10

Virtually Illicit: The Use of Social Media in a Hyper-Connected World

Tuesday Reitano and Andrew Trabulsi

With her customized pink AK-47 cocked on her shiny latex-covered hip, Claudia Ochoa Felix, the woman reported to be the new matriarch of "Los Antrax," the killing squad of Mexico's Sinaloa drug trafficking cartel, personifies the spirit of narco-narcissism. Ochoa Felix' moniker as the "Kim Kardashian of the crime world" refers not only to her scarlet pucker, contoured cheeks, and pert glutes, but also to her obsessive use of social media to flaunt the wealth and status that accompany her fearsome reputation. The 20-something mother-of-three's Instagram and Twitter accounts are replete with images of luxury cars, designer clothes, beautiful people, and fabulous parties. One now infamous image shows her toddler lying on a bed blanketed in dollar bills. Despite her success, she is far from alone in successfully cultivating such an image on social media. From the street gangs in the United States to the mafia in Palermo, social media is becoming increasingly ostentatious and ubiquitous. Where organized crime was once something that previously lived furtively in the shadows, with secrecy being a premium commodity, in today's hyper-connected world, social media has become the showcase of organized criminal groups to demonstrate their power and profits with impunity.

By virtue of its prodigious use of social media, the Islamic State of Iraq and the Levant (ISIL) has managed to develop a large number of globally dispersed supporters, which has enabled ISIL to exert an outsized impact on how it is perceived by the world. Violent achievements such as the beheadings of Western journalists and aid workers are trumpeted on Twitter, YouTube, and Instagram, raising the group's profile, mobilizing funds, and recruiting new fighters.[1] As of January 2015, ISIL had recruited an estimated 4,500 foreign terrorist fighters from Western countries, many of whom have been lured by an aggressive social media outreach strategy that preys on the isolated, marginalized, or vulnerable.[2] Regardless of the means of recruitment, their physical journey to join ISIL will be coordinated by countless interactions with facilitators; corruption brokers offering fraudulent documents or safe passage through an accommodating border post; and faithful allies offering safe houses, secure transport, and fraudulent documents, all via a series of messages on ever-changing Twitter accounts, messaging apps, and encrypted platforms.

Society, identity, and connectivity are increasingly being defined in the social media space, rather than by the physical borders of geographic states. Facebook, for example, has

1.3 billion active users across the globe; only 2 of the world's countries can boast a larger population. This has created an open forum for the connection of individuals and exchange of ideas, goods, and services through which criminal organizations can ideologically thrive. It has become one of the primary means by which groups identify the like-minded, engage with them, and garner their support. This process is harmless when applied to gardening groups or fan pages dedicated to icons of pop culture, but infinitely more damaging when used to further criminal or terrorist agendas. The potency of social media comes in its unique ability to broadcast en masse, whilst at the same time delivering messages that seem intimate, allowing individuals to respond. As this chapter will explore, a myriad of deviant groups is using social media to shape opinion and elicit respect, fear, and terror. They are exploiting the functionalities of social media along all parts of their enterprise chain, from identification of allies and victims, to executing operational capacities such as logistics and fundraising. In doing so, social media is blurring definitional categorization between criminal groups, terrorists, political activists, and insurgents; perhaps more importantly, it is increasingly conferring legitimacy on their acts by drawing average citizens into this spectrum.

The challenges of responding to this growing convergence are significant, and the majority of efforts deployed by states at counter-messaging and/or identifying and disabling key nodes in social media networks have proven largely fruitless, sometimes laughable, and often counterproductive. These efforts inflame, rather than subdue, the calls to arms that such social media campaigns represent. Traditional law enforcement tools have struggled to gain traction in this landscape: intelligence gathering techniques are challenged to embed themselves effectively to understand transnationally spread groups and operations, with highly contextualized roots but a compelling shared ideology; anti-money laundering (AML) and countering the financing of terrorism (CFT) protocols remain focused on formal economy transactions and lack the data or instruments to engage in cash economies and through informal value transfer systems. Much is spoken of the capacity of big data to offer solutions, but efforts are still highly experimental and require technical knowledge, systems, and advanced contextual analyses that are often missing from state capacity. Efforts to offset the threat by mobilizing the power of social media for the public good have equally fallen short of the mark, with campaigns "going viral" and creating a short-lived public pressure that might result in rapid and flamboyant mobilization but rarely sustained commitment. Instead, the private sector and motivated vigilantes are most often seen standing at the frontier of combating social media security threats and their manifestations, while the primary onus on preventing radicalization and criminalization lies in the hands of the individual. Social media's potency comes from its authenticity of voice, and its ability to create a community of shared vision and understanding. This is best done organically, and in that case, arguably the correct role for the international community is to serve as incubator and defender of those brave voices that continue to champion freedom from fear and insecurity.

Individuals, Identity, and Ideology

In his 2006 book *Terror on the Internet*, Gabriel Weimann outlined the major uses of the internet by extremist groups: communication among members, transfer of information such as instructions on bomb-making or training videos, research of potential targets, and cyberterrorism.[3] Since then, however, with new technology and greater experience, the uses of the internet and social media by groups with a violent extremist or terrorist agenda have become manifold and prolific. Terrorist groups now use the internet, social media, and messaging applications for recruitment, fundraising, spreading ideology, influencing public opinion, and calling a diverse audience to arms in support of their cause. This is a nuanced agenda that plays on individuals' fears, isolation, and desire for empowerment, and as a consequence is arguably more potent and potentially damaging than was previously understood.

An area of social media usage that has risen to particular prominence with the ascendency of ISIL is the capacity of social media to be used as a tool for recruiting foreign fighters. Foreign fighters add not only considerable cachet to a jihadist agenda, but they may also bring to the table sets of skills and local knowledge that increase the capacity to manipulate Westphalian narratives and inspire terror. For many, however, the concern is less the possibility for recruitment of foreign fighters, which will always only reach out to a very tiny margin of the population. Instead, it is the narrative power that ISIL and other terrorist groups gain by using social media as a broadcasting tool. Like all propaganda, public perception can be partially engineered with these tools, and ISIL does this remarkably well. Highlighting their violence and their successes, even if the narrative is overplayed, influences the thoughts of the general public, which in turn becomes an obstacle that must be addressed by both policymakers and the intelligence community.

The messaging used by terrorist groups on social media involves appealing to three motives: humanitarian or moral imperative, ideology, and identity.[4] In the first instance, they speak to abuses by the opposing force and express moral outrage in order bestow legitimacy on their struggles and to portray themselves as fighting injustice. Foreign fighters in Syria regularly post pictures of young children allegedly killed by the Assad regime, and Jabhat al-Nusra has posted videos of their fighters rescuing civilians. Throughout the war in Afghanistan, the Taliban regularly used Twitter to document war atrocities committed by the International Security Assistance Force (ISAF) troops and spoke aggrievedly of the "occupiers" and their illegitimate wars.[5]

Terrorist groups also broadcast their ideology through social media as a call to arms, to raise local morale and attract supporters further afield. Somalia's al-Shabaab has long had quite active campaigns on Twitter and Facebook, and spends considerable energy on propagating its radical ideology through slick propaganda, targeted media campaigns, and clever use of media networks—and their use of social media has evolved over time. In 2011 and 2012, al-Shabaab created its first Twitter accounts, and used it to provoke the Kenya Defence Force (KDF), and later the African Union Mission in Somalia (AMISOM), into long "Twitter duels," where they traded insults and military successes with a

surprising degree of engagement and wit. One entertaining interchange followed a post by the KDF spokesman, Major Emmanuel Chirchir (@MajorEChirchir), threatening to bomb concentrations of donkeys that might be moving weapons for the insurgents. Al-Shabaab (@HSMPress) responded, "Your eccentric battle strategy has got animal rights groups quite concerned, Major."[6] More recently, either inspired by (or in competition with) ISIL, the group appears to be putting more effort into using social media platforms to attract international attention and call followers to action. On February 22, 2015, al-Shabaab released a video on YouTube in which they called for an attack on London's Oxford Street, as well as Westfield and White City Malls. The video compared such attacks to the attack by al-Shabaab on Westgate Mall in Kenya in 2013. Other malls, like the Mall of Americas in the United States, were also mentioned. These locations are home to the largest Somali diaspora communities, which is apparently the target audience of the appeal, rather than foreign fighters, which were the ambition of ISIL strategies. In the video, an al-Shabaab member, speaking with a strong English accent, called upon jihadists living in the West to "answer the call of Allah and target disbelievers wherever they are."[7]

Finally, and perhaps their most potent weapon is that of identity, appealing to aspirations and vulnerabilities of their target group, to their sense of sense of self, pride, and family.[8] Conveyed across multiple social media channels, Twitter, YouTube, Facebook, Instagram, the messaging of ISIL manages to swell youths with a (false) sense of empowerment. "Access to weaponry and the ability to intimidate represent an antidote to the feelings of marginalization, alienation and powerlessness that young men felt in their former environment, whether a slum in a European or Middle Eastern city, or in a village as a peasant trying to help his family make ends meet."[9] They offer a sense of purpose, suggest that "war is cool," that they will find friendship and acceptance, both amongst brothers and with women. Much of the propaganda aimed at young men parallels popular culture: they use GoPro cameras to share the excitement of conflict, with set-up skirmishes that are self-labelled as being like popular video games.[10] ISIL has been the most successful group when it comes to recruiting women to their cause. Here, they target the socially isolated, appealing to their empathy, a sense of grievance, and message around acceptance, belonging, and the possibility of finding a mate.[11] Jihadist propaganda aimed at women tends to be counter-feminist, emphasizing that women are valued not as sexual objects, but as mothers to the next generation and guardians of the ISIL ideology, and they are encouraged to anticipate and think fondly of the husbands that they will have. Interestingly, it also frequently emphasizes the potential transience of such a union, as fighters give their lives for jihad.[12] Far from being exclusively "jihadi brides," female migrants into ISIL play crucial roles in the development of the group's internal social structure, from taking care of men who have returned from battle to vaccinating children. There is no singular profile for Western women in ISIL. Thus, the use of social media for female recruitment operations is varied. While some women romanticize their lives in the Caliphate on social media, others express hardship and sacrifice in making their lives inside it.

Around these primary sending accounts, groups create a bevy of followers that amplify, glorify, and reinforce the central message and its senders.[13] A 2014 census of

ISIL-supporting Twitter accounts, for example, found that the core of the activity emanated from a relatively small group of hyperactive users, numbering between 500 and 2,000 accounts that tweeted at concentrated bursts of high volume. However, around that central traffic were 46,000 to 70,000 accounts which would play a secondary supporting role, creating the vibrant and self-reinforcing perception of an active and inclusive community, and sending as many as 100,000 tweets per day.[14] New members of the dialogue are quickly identified and encouraged, with efforts made to then shift conversations from the public forums to private mediums, using internet-based messaging apps such as Skype, Facebook Messenger, Surespot, Telegram, Kik, or WhatsApp, where the relationship can be cultivated on an individualized basis, using textbook methods of attitude modification and indoctrination used in many faith-based groups, with creating a shared identity being central.[15]

The emphasis on identity used by terrorist groups on social media is also used by organized crime groups. Two main strategies long used by organized crime groups to ensure the loyalty of their subordinates are: first, through violence or the threat of violence; and second, by creating and emphasizing a sense of identity and belonging, and communicating this widely.[16] This is often because organized crime groups have grown out of a population that is marginalized, disenfranchised, or actively persecuted, and have created violent wings for self-protection. As the external threat has diminished, those providing protection have slowly morphed into a source of insecurity, demanding fees for their "protection," also known as extortion.[17] Identity becomes an important factor, as it creates a unity of purpose and reduces the likelihood of betrayal and competition. There are many markers used to affirm these identity—initiation rites, for example, or a strong emphasis on family. The use of tattoos is almost synonymous with criminality, used from the Asian groups like the Triads or the yakuza, to the Russian mafia prison groups and the street gangs of the Americas. This indelible brand of belonging simultaneously serves to unify cultures and represent distance from the established regime.[18] Similarly, symbolism, graffiti, code words, and signature moves have been used to create criminal subcultures, claim ownership of territory or violent acts, and to intimidate rivals.

The communication of power and the capacity to commit violence has always been an important part of the strategy of criminal groups, and social media has significantly amplified that. In the hyper-connected world, groups are taking these two distinguishing strategies online.[19] Social media has become the new means by which to display potency and initiate conflict. Graffiti "tags" have evolved into hashtags, and the same signs of prowess and success play out on social media sites, with the same intent as the symbols of the previous generation. In the typology of groups active along a spectrum of criminality, the ability to communicate and project their potency differs. The United Nations Office on Drugs and Crime (UNODC) has developed a working typology of five types of criminal groups, ranging from highly organized, hierarchical mafia-type groups which dominate some markets to more loosely organized networks or gangs which are active in others, and their communication requirements are different.[20] Arguably, groups with a wide

membership, who are very secure in their support, are the most likely to broadcast widely the symbols of their influence, whereas highly localized crime groups are least likely. For example, for the highly geographically dispersed Mara Salvatrucha (MS-13) group, social media (and violence) has been instrumental in maintaining allegiance across multiple countries and territories. Unlike many of the traditional hierarchical mafia groups, the MS-13 operates with a hierarchy, "but it is a 'hierarchy of influence' where 'respect' and loyalties are expressed through a networked structure," and the evidence of influence, respect, and authority are displayed online. Social media mapping work undertaken by the SecDev Foundation has demonstrated that social media has facilitated this networked structure to engage in transnational crime, with certain cities (and prisons) serving as communication hubs across multiple regions.[21] Robert Muggah, director of Brazil's Igarapé Institute and the leader of SecDev's analysis, observed, "They use it to tag (mark territory), they use it to coerce, they use it to recruit, they use it to move product, they use it to communicate directives."[22]

Groups posture and self-promote online. The Sinaloa cartel, arguably the most powerful crime group in Mexico, has a Twitter account (@carteidsinaloa) with more than 57,000 followers. The alleged account of their leader, El Chapo Guzman, has more than half a million followers (@elchap0guzman), and his bravado has extended to insults and threats to Mexican President Peña Nieto and U.S. presidential candidate Donald Trump.[23] In the highly violent drug wars of the Americas, in a practice known as "cyber-banging," groups trade threats and insults over Facebook and Twitter, tagging rivals as the next in line for hits. This may cause spikes in homicides in concentrated and unpredictable bursts that confound the standard intelligence and analytical tools of law enforcement that do not systematically monitor social media nor have the ability to predict which insults or threats might prompt the next bout of violence.[24]

Using data analytics software, we can find this behavior evident in ISIL's use of social media as well.[25] Data visualization software from San Francisco-based analytics firm Quid illustrates that over half of all tweets from ISIL's top Twitter handles focus on conflict reporting and promoting new Twitter accounts. Quid's software uses natural language processing and mathematical physics to identify and visualize patterns within structured and unstructured datasets. Further, Quid's analysis demonstrates that new Twitter account promotion and security precautions drive major spikes in conversation amongst ISIL's digital communities, fostering both support and enhancing operations. In Figure 10.1 below, each node represents one tweet, and the proximity of nodes designates the degree of semantic similarity each tweet has with others in the network.

Figure 10.1. Network of Tweets in English-Speaking ISIL Network from August 6 to 26, 2015 (conflict reporting outlined in black and account promotion in blue; n = 878 tweets)

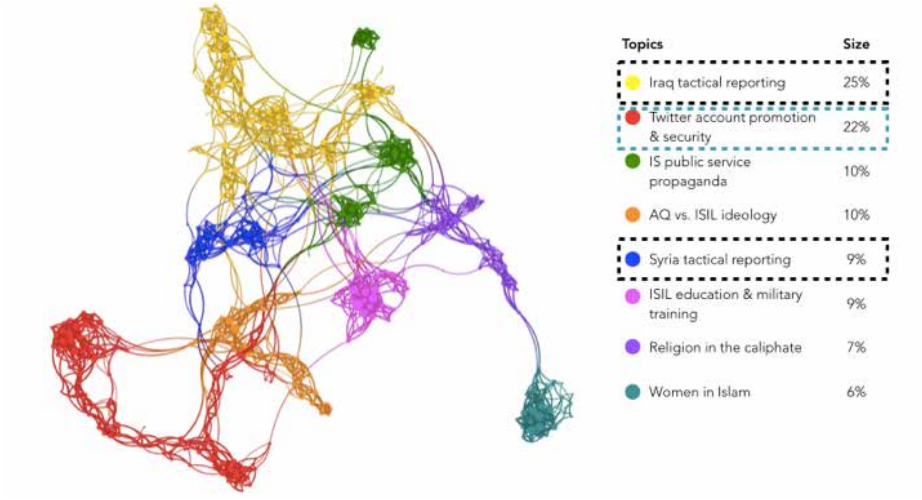
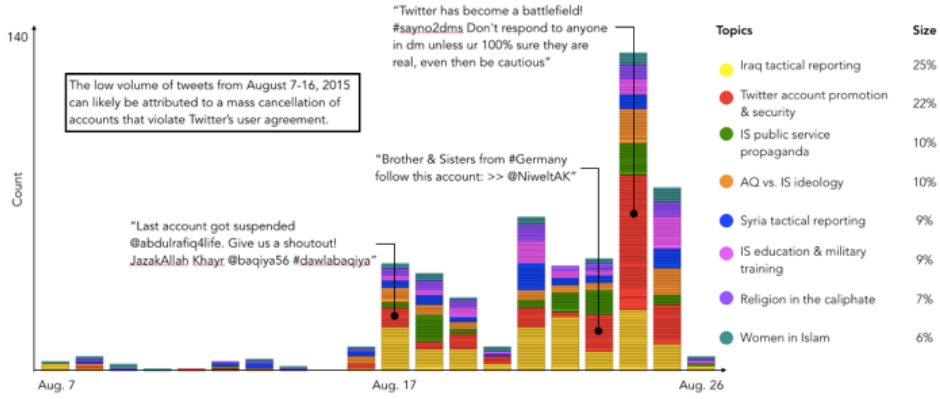


Figure 10.2. Timeline of Tweets in English-Speaking ISIL Network from August 6 to 26, 2015 (n = 878 tweets)



Social Media as a Service Provider for Underground Operations

Not only is social media helping deviant groups win hearts and minds and intimidate their opposition, it is also proving a more practical, tangible instrument in executing operations. Criminal groups and terrorists are exploiting the functionalities of social media along all parts of their enterprise chains, from the identification of allies and victims, to the execution of operational capacities such as logistics and fundraising, the procurement of services, and the development of their technical capacity. In the Americas, there has been a rise in kidnappings of software engineers and programmers as organized crime groups seek to reinforce their digital capabilities to ensure their technological dominance.[26]

One of the primary ways in which social media aids criminal and terrorist organizations is in identification and recruitment of victims, clients, service providers, and allies. Social networking sites contain reams of personal information about their users, which criminal groups use as intelligence gathering for possible targets. When soliciting new recruits, deviant groups can gather information about the friends, family, and habits of their victims. This helps them to customize their grooming strategy and to apply pressure on new recruits to conform. Individuals trying to exit from criminal or terrorist groups find themselves intimidated by threats, blackmailed and extorted until they find themselves forced to continue engaging with the groups. In one case of a teen courier working the Mexican-U.S. border, documented by *CNN*, he found himself locked into the cartel:

> "I told him that I didn't want to work for Los Zetas anymore and that I would rather be killed than to continue to work under him," Cesar said he declared after one night of constant text orders. The new boss called at 5 a.m. and told Cesar he was coming to pick him up to kill him. They met outside Cesar's house. The man pointed a gun at Cesar's face. Then, he started laughing. He told Cesar he wasn't going to kill him. But that he would keep working or his family would be killed. He had been working with the cartel for too long. He would have to work again that morning.[27]

In a similar vein, one of the most standard practices and lucrative earners for criminal and terrorist groups alike comes in the form of fraud, blackmail, and extortion. In these crimes, which range from 419 cyber-scams to "virtual kidnapping," social media again allows the capacity to profile victims, and can provide kidnappers with the exact location of a victim through photos, live feeds, and apps with geolocation features, which can be embedded in posts and pictures without owners even realizing it.[28]

In addition to supporting the planning and execution of international terrorism, secure social messaging apps like Kik, Wickr, and Surespot, which encrypt or destroy communications data, play a critical role in ISIL's bride-recruiting and kidnapping operations. According to the U.S. Homeland Security Committee, an estimated 550 Western women have traveled to the conflict zone to marry ISIL fighters, as of October 2015. Conversations that begin on social networking platforms like Twitter or ASKfm migrate to secure channels, where men and women affiliated with ISIL lure potential brides to Syria, to marry jihadists living within ISIL-controlled territories. A 2015 report from the Institute for Strategic Dialogue (ISD) and the International Centre for the Study of Radicalization (ICSR) found that within three months of arrival, women who join ISIL are expected to marry a fighter and start producing children. Under strict shariah law, women are prohibited from combat and combative activities, but those who are social media savvy may themselves become part of the recruitment effort.[29]

The same tools are being used to facilitate kidnappings and allow troops to communicate on the battlefield. The September 2015 issue of *Dabiq*, the ISIL magazine, lists the sale of newly captured hostages as advertisements. Each solicitation includes each man's purported occupation, date of birth, and home address, as well as a Telegram

number—a mobile social networking app that encrypts communication—for "whoever would like to pay the ransom for his release and transfer." Similar encryption-based messaging apps allow fighters to communicate both inside and outside of ISIL, even while on the battlefield. Use of such applications generates additional layers of exclusivity and security for ISIL members and their evangelists. These secure spaces allow fighters on the frontlines to connect with others through social media to promote messages, warn of impending security risks, and facilitate transactions that keep operations humming within the operations of ISIL itself. Such technological advances are wholly new and represent a transformation in the ways that global jihadist movements, and more broadly criminal enterprises, can conduct business and expand their presence.

Social media also serves as a marketplace for the exchange of illicit goods and deviant services. Websites where document forgers, hackers, heavies, and hit men all proffer their services have been discovered. While these have migrated mainly to the Dark Web, onto sites such as the Silk Road or variations thereof—they also have been found on normal social media sites like Facebook.[30] On one social media site found in Mexico, while others boasted of their exploits, aspiring contract killers sought mentors and training: "I want to learn how to be a hit man," wrote one on Los Pulpos' wall, "Someone train me. I am capable of killing whoever [sic]."[31] Criminals operating online can be surprisingly service-oriented, offering help desks, customer service, and translations to support non-native speakers in their effort to communicate with potential victims.[32] In the migrant smuggling trade, smugglers advertise their illicit migration packages overtly to potential migrants, not only openly offering different classes of travel at varying prices, but also fraudulent documents and "relocation consultants" who will help illegal migrants successfully seek asylum and maximize their benefit packages.[33]

Social media is enabling a new category of professional "terrorist financiers" within terrorist groups, as they rely more heavily on social media to solicit donations and communicate with both donors and recipient radicals.[34] The U.S. National Terrorist Financing Risk Assessment identified nine terrorist financing cases that involved personal fundraising online or through social media, and in August 2014, the United States designated an al-Nusra Front financial facilitator who regularly solicited funds over social media.[35] Such social media accounts, known as *Ansar* accounts to ISIL—literally translating into "helpers," in reference to Arabian tribesmen who gave shelter and a home to the Prophet Muhammad and Islam "at the most critical point of the Prophet's mission,"—provide channels beyond media distribution and recruiting, to support operational coordination and broader development goals.[36] Social media serve as the primary interface for a number of terrorist financing transactions that take place in the informal economy, through *hawala* dealers, contributions to front nongovernmental organizations (NGOs), or even fake crowdfunding activities.[37] This presents an extraordinary challenge to law enforcement, as the majority of informal financial transfer systems have their foundations in trust-based relationships, rather than actual physical or electronic transactions. The majority of *hawala* transactions, an estimated 80 percent, occur only through local cash transactions, with a

periodic "net settlement" of funds between *hawala* operators. Thus, the ability to ensure secure channels of communication are critical to ensuring that trust can be built and that the system functions effectively.[38]

Social media also facilitates information sharing of privileged material, both discretely as well as more broadly. An ISIL-affiliated British-born hacker and propagandist under the *nom de guerre* Hussain al-Britani, for example, was linked to fomenting lone-wolf terrorist attacks internationally, including a shooting at a Garland, Texas event featuring cartoon images of the Prophet Muhammad. Before his death via drone strike in August 2015, the 21-year-old disseminated a kill list of 1,351 American government and military personnel—obtained from a Kosovo national—via social media, threatening to "strike at your neck in your own lands."[39]

Tools that allow for encryption of communication make the job of intelligence officials all the more difficult. As the Federal Bureau of Investigation's top counterterrorism official, Michael B. Steinbach said in response to new uses of social media technologies by global criminal organizations, "We're past going dark in certain instances. We are dark."[40] In addition, *Ansar* accounts continuously monitor supporting social media communities for both terrorist groups and drug cartels. For example, in response to hacks allegedly stemming from Western intelligence communities, an ISIL sympathizer (@Moha5er) recently tweeted, "Warning significant Ansar accounts compromised today. Beware of opening any link without verifying the integrity of the author." Use of such methods seeks to delegitimize efforts taken by Western governments to stem the growth of such criminal organization online.

Evaluating and Strengthening Responses to Social Media Capture

Recognizing and acknowledging the extent to which illicit markets and deviant groups are enabled by social media is the first obstacle, and a considerable one. Finding effective and appropriate responses is proving an even greater challenge. The threat presented by terrorist and criminal activities on social media is clearly vast. Awareness and initiatives are growing in number, but are still highly fragmented and experimental. Along with task forces developed by states and social media companies themselves, online vigilantes—from collectives tied to the online activist group "Anonymous" to individual white hat hackers—are taking on criminal organizations, reporting their activity and working to mitigate their outreach.

If use of social media is propaganda in the modern day, and an instrumental tool in the hybrid warfare of the 21st-century battlefield, the insurgents are far outstripping states in their efficacy of use. The U.S. Department of State's counter-narrative effort is a campaign known as "Think Again, Turn Away" (@ThinkAgain_DOS), which has a mere 23,000 followers and lacks engagement, personalization, or creativity. In Europe, the Western region hardest hit by the foreign terrorist fighter phenomenon, the number of social media counter-messaging and outreach efforts have proliferated exponentially, but have had minimal impact. For example, a British group has started a video campaign

known as #NotAnotherBrother, which targets young Muslim men in the UK who are considering going to fight for ISIL, highlighting the damage to families, but the video has been heavily criticized for its failure to resonate with the priorities of its target demographic.[41] States' institutions and mechanisms are, arguably, poorly suited to achieve the level of individualized attention required to successfully counter-message either within the framework of violent radicalization or gang identity. States necessarily work from the viewpoint of the protection needs of their citizens and gain their legitimacy precisely from the mass majority from which those attracted to deviant groups feel a sense of alienation or grievance. Their clumsy efforts to counter-message read more like propaganda than compelling rhetoric, and efforts to engage in dialogue with opposing groups have come across as defensive, often reinforcing terrorist arguments rather than breaking them down.[42] As a recent leak of a confidential U.S. State Department assessment of ISIL strategy soberly concluded, "When it comes to the external message, our narrative is being trumped by ISIL's. We are reactive—we think about 'counter-narratives' not 'our narrative.'"[43]

Experts have suggested that states' efforts would be better directed at development interventions targeting root causes, or classic law enforcement investigations to disrupt operations, rather than trying to battle extremist groups and criminal enterprises in the battle for hearts and minds. Fundamentally, states will rarely have the kind of manpower to engage in the long-term cultivation of relationships on an individual basis that ISIL recruiters have shown, for example, nor would it be their priority to do so. It is only in the case of high-value targets that such investment of resources would be justifiable, but in those cases the result is more likely to be sting operations or indictments, rather than ideological challenges, though these strategies are not without their concerns.[44] As criminals and terrorists increasingly take to social media, law enforcement agencies have developed new investigative strategies, and had some notable successes. One self-promoting, web-addicted drug lord, Rodrigo Arechiga Gamboa (known as El Chino and rumored to be the lover of Claudia Ochoa Felix) was arrested by U.S. authorities in December 2013, as he arrived at Schiphol Airport in Amsterdam. Authorities identified him not by his face, which was always obscured, but by the skull-shaped diamond ring, which he used as his signature in the pictures on his multiple social media accounts of his sports cars, yachts, weapons, jewelry, money, and extravagant parties.[45] Eighty percent of U.S. law enforcement professionals profess to actively use social media in investigations, but this remains an organic and informal process; 75 percent of those officials were self-taught, as less than half of these agencies have a formal procedure for the use of social media in criminal investigations. They have employed social media for everything from collecting evidence, seeking witnesses, identifying criminals and crime scenes, and mapping criminal networks. "My biggest use for social media has been to locate and identify criminals. I have started to utilize it to piece together local drug networks," said a police officer quoted in a LexisNexis survey.[46]

Tracking and monitoring social media interactions through social network analysis (SNA) tools allows the visual documentation of the relationships between actors, highlighting

strong connections that could span a global domain. While use of SNA-style investigations are embryonic in the United States, they are even scarcer elsewhere, especially in countries where escalating crime and violence are pressing social problems. Fundamentally, moving towards SNA-style analysis is a big shift for law enforcement, which has traditionally focused on specific crime types (e.g., drug trafficking, human trafficking, arms dealing) or even individual incidents, each in its own silo. This is a nonsensical restriction when organized crime groups are increasingly poly-crime syndicates working in a versatile manner across criminal markets. Furthermore, national law enforcement agencies are predominantly constrained within their national boundaries, with knowledge concentrated within their local environment. For example, even while awareness has grown about the links between West African and Latin American groups trafficking cocaine to Europe, cooperation is minimal and there is still precious little information or common knowledge of their connections and interactions.[47] Instead, when SNA enabled by technology is included within the analysis, it can help to identify pivotal "nodes" in the criminal economy, or actors that function as a bridge between the criminal and the legitimate economy (e.g., lawyers, bankers, businessmen, corrupt state officials) and which are often points of vulnerability to be seized by law enforcement investigations.[48]

The need to update tools to counter the financing of terrorism through social media and informal economies is becoming increasingly urgent. The Financial Action Task Force (FATF)—the principle custodian of AML, CFT policy, and best practices—remains unable to offer better solutions, but flags the issue as being of primary concern. Reducing access to funding will have a potent impact on the ability of both criminal and terrorist groups to conduct their activities and meet their objectives, and warrants considerable extra analysis and attention.[49] Continuing to invest in and rely upon traditional AML approaches may give the impression of action in the traditional sense of technical cooperation (i.e., passing legislation, building capacity, etc.), but is largely ineffectual. Symbolic prosecutions and asset seizure in the case of criminal groups in particular, given that the ability to communicate power and influence is so central to their identities and efficacy, can prove a powerful counter-message and undermine their authority.

In environments of chronic insecurity, whether due to terrorist conflict or criminally motivated gang violence, a further impact has been to compromise the capacity of state institutions and the media to play their role as a bulwark against insecurity and the erosion of civil liberties. A combination of violence and corruption has had a highly detrimental effect on public protest and media freedom in a number of theaters, as crime groups and terrorists have targeted state officials, law enforcement, and journalists. In the war of words, ideas, and influence, the role of those that are the principle broadcasters have become particularly central. ISIL and al-Shabaab both target journalists as a way of sending a message to the broader population; as a consequence, Somalia is consistently ranked in the top three most dangerous places in the world for journalists.[50] A Reporters Without Borders inquiry report in 2013 found that organized crime has become a "fearsome predator for journalists in many parts of the world," identifying Honduras, Guatemala, Brazil, and

Paraguay in Latin America, as well as Afghanistan, Pakistan, China, Kyrgyzstan, and the Balkans, as countries where the beat is most dangerous. They found that 141 media workers and journalists had been killed during the decade of the 2000s, in attacks and reprisals blamed on criminal groups.[51] Increasingly, these killings are preceded by threats, frequently delivered through social media. The Committee to Protect Journalists estimated that almost a third of the murdered journalists were either taken captive or tortured before their deaths, with the intention to send "a chilling message to the entire news media."[52] The result has been a self-censoring effect on news media across a number of parts of the world, and a devastating impact on one of the primary means by which to fight organized crime.[53]

Similarly, states are making efforts to silence the voices of those promoting criminal acts or terrorist agendas. As states have struggled with issues of capacity and resources, much of the emphasis has also been placed on the potential role and responsibility of the private sector to engage in the fight against deviant networks and behavior. States have put pressure on internet firms and social media sites to be more vigilant in monitoring content, filtering, and closing accounts that are deemed to be a security risk, and in some cases have heavily criticized platforms for failing to proactively alert law enforcement to potential risks. For example, the UK's Intelligence and Security Committee (ISC) investigation into the murder of a British soldier, Lee Rigby, by two Islamic extremists concluded that the only "decisive" possibility for preventing the attack involved cooperation and proactive engagement by Facebook. The social media platform had committed to communicate the graphic intent to murder a soldier, but the company failed to either identify or pass on the threat.[54] The UK's subsequent introduction of the Counter Terrorism and Security Act in 2015, grants intelligence agencies the power to conduct mass surveillance and store data from emails and other internet data from social networking sites and messaging services.[55] Similarly, the U.S. Senate Intelligence Committee approved a bill in June 2015, which would require social media companies to alert federal authorities when they become aware of terrorist-related content on their sites. Repressive states that make moves to limit the access of their citizens to social platforms come under heavy censure from the international community (consider, for example, the recent efforts by the Turkish government to ban Twitter and YouTube), but according to watchdog Freedom House, in one year alone between May 2013 and May 2014, 41 countries (20 percent of the world's states) passed or proposed legislation to penalize legitimate forms of speech online, increase government powers to control content, or expand government surveillance capabilities, including many Westphalian states that pride themselves on their democratic tradition and freedom of speech, as the fight against crime and terrorism increasingly come into conflict with the right to privacy.[56]

Consequently, the various platforms have struggled with their obligations in this war of ideas and identity. Most have developed policies forbidding the posting of violent, extremist, or offensive (hate crime) material on their platforms, but have found it difficult to control the rapid exchange of content and ideas, especially as accounts can be opened and closed in a manner of minutes. But at a more fundamental level, both the internet and

social media were precisely created—and have since thrived—to allow the free exchange of ideas and information. The social media companies, while broadly supportive of efforts to prevent terror and compliant with national laws for disclosure, have, at the same time, been reticent to infringe on their users' rights to privacy, to impact on the platforms' ability to promote free speech, or to deny historical fact, regardless of its propaganda value.[57] Subsequently, they have shown even greater resistance to overtures from states to be drawn into direct efforts to create explicit counter-messaging strategies and content.[58] In their own words, "The internet is fundamentally a connective technology, and as it continues to grow, it has enabled illicit actors to better connect and coordinate complex actions, better manipulate and launder money, and better map and understand data in realtime [sic]. It behooves us in the technology community to ensure that innovative tools are also being used to disrupt illicit networks, and that on balance technology is a force for good. This is a mission we welcome."[59] And thus, their engagement has predominantly been restricted to providing some basic capacity building for public officials on how to make messaging impactful, funding civil society efforts to enhance security through social media, and offering space for discussion and debate. For example, the first Google Ideas conference in 2011 took the theme of "Terrorist Networks," the second in 2012 was titled "Illicit Networks," and the follow-up was to create a secure platform for "formers"—former terrorist combatants—to contribute to efforts to counter violent extremism.[60]

With the state rendered ineffective, traditional media silenced, and the private sector reluctant to actively engage, countering the negative influences of social media has, thus, increasingly fallen into the domain of civil society and nonstate actors. There are a number of ways that social media in the hands of civil society can and have been used to enhance civilian security and counter the pernicious influence of deviant groups. These have ranged from addressing local conflicts and creating community-based solutions, to internationally focused advocacy and awareness raising.

On a number of occasions, social media have been instrumental in campaigns to galvanize the international community to engage in ongoing crisis or conflict resolution efforts, calling attention to violence or injustice. The risk in these large-scale campaigns is that while they can be incredibly powerful in capturing attention and mobilizing public opinion in the short term, they have a tendency to very quickly fall out of vogue. As opposed to genuine activism, this has resulted in a phenomenon known as "clicktivism" that uses the power of social media to exert pressure on political actors. However, because of its nature, it tends to result in a specific style of politically expedient response, one that is typically high in visibility but lacking in long-term commitment and sustainable momentum required to have a genuine impact on the challenge. There are numerous examples. The high-profile #BringBackOurGirls campaign, which was launched in response to the kidnapping of more than 275 schoolgirls by the Nigerian terrorist group Boko Haram in April 2014, resulted in widespread and high-profile outrage, but little in terms of results—the majority of those girls are still missing over 2 years later, and Amnesty International estimates that Boko Haram has subsequently abducted more than 2,000 women with little

fanfare from the international community.[61] What the campaign did mobilize, however, was the necessary justification for the Nigerian government to mount a highly militarized and violent campaign against Boko Haram, consisting of a security crackdown that certainly exacerbated tensions between the group and the state and made a negotiated solution more remote.

A similar example of clicktivism at work can be found in the sudden global awakening to the crisis of Syrian migration, responding to images of #AlyanKurdi, a three-year-old child drowned on the shores of Turkey while trying to get to Europe. That single image brought home the severe consequences of a crisis that has been building for years, and triggered a response that the thousands who died in boats in the Mediterranean, or in the brutal Sahara, had failed to mobilize. But what was that response? Celebrity singles and touching artwork, campaign funding to NGOs to support humanitarian work, and migrant protection; all of these are useful, but ultimately insufficient, including a promise by European leaders to "get tough on smugglers" which materialized as warships in the Mediterranean and a meaningless Security Council Resolution, a response that two UN Special Envoys said in an open letter, "misses the mark."[62] As with the Boko Haram case, a clicktivist response comes with the flamboyant use of the military, without offering legal channels for migration or addressing the long-term root causes of displacement and mobility. The damaging consequence of such a response is that not only does it not respond to the genuine drivers of the crisis, but it is far more likely to result in pushing migrants more deeply underground and further from protection, entrenching the role of smuggling rings and increasing the risks of human rights violations. Furthermore, in less than a month, searches for the word "refugee" or "migrant" have already declined by half, as the refugee crisis fades again from public consciousness in favor of a new *cause célèbre.* The seeds for longer-term social, economic, and justice challenges have not been sown.[63]

There is little doubt that social media activism has a tendency to create lazy, feel-good solutions and short-term outpourings of aid, as opposed to genuine, long-term advocacy for reform. Where it can have value, however, is when it is properly curated within a national audience, aligned to a genuine political movement, and targeted to apply systematic pressure on political systems to change, or to create a grassroots campaign to enhance information, transparency, and democratic reform. In this way, social media can be used to make states more sensitive to audience costs (that is, the benefits and drawbacks that it could accrue from lying or telling the truth) as it allows citizens to engage with their governments and with others in civil society in ways that were not possible in the past. Much has been attributed to the role of social media in initiating the Arab Spring, for example, though its subsequent sustainability has clearly been brought into question. This has also been used to good effect in the case of the #Iguala, where student protestors in the Mexican city of Iguala were handed to organized crime groups by local governors to have them "disappear." Sustained momentum on the part of social activists has seriously damaged the credibility of the Peña Nieto administration and ensured that the impressive economic performance has failed to offset his government's inadequacy in addressing

human rights abuses, criminal impunity, and rising violence. At a less transformative level, social media can also lead to a greater degree of clarity or veracity in reporting about events and provide alternatives to state-controlled media.

At the local level, digital activists are self-organizing in virtual communities and are using their networks to curate and disseminate information to protect themselves.[64] Social media platforms have helped to reduce civilian casualties by serving as early warning systems, helping citizens stay connected to rapid response humanitarian organizations or security providers, and by providing information to citizens during and in the aftermath of crimes. A Kenyan village chief claims to have drastically reduced crime rates in his community by sending out tweets instructing citizens what to do in the aftermath of insecurity.[65] In Mexico, Twitter has been used to create a real-time "security monitor" that allows average citizens to report crimes as they happen, allowing a mapping of flare-ups of violence or areas of particular insecurity, and research suggests that about 1.5 percent of all Mexicans have tweeted about the drug war, which amounts to almost 5 percent of the country's online population.[66] The costs of doing so, however, have become increasingly lethal. Mexican bloggers and online activists are finding themselves violently targeted in parallel ways to the fear tactics used to silence the country's traditional media reporters. In October 2014, the site administrator for one such security monitoring site, *Valor por Tamaulipas*, a community site which has more than 100,000 followers on Twitter and over half a million on Facebook, had her execution at the hands of local drug trafficking groups broadcast via her own Twitter feed. This middle-aged mother, a physician and concerned citizen, had used the site to build her community and urged its citizens to speak out against gang violence.[67]

Whether social media ultimately will prove itself to be a tool of greater pacification or belligerence remains to be seen; that it certainly serves a powerful lever capable of conveying advantages to whichever side in a conflict wields it most strategically is beyond question. Fundamentally, free societies have always relied upon their citizenry and their values to be their last line of defense, and as nascent lessons from state-led efforts have demonstrated, authenticity of voice is extremely important. Seeking better solutions to the criminalization of social media will require creating safe spaces for courageous voices to share information and communicate without fear and intimidation. Doing this well is a design challenge that poses further questions about free speech, rights of expression, and personal protection in the global digital ecosystem, but it is an urgent and necessary priority.[68] It will also require all of the online community recognizing the power and choices that it makes when engaging with social media. Clicktivism has demonstrated the ease of mobilization on social media, but it has also made us lazy and immune to consequences. Clicking on something—whether to watch, "like," or share—amplifies its message, whether that is one of social good or fear, and as citizens within a global social media community we need to learn to click responsibly. In the social media space, where identity, ideas, and ideology have the greatest currency, a multitude of voices and sustained commitment are required to have an impact.

Notes

[1]J.M. Berger and Jonathon Morgan, *The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter* (Washington, DC: Brookings Institution, 2015), available at <http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf>.

[2] Peter Bergen, Courtney Schuster, and David Sternman, "ISIS in the West," *New America Foundation,* November 16, 2015, available at <https://www.newamerica.org/new-america/isis-in-the-west-2/>; Rachel Briggs and Tanya Silverman, *Western Foreign Fighters Innovations in Responding to the Threat* (London: Institute for Strategic Dialogue, 2015), available at <http://www.strategicdialogue.org/ISDJ2784_Western_foreign_fighters_V7_WEB.pdf>; Rukmini Callimachi, "ISIS and the Lonely Young American," *The New York Times,* June 27, 2015, available at <http://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html?_r=0>.

[3] Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: U.S. Institute of Peace Press, 2006).

[4] Briggs and Silverman, *Western Foreign Fighters Innovations.*

[5] Rory Medcalf, "War Tweets: War propaganda has finally moved onto Twitter," *American Review,* available at <http://americanreviewmag.com/opinions/War-tweets>.

[6] Duncan Omanga and Pamela Chepngetich-Omanga, "Twitter and Africa's 'War on Terror': News Framing and Convergence in Kenya's Operation Linda Nchi," in *New Media Influence on Social and Political Change in Africa,* ed. Anthony Olorunnisola and Aziz Douia (Hershey, PA: IGI Global, 2013), 241-256; David Smith, "Al-Shabaab in war of words with Kenyan army on Twitter," *The Guardian*, December 13, 2011, available at <http://www.theguardian.com/world/2011/dec/13/al-shabaab-war-words-twitter>.

[7] Darren Boyle, "Somali terror group Al-Shabaab calls for 'Westgate-style' shopping centre attack on London's Oxford Street and Westfield malls in Stratford and White City in chilling new video fronted by 'English' Jihadi," *DailyMail*, February 23, 2015, available at <http://www.dailymail.co.uk/news/article-2964218/Somali-terror-group-Al-Shabaab-calls-Westgate-style-shopping-centre-attack-London-s-Oxford-Street-chilling-new-video.html>.

[8] Briggs and Silverman, *Western Foreign Fighters Innovations.*

[9] Eric Davis, "ISIS's Strategic Threat: Ideology, Recruitment, Political Economy," *The New Middle East,* August 17, 2014, available at <http://new-middle-east.blogspot.com/2014/08/isiss-strategic-threat-ideology.html>.

[10] Briggs and Silverman, *Western Foreign Fighters Innovations.*

[11] Erin Saltman and Melanie Smith, *Till Martyrdom Do Us Part: Gender and the ISIS Phenomenon* (London: Institute for Strategic Dialogue, 2015).

[12] Carolyn Hoyle, Alexandra Bradford, and Ross Frenett, *Becoming Mulan? Female Western Migrants to ISIS* (London: Institute for Strategic Dialogue, 2015), available at <http://www.strategicdialogue.org/ISDJ2969_Becoming_Mulan_01.15_WEB.PDF>. The phenomenon is beautifully described in the outstanding investigation in Callimachi, "ISIS and the Lonely Young American."

[13] Briggs and Silverman, *Western Foreign Fighters Innovations*.

[14] Berger and Morgan, *The ISIS Twitter Census Defining and describing the population of ISIS supporter*s.

[15] Hoyle, Bradford, and Frenett, *Becoming Mulan?*

[16] Gambetta, *Codes of the Underworld.*

[17] Reitano and Hunter, *Contests and Compacts*.

[18] Wahlstedt, *Tattoos and Criminality.*

[19] Gambetta, *Codes of the Underworld.*

[20] UNODC, *Results of a pilot survey of forty organized criminal groups in sixteen countries* (Vienna: United Nations, 2002).

[21] John P. Sullivan and Samuel Logan, "MS-13 Leadership: Networks of Influence," *The Counter Terrorist*, August 2010, available at <http://digital.ipcprintservices.com/display_article.php?id=428186>.

[22] Ciara Byrne, "Drugs, Guns and Selfies: Gangs on Social Media," *Fast Company*, February 15, 2015, available at <http://www.fastcompany.com/3041479/drugs-guns-and-selfies-gangs-on-social-media>.

[23] Hasani Gittens, "El Chapo's 'Official' Twitter Takes On Trump, Mexican President," *NBC News,* July 14, 2015, available at <http://www.nbcnews.com/news/latino/el-chapos-official-twitter-takes-trump-mexican-president-n391411>.

[24] Sandy Banks, "'Cyber banging' drives new generation of gang violence," *LA Times,* October 3, 2015, available at <http://www.latimes.com/local/crime/la-me-1003-banks-lapd-gang-shootings-20151003-column.html>.

[25] For more information on Quid, the data analytics software used in the chapter, please visit http://www.quid.com.

[26] Robert Muggah, "The rising threat of organised crime on social media," *World Economic Forum,* July 27, 2015, available at <http://www.weforum.org/agenda/2015/07/social-media-violence/>.

[27] Evelio Contreras, "Inside the life of a drug trafficking teen," *CNN*, August 15, 2015, available at <http://www.cnn.com/2015/08/12/us/inside-the-life-of-a-drug-trafficking-teen/>.

[28] News Team, "Use of Social Media in Kidnapping and Extortion," *KR Magazine*, October 2, 2015, available at <http://www.krmagazine.com/2015/10/02/analysis-olive-group-use-of-social-media-in-kidnapping-and-extortion/>.

[29] Saltman and Smith, *Till Martyrdom Do Us Part.*

[30] Raj Samani, "Cybercrime as a Service," *McAfee Research*, 2014, available at <http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf>.

[31] Miriam Wells, "Facebook Hitman Highlights Organized Crime's Online Presence," *InSight Crime,* June 21, 2013, available at <http://www.insightcrime.org/news-analysis/facebook-hitman-highlights-organized-crimes-online-presence>.

[32] Samani, "Cybercrime as a Service."

[33] Based on an extensive series of interviews by the Global Initiative with law enforcement in Europe and North Africa.

[34] Samuel Rubenfeld, "Social Media Emerges as Terrorism Fundraising Tool," *Wall Street Journal,* August 11, 2014, available at <http://blogs.wsj.com/riskandcompliance/2014/08/11/social-media-emerges-as-terrorism-fundraising-tool/>.

[35] Financial Action Task Force (FATF), *Emerging Terrorist Financing Risks* (Paris: FATF, 2008), available at <http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>.

[36] S.H.M. Ja'fri, *The Origins and Early Development of Shi'a Islam* (Oxford: Oxford University Press, 2002).

[37] FATF, *Emerging Terrorist Financing Risks*.

[38] FATF, *The role of hawala and other similar service providers in money laundering and terrorist financing*, (Paris: FATF, 2013), available at <http://www.fatf-gafi.org/publications/methodsandtrends/documents/role-hawalas-in-ml-tf.html>.

[39] Ja'fri, *The Origins and Early Development of Shi'a Islam*.

[40] Brian Bennett, "With Islamic State using instant messaging apps, FBI seeks access to data," *LA Times,* June 8, 2015, available at <http://www.latimes.com/world/middleeast/la-fg-terror-messaging-20150608-story.html>.

[41] Trevor Gundy, "In Britain, glut of anti-terrorism campaigns draws fans and critics," *USA Today,* August 15, 2015, available at <http://www.usatoday.com/story/news/world/2015/08/15/britain-glut-anti-terrorism-campaigns-draws-fans-and-critics/31773737/>.

[42] Briggs and Silverman, *Western Foreign Fighters Innovations*.

[43] Richard Stengel, "State Department Memo on the Islamic State Group," *New York Times,* June 9, 2015, available at <http://www.nytimes.com/interactive/2015/06/12/world/middleeast/document-state-department-memo-on-the-islamic-state-group.html>.

[44] Vanda Felbab-Brown, *Despite its siren song, high-value targeting doesn't fit all: matching interdiction patters to specific narcoterrorism and organised crime contexts* (Washington, DC: Brookings Institution, 2013), available at <http://www.brookings.edu/research/papers/2013/10/01-matching-interdiction-patterns-narcoterrorism-organized-crime-contexts-felbabbrown>.

[45] See: Tom McKay, "These 28 Instagram Pictures Just Busted One of the Biggest Mexican Drug Lords," *News Mic,* January 23, 2014, available at <http://mic.com/articles/79841/these-28-instagram-pictures-just-busted-one-of-the-biggest-mexican-drug-lords#.E3CCtDA50>; Tom Porter, "Mexican Cartel Members Face Arrest After Sharing Crimes on Facebook and Twitter," *International Business Times,* January 5, 2014, available at <http://www.ibtimes.co.uk/mexican-cartel-members-face-arrest-after-sharing-crimes-facebook-twitter-1431081>.

[46] LexisNexis Risk Solutions, *Survey of Law Enforcement Personnel and Their Use of Social Media*, 2014, available at <www.lexisnexis.com/investigations>.

[47] Margaret Shaw, "Illicit Narcotics Transiting West Africa: Actors, Finances and Impact," in *Illicit Financial Flows: The economy of illicit trade in West Africa,* OECD/AfDB (Paris: OECD Publishing, forthcoming).

[48] Anine Kriegler, "Using Social Network Analysis to Profile Organised Crime," *Institute for Security Studies*, 2014, available at <https://www.issafrica.org/uploads/PolBrief57.pdf>.

[49] FATF, *The role of hawala and other similar service providers.*

[50] Reporters Without Borders, "Non-State Groups: Tyrants of Information," 2015, available at <https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Ranglisten/Rangliste_2015/150211_Nichtstaatliche_Gruppen_EN.pdf>.

[51] Benoit Hervieu, "Organized Crime Muscling in on the Media," 2014, available at <https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Presse/Downloads/Berichte_und_Dokumente/2011/110224_RSF-Bericht_Organisierte_Kriminalitaet_Pressefreiheit.pdf>.

[52] Elisabeth Witchel, "Getting Away with Murder," *Committee to Protect Journalists,* April 16, 2014, available at <https://cpj.org/reports/2014/04/impunity-index-getting-away-with-murder.php>.

[53] Global Initiative, "Dangerbeat: Journalists Under Fire for Investigating Organized Crime," *Global Initaitive against Transnational Organized Crime*, August 14, 2014, available at <http://www.globalinitiative.net/dangerbeat-journalists-under-fire-for-investigating-organized-crime/>.

[54] Natasha Lomas, "U.K. Government Points Finger Of Blame At Web Firms For Counter-Terror Failures," *Tech Crunch,* November 26, 2014, available at <http://techcrunch.com/2014/11/26/surveillance-scapegoats/>.

[55] *Counter-Terrorism and Security Act 2015,* London, 2015, available at <http://www.legislation.gov.uk/ukpga/2015/6/contents/enacted>.

[56] Eliana Dockterman, "Turkey Bans Twitter," *TIME,* March 20, 2014, available at <http://time.com/32864/turkey-bans-twitter/>; "Freedom on the Net 2014," *Freedom House*, 2015, available at <https://freedomhouse.org/report/freedom-net/freedom-net-2014#.Vp5QW_nR_IU>.

[57] Scott Higham, and Ellen Nakashima, "Why the Islamic State leaves tech companies torn between free speech and security," *The Washington Post,* July 16, 2015, available at <https://www.washingtonpost.com/world/national-security/islamic-states-embrace-of-social-media-puts-tech-companies-in-a-bind/2015/07/15/0e5624c4-169c-11e5-89f3-61410da94eb1_story.html>.

[58] Nancy Scola, "Obama's anti-ISIL push falls flat on social media," *Politico*, August 12, 2015, available at <http://www.politico.com/story/2015/08/obamas-anti-isil-push-falls-flat-on-social-media-121301>.

[59] Jared Cohen, Director, Google Ideas, as quoted in Neal Ungerleider, "How Google Fights Terrorists and Human Traffickers," *Fast Company,* July 17, 2012, available at <http://www.fastcompany.com/1842993/how-google-fights-terrorists-and-human-traffickers>.

[60] Google Ideas, *Summit against Violent Extremism,* June 26-29 2011, available at <https://www.google.com/ideas/events/save-2011/formers/>.

[61] See: Maeve Shearlaw, "Did the #bringbackourgirls campaign make a difference in Nigeria?" *The Guardian,* April 14, 2015, available at <http://www.theguardian.com/world/2015/apr/14/nigeria-bringbackour-girls-campaign-one-year-on>; Amnesty International, "Our job is to shoot, slaughter and kill," *Boko Haram's reign of terror in North East Nigeria*, 2015, available at <http://www.coalitionfortheicc.org/documents/AFR4413602015ENGLISH.PDF>.

[62] François Crépeau and Francisco Carrión Mena, "Statement by the Special Rapporteur on the human rights of migrants, François Crépeau, and the Chair of the UN Committee on the Protection of the Rights of Migrant Workers and Members of Their Families, Francisco Carrión Mena," *United Nations Human Rights,* October 23, 2015, available at <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16641&LangID=E>.

[63] Kim Ghattas, "The Sad Fading Away of the Refugee Crisis Story," *Foreign Policy,* October 19, 2015, available at <http://foreignpolicy.com/2015/10/19/the-sad-fading-away-of-the-refugee-crisis-story/>.

[64] Muggah, "The rising threat of organised crime on social media."

[65] Gabrielle Ramaiah and Jason Warner, "Four ways social media could transform conflict in Africa," *CNN,* July 16, 2012, available at <http://globalpublicsquare.blogs.cnn.com/2012/07/16/fours-ways-social-media-could-transform-african-conflicts/>.

[66] Andres Monroy-Hernández, Emre Kiciman, Danah Boyd, and Scott Counts, "Narcotweets: Social Media in Wartime," *Microsoft Research*, 2012, available at <http://research.microsoft.com/pubs/160480/ICWSM12-093.pdf>; Muggah, "The rising threat of organised crime on social media."

[67] Jason McGahan, "She Tweeted Against the Mexican Cartels, They Tweeted Her Murder," *The Daily Beast*, October 21, 2014, available at <http://www.thedailybeast.com/articles/2014/10/21/she-tweeted-against-the-mexican-cartels-they-tweeted-her-murder.html>.

[68] Muggah, "The rising threat of organised crime on social media."