Testimony of

Evan F. Kohlmann

with Laith Alkhouri and Alexandra Kassirer

Before the

House Committee on Foreign Affairs
Subcommittee on Terrorism, Nonproliferation, and Trade

"The Evolution of Terrorist Propaganda: The Paris Attack and Social Media"

Charlie Hebdo and the Jihadi Online Network: Assessing the Role of American Commercial Social Media Platforms

January 27, 2015; 2:30pm

2172 Rayburn House Office Building

Washington D.C.

Evan F. Kohlmann
Co-Founder - Chief Innovation Officer
Flashpoint Global Partners; New York, NY
www.flashpoint-intel.com - info@flashpoint-intel.com
Voicemail/Fax: (206)202-4911

EVAN F. KOHLMANN
A Biographical Sketch

Evan Kohlmann is a co-founder of Flashpoint Global Partners, a New York-based "dark web" data mining and security consulting firm, and is responsible for innovation and product development. He has served as a private sector International Terrorism Consultant who has spent more than a decade tracking Al-Qaida and other terrorist organizations by studying their digital and online communications. Mr. Kohlmann has testified over thirty times as an expert witness in U.S. federal courts, and has served at various times as a contract consultant in terrorism matters on behalf of the U.S. Department of Defense, the U.S. Department of Justice, the Federal Bureau of Investigation (FBI), the Office of the High Representative (OHR) in Bosnia-Herzegovina, the International Criminal Tribunal for the Former Yugoslavia (ICTFY) at the Hague, the Australian Federal Police (AFP), the U.K. Crown Prosecution Service (CPS), Scotland Yard's SO-15 Counter Terrorism Command, the Central Scotland Police, West Yorkshire Police, the Danish Security and Intelligence Service (PET), and the Swiss Federal Prosecutor's Office. Mr. Kohlmann also currently serves as an on-air analyst on behalf of NBC News / MSNBC.

Mr. Kohlmann holds an undergraduate degree in International Politics from the Edmund A. Walsh School of Foreign Service (Georgetown University), and a graduate degree in law from the University of Pennsylvania Law School. Kohlmann is also the recipient of a certificate in Islamic studies from the Prince Alwaleed bin Talal Center for Muslim-Christian Understanding (CMCU) at Georgetown University.

As more young people from the United States and other Western countries—who have no prior links to Syria or the jihadi organizations fighting there—seek to depart to join the frontline in the Levant, there has been an increasing public awareness of the role that jihadi online social media and networks are serving in recruiting them to the cause and providing them with the basic guidance necessary to reach their destination. This has come both in the form of indirect recruitment (i.e. glossy English-language propaganda videos and magazines distributed on the Internet), as well as direct recruitment by Western jihadists in Syria and Iraq who have regular access to major commercial social media platforms like YouTube, Facebook, Twitter, Skype, Tumblr, and Kik. Several weeks ago, Zarine Khan—the mother of a 19-year-old Illinois man facing federal charges for attempting to travel to Syria—emotionally addressed a news conference and denounced "the brainwashing and recruiting of children through the use of social media and the Internet… We have a message for ISIS, Mr. Baghdadi and his fellow social-media recruiters: Leave our children alone!"[1]

The influx of Americans and other social-media-savvy Westerners seems to have bred a noticeable divergence from traditional proprietary Arabic-language jihadi chat forums to the slicker interfaces and enormous global audience afforded by services like Facebook and Twitter. The odd sense of comfort that Western jihadists fighting in Syria and Iraq feel in using such platforms is somewhat disturbing. After engaging in live discussion for several hours last October via the Kik Messenger service with Farah Shirdon, a Somali-Canadian ISIS fighter in Mosul, he told me, "for the next week I'll be busy going to Syria to handle some[thing] so we need to finish this up tomorrow." Young millenials like Mr. Shirdon are so confident in the reliability and security of these big name social media companies that they have not even a second thought about disclosing such potentially sensitive information—even to known adversaries.

The trend towards jihadists exploiting (and indeed relying upon) Western commercial social media platforms for their online communications has been in full view in the aftermath of this month's terrorist attacks in Paris. Though relatively little is known about how the Kouachi brothers and Amedy Coulibaly were using social media prior to the attacks, claims of responsibility for the tragic events in Paris emerged quite quickly from Al-Qaida in the Arabian Peninsula (AQAP)—all of which were distributed exclusively via Twitter. On January 9, an account purportedly run by a fighter in the ranks of AQAP, "Bakhsarouf Al-Yemen," tweeted that AQAP was behind the attack and promised his followers that an official claim of credit would soon be released, but that it had been delayed due to "security reasons."[2] The Twitter user directly addressed "the relationship between Al-Qaida and the Charlie Hebdo battle: the relationship is direct and the operation was supervised by Al-Qaida's branch in the Arabian Peninsula. The operation was directed by the leadership of AQAP, and they chose these targets carefully, to avenge the honor of our prophet... and in France specifically, for its role that is not hidden in the war on Islam."[3]

Later on the same day, AQAP's official Al-Malahem media wing used its account on Twitter to disseminate download links for an audio message of AQAP official Hareth

[1] Tarm, Michael. "Mother of Chicago teen to Islamic State: 'Leave our children alone!'" Associated Press. January 13, 2015.

[2] https://twitter.com/ba_yman/status/553652768628813825

[3] https://twitter.com/ba_yman/status/553652768628813825

al-Nadhari praising the Paris attacks and condemning France: "men from among the faithful soldiers of Allah embarked and taught them how to be polite and the limits on freedom of expression; soldiers came to you who love Allah and his messenger, who do not care about death, and who are fond of martyrdom for the cause of Allah… O' heroic mujahideen... may your hands be preserved... I wish I was there with you."[4] On January 14, again using the same Twitter account, AQAP distributed download links for a direct claim of responsibility for the Paris attacks in the form of a video from senior AQAP leader Nasr bin Ali al-Ansi.[5] In the video, al-Ansi declared that AQAP engineered the attacks "as a vengeance for the Messenger of Allah. We clarify to the ummah that the one who chose the target, laid the plan and financed the operation, is the leadership of the organization." Al-Ansi further mocked the unity rallies that took place in Paris in the wake of the attacks: "Look at how they gathered, rallied and supported each other; strengthening their weakness and dressing their wounds. Those wounds have not healed and they won't, be it in Paris, New York or Washington, or in London or Spain."[6]

In fact, as of the time of this testimony, AQAP—a designated foreign terrorist organization according to U.S. law—has not one, but two official accounts on Twitter—one for releasing videos and recordings and the other for releasing statements and breaking news updates. Nor is AQAP alone—other allied factions such as Al-Qaida in the Islamic Maghreb (AQIM) have also begun to eschew the traditional established route of publishing jihadi media through password-protected proprietary jihadi chat forums and instead they have been releasing material directly via Twitter. This process has taken place quite seamlessly despite reported initiatives by Twitter to curb the use of its network for terrorist propaganda in the wake of the recorded beheadings of James Foley and other Western journalists captured in Syria. Over the past three months, AQAP's public Twitter account has only been disabled by system administrators on four occasions. Each time it has been disabled, AQAP has merely created a new account with the same name, appended with "1", "2", "3", and "4" respectively. Thus, there is hardly any mystery in what Twitter account AQAP will register next.

The failure of Twitter to learn from and adapt to this rudimentary pattern would suggest fundamental failures in its responsibility to prevent its service from becoming a mouthpiece for terrorist organizations. One jihadist has smugly advised Twitter to simply sit back and "let us continue spread our daawah (JIHAD)" because the company's current efforts aimed at thwarting such uses are pointless: "it takes 2 minutes to get new acc[ounts]."[7] It should be emphasized that AQAP's videos and statements about the Paris attacks have only been released on Twitter, and—weeks later—still have yet to appear in the areas of elite Arabic-language jihadi chat forums that are reserved for the group. This means that Twitter is not only their preferred means of propaganda distribution, it is verging on being their sole one as well. While Twitter's CEO Dick Costolo has insisted that Twitter is "actively suspending accounts as we discover them", the company also acknowledges that some offending accounts are nonetheless left online

[4] https://twitter.com/AMOJAH3/status/553666443355910144
[5] https://twitter.com/amojah3/status/555305155437268992
[6] https://twitter.com/amojah3/status/555305155437268992
[7] https://twitter.com/Abuhaitham12/status/559324286314618880

by system administrators due to "public interest factors such as the newsworthiness of the content."[8]

Nonetheless, Twitter is not the only offender here. The primarily text-based communication service may be ideal for rapidly distributing download links, but not broadcasting the video files themselves. The actual AQAP audio and video content addressing the Paris attacks are hosted on services that include Google's YouTube streaming service; Shenandoah, Texas-based cloud storage company Mediafire.com; and the San Francisco-based 501(c)(3) non-profit Internet Archive (www.archive.org). While YouTube and Mediafire.com have become somewhat more adept at disabling terrorist propaganda hosted on their networks, the Internet Archive has become the de-facto preferred storage point for jihadi audio and videos, whether from AQAP or ISIS. Archive.org was founded in 1996 with the noble intent of building an Internet library and providing "permanent access" to "historical collections that exist in digital format."[9] Unfortunately, in the present era, the term "historical collections" is now broad enough to encompass jihadist propaganda in the form of graphic beheading and execution videos, suicide bombings, and claims of responsibility for the attacks in Paris—which have been permanently preserved on Archive.org in their original, high-resolution formats. The fact that this powerful propaganda remains easily accessible raises the question of when the principles of open reporting and freedom of speech can or should be extended to include incitement to racial and ethnic hate, and calls for violence from terrorist organizations.

This leads to another aspect of jihadi social media that surfaced as a result of the Paris attacks: the apparently conflicting video released on January 10 that featured Amedy Coulibaly claiming responsibility for the attacks in the name of ISIS. In the video, Coulibaly condemned recent Western airstrikes on ISIS and insisted, "You act like the victims as if you don't understand what's been happening for months… If you attack the Caliphate, if you attack the Islamic State, we will attack you. You can't attack and not expect a response."[10] He also explained the nature of his relationship with the Kouachi brothers: "Brothers in our team divided themselves in two... We worked partly together, but also partly separate, it's more like a pact." Links to the Coulibaly video were first posted in a general discussion room of the main ISIS online chat forum Alplatformmedia.com by an ordinary registered user "Amir Monsaf"—and not by an authorized courier from ISIS' official media wing.[11] After the content of the video became clear, the message containing the download links was moved by forum administrators to the official ISIS media room. This sequence of events, and the lack of any watermark on the video from an official ISIS media unit, strongly suggests that it was produced and distributed by unknown parties independent of ISIS. As with the AQAP videos, the video of Mr. Coulibaly itself was hosted on YouTube, the Internet Archive, and several other U.S.-based cloud hosting services.

The natural question that follows from this analysis is how does ISIS manage to reliably operate its own official proprietary dot-com social media platform on the Internet in order to disseminate videos such as the beheading of James Foley and the

[8] Parkinson, Hannah Jane. "James Foley: How social media is fighting back against Isis propaganda." Guardian (London). August 20, 2014.
[9] https://archive.org/about/
[10] http://www.alplatformmedia.com/vb/showthread.php?t=77118.
[11] http://www.alplatformmedia.com/vb/showthread.php?t=77118.

"martyrdom" will of Amedy Coulibaly? The answer is another San Francisco-based American tech security company called CloudFlare, which aims to shield Internet websites and resources from being targeted by spammers, cybercriminals, and frustrating denial-of-service attacks. CloudFlare, which boasts that 4% of all web requests flows through its network, in essence serves as gatekeeper to control the flow of visitors to given sites and to verify that those visitors have a legitimate purpose in visiting them.[12] It has advanced detection features that complicate (or thwart entirely) attempts by automated robots to scrape data from and monitor these forums, including browser tests and so-called "captcha codes." In fact, two of ISIS' top three online chat forums—including the notorious Alplatformmedia.com—are currently guarded by CloudFlare. Without such protection from CloudFlare, these sites would almost certainly succumb to the same relentless online attacks that have completely collapsed several major jihadi web forums over the past two years.

In 2013, after CloudFlare was contacted by journalists over allegations that their service was providing protection to terrorist websites, the company's CEO Matthew Prince published a full explanation of their policy in this regard. According to Prince, it would not "be right for us to monitor the content that flows through our network and make determinations on what is and what is not politically appropriate. Frankly, that would be creepy… Removing this, or any other site, from our network wouldn't remove the content from the Internet: it would simply slow its performance and make it more vulnerable to attack."[13] In his response, Prince also asserted:

> "A website is speech. It is not a bomb. There is no imminent danger it creates and no provider has an affirmative obligation to monitor and make determinations about the theoretically harmful nature of speech a site may contain… There are lots of things on the web I find personally distasteful. I have political beliefs, but I don't believe those beliefs should color what is and is not allowed to flow over the network. As we have blogged about before, we often find ourselves on opposite sides of political conflicts. Fundamentally, we are consistent in the fact that our political beliefs will not color who we allow to be fast and safe on the web."[14]

In June 2010, in the context of the case of Holder v. Humanitarian Law Project, the U.S. Supreme Court upheld a strict view of the "expert advice and assistance" clause of U.S. counterterrorism laws, making even nonviolent advocacy potentially an illicit form of material support if it is carried out in conjunction with a proscribed terrorist organization.[15] The case had specifically centered on a group of American civil rights activists who advertised their mission as helping such groups "find peaceful ways to achieve [their] goals." It is extremely difficult to reconcile the logical paradox that it is currently illegal to give pro-bono assistance to a terrorist group in order for them to adopt politics instead of violence, but it is perfectly legal for CloudFlare to commercially profit from a terrorist group by assisting them to communicate securely with recruits and to publicly disseminate recordings of mass murder. Indeed, CloudFlare CEO Matthew

[12] https://blog.cloudflare.com/cloudflare-and-free-speech/

[13] https://blog.cloudflare.com/cloudflare-and-free-speech/

[14] https://blog.cloudflare.com/cloudflare-and-free-speech/

[15] Liptak, Adam. "Court Affirms Ban on Aiding Groups Tied to Terror." New York Times. June 21, 2010.

Prince has been adamant in his declarations that "CloudFlare abides by all applicable laws in the countries in which we operate and we firmly support the due process of law."[16] Prince continues to insist, "We have never received a request to terminate the site in question from any law enforcement authority, let alone a valid order from a court."[17]

In deference to CloudFlare, it is possible that the company has received a formal request from law enforcement to continue providing its services to such an illicit online forum. Yet, even as one who has repeatedly advocated leaving jihadi forums online in order to study those who use them, this possibility gives me pause for reflection. If so, there must be a careful assessment of the potential negative policy impacts of leaving ISIS recruitment platforms online and unmolested in light of the recognition that Western security services are abjectly failing to track, identify, and stop all of those who are using these sites.

The multi-billion dollar U.S. companies who provide social media services to ISIS and Al-Qaida are well aware that the way American law is presently structured, it is almost impossible for them to ever be held legally liable or responsible for the potential mayhem that their paying users might cause. The only real incentive they have to address this problem is when it becomes so glaring and embarrassing, as it was in the case of slain American journalist James Foley, that they are temporarily forced to take action to save public face. Without concerted pressure both from the American people as well as the Congress—in addition to meaningful legal reform aimed at closing loopholes that allow service providers to turn a blind eye to the identities of their users—this problem is almost certain to grow steadily worse in the months and years to come. Permitting U.S. commercial interests to simply ignore vital national security concerns and earn profits from consciously providing high-tech services to banned terrorist organizations is not an acceptable legal framework in the 21st century.

[16] https://blog.cloudflare.com/cloudflare-and-free-speech/

[17] https://blog.cloudflare.com/cloudflare-and-free-speech/