/faculty/jmueller/since.html
12 Hughes and Meleagrou-Hitchens, p. 7.
13 United States of America v. Munir Abdulkader, Sentencing Memorandum, November 10, 2016, p. 4.
14 Hughes and Meleagrou-Hitchens, p. 3; United States of America v. Munir Abdulkader, Sentencing Memorandum, p. 13.
15 United States of America v. Munir Abdulkader, Sentencing Memorandum, pp. 3-13.
16 Mueller, Terrorism Since 9/11, case 66 by Sam Zacher. See also Rukmini Callimachi, "Clues on Twitter Show Ties Between Texas Gunman and ISIS Network," *New York Times*, May 11, 2015; Susan Zalkind, "How ISIS's 'Attack America' Plan Is Working," Daily Beast, June 22, 2015; James Eng, "FBI Director: Encrypted Messages Stymied Probe of Garland Shooting," NBC News, December 9, 2015.
17 "Affidavit in Support of an Application for a Criminal Complaint and Arrest Warrant," Case of Erick Jamal Hendricks, August 3, 2016; Katie Zavadski, "FBI Agent Apparently Egged on 'Draw Muhammad' Shooter," Daily Beast, August 4, 2016; Murtaza Hussain, "FBI Agent Goaded Garland Shooter to 'Tear Up Texas'," Intercept, August 9, 2016. See also "60 Minutes investigates first ISIS-claimed attack in U.S. and what the FBI knew," CBS News, March 26, 2017.
18 Hughes and Meleagrou-Hitchens, p. 3.
19 United States of America v. David Daoud Wright and Nicholas Alexander Rovinski, First Superseding Indictment, April 21, 2016, pp. 4-7.
20 Katherine Q. Seelye, "In Blurry Video of Boston Shooting, Officers' Retreat Is Clear but Knife Is Not," *New York Times*, June 8, 2015.
21 United States of America against Fareed Mumuni, Complaint, June 17, 2015, pp. 3-4.
22 Hughes and Meleagrou-Hitchens, p. 5.
23 United States of America v. Justin Nojan Sullivan, Bill of Indictment, January 20, 2016, p. 2.
24 Michael Gordon, "Teen talked of killing in the name of ISIS. But the question remains, why?" *Charlotte Observer*, February 24, 2017.
25 United States of America v. Justin Nojan Sullivan, Factual Basis, November 14, 2016, p. 2.
26 Gordon. Gasoline: United States of America v. Justin Nojan Sullivan, Criminal Complaint, June 22, 2015, p. 4.
27 United States of America v. Justin Nojan Sullivan, Factual Basis, November 14, 2016, p. 11. For cyanide reference specifically, see United States of America v. Justin Nojan Sullivan, Criminal Complaint, June 22, 2015, p. 7.
28 United States of America v. Justin Nojan Sullivan, Factual Basis, p. 12.
29 Ibid., pp. 9, 15-16.
30 Ibid., p. 5. For more on Hussain, see Lorraine Murphy, "The Curious Case of the Jihadist Who Started Out as a Hacktivist," *Vanity Fair*, December 15, 2015.
31 Author communication, Michael Gordon, journalist, May 2017.
32 Hughes and Meleagrou-Hitchens, pp. 4-5.
33 United States of America v. Mohamed Bialor Jalloh, Affidavit in Support of a Criminal Complaint, July 3, 2016, pp. 11, 13.
34 Peter Nesser, Anne Stenersen, and Emilie Oftendal, "Jihadi Terrorism in Europe: The IS-Effect," *Perspectives on Terrorism* 10:6 (2016): pp. 4-5, 9.
35 Nesser, Stenersen, and Oftendal, Appendix 2. (See note 29 in the article.)
36 Moreng; Burke; Jérémie Pham-Lê, Victor Garcia et Claire Hache, "Rachid Kassim, le djihadiste qui a inspiré les assassins du père Hamel," L'Express, August 18, 2016; Pierre Alonso and Willy Le Devin, "Les flux furieux de Rachid Kassim," Liberation, September 16, 2016; "Did jihadist Rashid Kassim lure French youths to plot attacks?" BBC News, September 15, 2016.
37 Nesser, Stenersen, and Oftendal, Appendix 1, pp. 9-10. (See note 5 in the article.)
38 Georg Heil, "The Berlin Attack and the 'Abu Walaa' Islamic State Recruitment Network," *CTC Sentinel* 10:2 (2017).
39 Florian Flade, "Was das LKA bei Amris Terror-Chat mitlas," *Die Welt*, March 27, 2017.
40 Nesser, Stenersen, and Oftendal, p. 3.
41 Raffaello Pantucci, "Britain on Alert: The Attacks in London and Manchester and the Evolving Threat," *CTC Sentinel* 10:7 (2017).
42 Allisa J. Rubin, Patrick Kingsley, and Palko Karasz, "How a Shadowy Imam Evaded Scrutiny and Forged the Barcelona Cell," *New York Times*, August 23, 2017.
43 "Alleged Barbie bomb plot revealed after marriage slip-up," *Australian*, August 24, 2017.
44 Paul Maley, "From Syria to Sydney: how the airport plot unfolded," *Australian*, August 5, 2017.
45 Australian Federal Police, Press Conference, Sydney, August 3, 2017, available at https://twitter.com/AusFedPolice/status/893244987315331072
46 "Plot foiled to blow up UAE-bound plane with Barbie doll bomb," Sky News, August 21, 2017.
47 Maley.
48 "Alleged Barbie bomb."
49 Australian Federal Police. Tom Westbrook and Jonathan Barrett, "Islamic State behind Australians' foiled Etihad meat-mincer bomb plot: police," Reuters, August 3, 2017.
50 Maley. Australian Federal Police.
51 Australian Federal Police.
52 On the difficulties of trying to take down airliner with an on-board bomb, see Mark G. Stewart and John Mueller, *Are We Safe Enough? Measuring and Assessing Aviation Security* (Amsterdam: Elsevier, 2017), pp. 74-77.
53 Maley. Australian Federal Police.
54 Brian Michael Jenkins, *Stray Dogs and Virtual Armies: Radicalization and Recruitment to Jihadist Terrorism in the United States since 9/11* (Santa Monica, CA: RAND Corporation, 2011), p. 1. See also Brian Michael Jenkins, *Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States since September 11, 2001* (Santa Monica, CA: RAND, 2010); Bruce Schneier, "Portrait of the Modern Terrorist as an Idiot," *Wired*, June 14, 2007; Risa A. Brooks, "Muslim 'Homegrown' Terrorism in the United States: How Serious is the Threat?" *International Security* 36:2 (2011): pp. 7-47; Louis Klarevas, "The Idiot Jihadist Next Door," *Foreign Policy*, December 1, 2011; John Mueller and Mark G. Stewart, "The Terrorism Delusion: America's Overwrought Response to September 11," *International Security* 37:1 (2012): pp. 81-110; Trevor Aaronson, *The Terror Factory* (Brooklyn, NY: Ig Publishing, 2013); Mueller and Stewart, *Chasing Ghosts*, pp. 91-100; Marc Sageman, *Misunderstanding Terrorism* (Philadelphia, PA: University of Pennsylvania Press, 2017). Also Michael Sheehan, *Crush the Cell: How to Defeat Terrorism Without Terrorizing*

Ourselves (New York: Crown, 2008). For the suggestion that many would-be terrorists in the West rather closely resemble those depicted in the brilliant fictional British film *Four Lions*, see Mueller and Stewart, *Chasing Ghosts*, pp. 112-115.

55 Gartenstein-Ross and Blackman.

56 Michael Kenney, "'Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft Among Islamist Militants in Britain and Spain," *Studies in Conflict & Terrorism* 33:10 (2010): pp. 911-922.

57 Michael Kenney, "Beyond the Internet: Metis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists," *Terrorism and Political Violence* 22:2 (2010): pp. 177-197. Another study documents the difficulties of network coordination that continually threaten the terrorists' operational unity, trust, cohesion, and ability to act collectively. See Mette Eilstrup-Sangiovanni and Calvert Jones, "Assessing the Dangers of Illicit Networks," *International Security* 33:2 (2008): pp. 7-44.

58 Mueller and Stewart, *Chasing Ghosts*, pp. 97-100.

59 Daniel Byman and Jeremy Shapiro, "We Shouldn't Stop Terrorists from Tweeting," *Washington Post*, October 9, 2014; Daniel Byman and Jeremy Shapiro, *Be Afraid. Be a Little Afraid: The Threat of Terrorism from Foreign Fighters in Syria and Iraq* (Washington, D.C.: Brookings Institution, Policy Paper 34, November 2014). See also Brooks; David C. Benson, "Why the Internet Is Not Increasing Terrorism," *Security Studies* 23:2 (2014): pp. 293-328; Ronald Bailey, "The Internet Does Not Increase Terrorism: Most terrorism takes place in Internet-free zones," Reason, November 28, 2014; and Fawaz A. Gerges, *The Rise and Fall of Al-Qaeda* (New York: Oxford University Press, 2011), p. 192.

60 Hughes and Meleagrou-Hitchens, p. 7.

61 Rukmini Callimachi, "A Global Network of Killers, Built by a Secretive Branch of ISIS," *New York Times*, August 4, 2016.

62 Ibid.

Contents

FEATURE ARTICLE

1 **Crime as Jihad: Developments in the Crime-Terror Nexus in Europe**
Rajan Basra and Peter R. Neumann

INTERVIEW

7 **A View from the CT Foxhole: Lisa Monaco, Former Assistant to President Barack Obama for Homeland Security and Counterterrorism**
Paul Cruickshank

ANALYSIS

13 **New Developments in the Islamic State's External Operations: The 2017 Sydney Plane Plot**
Andrew Zammit

19 **The Evolution of the Islamic State's Chemical Weapons Efforts**
Columb Strack

24 **The Hawija Offensive: A Liberation Exposes Faultlines**
Derek Henry Flood

29 **The Cybercoaching of Terrorists: Cause for Alarm?**
John Mueller

FROM THE EDITOR

In our October cover article, Rajan Basra and Peter Neumman explore the strong nexus between crime and jihadism in Europe. With a significant proportion of European foreign fighters having criminal backgrounds, they outline how the Islamic State is going out of its way to depict crime as helpful to its cause and to recruit criminals for terrorist enterprises. Our interview this month is with Lisa Monaco, President Obama's chief counterterrorism advisor during his second term.

In July, police in Sydney, Australia, discovered alleged plots by two brothers to detonate a bomb on a passenger jet and release poison gas on a target such as public transportation. Andrew Zammit outlines why it set off alarm bells in counterterrorism agencies worldwide. An Islamic State cybercoach in Syria allegedly arranged for a partially constructed bomb with military-grade explosives to be air-mailed to the plotters from Turkey and provided sufficient instructions for them to build a fully functioning device. This 'IKEA-style' approach to terrorism could be a game-changer because untrained Western extremists have hitherto found it difficult to make high explosives. The Islamic State cybercoach also transmitted know-how on making a poison gas dispersal device to the Australian cell.

Columb Strack looks at the evolution of the Islamic State's chemical weapons efforts in Syria and Iraq and the possibility that the group could export chemical terror to the West. John Mueller examines the degree to which the cybercoaching of terrorists should be cause for concern, arguing that in many cases cybercoaches have little control over their amateurish charges.

Finally, Derek Flood, recently back from the frontlines, outlines how the capture of Hawija, the Islamic State's last remaining urban stronghold in northern Iraq, exposed faultlines between Baghdad and Erbil, which set the stage for the dramatic events unfolding in the Kirkuk area.

Paul Cruickshank, *Editor in Chief*

CTC SENTINEL

Editor in Chief
Paul Cruickshank

Managing Editor
Kristina Hummel

CONTACT

Combating Terrorism Center
U.S. Military Academy
607 Cullum Road, Lincoln Hall
West Point, NY 10996
Phone: (845) 938-8495
Email: sentinel@usma.edu
Web: www.ctc.usma.edu/sentinel/

SUBSMISSIONS

The *CTC Sentinel* welcomes submissions. Please contact us at sentinel@usma.edu.

Cover: A bullet impact is pictured on a window in the entrance hall of a building on the Champs-Élysées avenue in Paris on April 21, 2017, a day after a gunman opened fire on police on the avenue, killing a policeman and wounding two others in an attack claimed by the Islamic State just days before the first round of the presidential election. (Philippe Lopez/AFP/Getty Images)