

**STATEMENT OF JOHN K. DONOHUE
FELLOW, RUTGERS UNIVERSITY, MILLER CENTER FOR COMMUNITY
PROTECTION AND RESILIENCE
FORMER CHIEF OF STRATEGIC INITIATIVES, NEW YORK CITY POLICE
DEPARTMENT**

**HEARING ON “ASSESSING THE THREAT FROM ACCELERATIONISTS AND
MILITIA EXTREMISTS”**

**BEFORE THE U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM**

**VIA WEBEX, WASHINGTON, DC
THURSDAY, JULY 16, 2020**

Good morning Chair Rose, Ranking Member Walker, and members of the subcommittee. I am John Donohue, a Fellow at Rutgers University, Miller Center for Community Protection and Resilience and a recently retired Chief of the New York City Police Department (NYPD) having spent thirty-two years in service of the people of New York in a variety of assignments, notably in patrol, policy, strategy, and intelligence. I am pleased to testify before your subcommittee today to discuss the significant public safety concerns and, specifically, challenges to law enforcement raised by the growing phenomenon of cyber-social militia extremism and the power of on-line movements to influence violent action domestically.

Overview:

The use of social media for promoting ideas is well documented. These technology platforms, now mobile and near ubiquitous, have usurped the traditional venues of the public square and printed newspapers for communicating the concerns, likes and desires of hundreds of millions of people world wide. Here in the United States where we cherish the constitutional right to speak freely, assemble and protest, social media has been embraced by virtually everyone with access to the internet to share their opinions on any topic, at any time. The ability to garner an audience to any cause beyond mere affinity, however, considering the vast number of people on the vast number of social media platform, requires a few more powerful ingredients. Before the COVID-19 pandemic, these ingredients - social isolation, vast unemployment, fear of changing social order, and the most powerful ingredient, a perceived martyr for the cause - existed to a much lesser degree. During the pandemic, in contrast to any previous time in world history, those ingredients have dramatically come into alignment. What is observable and quantifiable from social media data is an exponential growth in participation in the cyber-social domain that has coalesced around revolutionary extremist themes at either end of the ideological spectrum. And those revolutionary extremists have federal, state and local law enforcement squarely in their sights. The outcomes are not predictable, and the time for acknowledging this phenomenon and rapidly working to preserve civil society is upon us.

Cyber-social Domain for Recruitment:

In the internet, as in all media, content is king. Recent history is rife with the use of social media content to recruit people to a cause. In less than a generation, the hashtag “#” has become the easiest way of identifying - and identifying with - a message. Merely clicking like, commenting on or sharing content serves to boost those messages. Add memes or brief videos to the content and the message will meet the desired audience, literally in the palm of their hand. In a few cases some messages “go viral” into the mainstream, where even casual users of social media will be exposed to the content. We’ve seen this in the #bringbackourgirls and #metoo movements. To accelerate a message, add issues with intense emotional attachment, such as religious or strongly held political beliefs, and the content can become a tool of recruitment to further activity of the cause.

For example, we know that in early 2013 and 2014 in the earliest stages of the ISIS caliphate, the use of social media motivated some youth, impressionable, isolated, disaffected, and religiously influenced, to leave their homes, including here in the United States, and take up arms in support of Abu-bakkar Al Baghdadi and ISIS. Social media companies were slow to respond in blocking content that drew youth into that sphere. Some criminal cases showed once a person was drawn into the movement and became engaged in social media (liking, sharing, posting, creating content) they could be recruited into a much deeper level of involvement. That’s when conversations migrate from the surface web, to deep web forums and to encrypted communication platforms in which there is no visibility.

The same cycle is happening domestically with militia movements of the far-right and far-left. The report I co-authored in May of this year for the Rutgers University Miller Center and Network Contagion Research Institute (NCRI)¹ demonstrates how on social media sensational memes become viral and evolve, permitting extremists to plant hateful or revolutionary ideas in the public eye, often disguised as inside jokes or codewords for those “in the know.” The boogaloo, big igloo, or big luau, code for the second revolution, is an example of the far-right militia movement. In protest of the recent pandemic lockdowns, followers of the movement played out the inside joke by wearing Hawaiian shirts and carrying semi-automatic rifles in the center of a few major cities. The volume and intensity of posts with boogaloo affinity on reddit doubled in one year through April 2020². Among the boogaloo meme contributors are those who “gamify” assaults on police and law enforcement, encouraging violence through jargon known in the video gaming community.

While it appears that the preponderance of the on-line militia sphere is inhabited by far-right extremists, they are by no means alone. In a forthcoming report, we at Rutgers and Network

¹ Finkelstein, Donohue, Goldenberg, Baumgartner, Farmer, Zannettou, & Blackburn (2020) COVID-19, Conspiracy and Contagious Sediton: A Case Study on the Militia-Sphere. The Network Contagion Research Institute. (online at www.ncri.io/reports/covid-19-conspiracy-and-contagious-sediton-a-case-study-on-the-militia-sphere/)

² id.

Contagion Research Institute will demonstrate that online anti-police messaging on anarchist and other far-left social media spaces, such as on sub-reddit forums saw exponential increases during the most recent period of civil unrest in America following the killing of George Floyd. These messages have broken into the mainstream including Facebook and Twitter. Memes advocating the murder of law enforcement, and slogans found on the internet such as ACAB, F12, 1312 used by the far-left appeared scrawled on the defaced monuments and buildings all over America. Assaults on and the murder of law enforcement that occurred during the recent civil unrest were motivated in part by the themes in these memes and slogans³.

Inherent Tension between Constitutionally Protected Activities and Policing:

Among the many rights afforded to us in the First Amendment to the United States Constitution is that Congress cannot pass laws limiting freedom of speech and peaceful assembly. The Second Amendment protects Americans' right to keep and bear arms. The Fourteenth Amendment ensures those rights are protected in every state. Those rights are not absolute, as the Supreme Court has interpreted from time to time. For example, we know that reasonable time, place and manner restrictions can be applied to public assembly, and reasonable restrictions exist with regard to commercial speech. There are also some state specific laws that permit open-carry of lawfully owned firearms, and other states that have outlawed that practice - both have withstood constitutional scrutiny. I use these two amendments for examples because in real life, on the street, when tens, or tens of thousands of people are assembled is where the tension exists. In those circumstances, explaining the finer points of constitutional law to a crowd just doesn't work, that's why police are generally at a disadvantage, and specifically challenged when they are the *target* of the protests. The presence of armed militia members raises the complexity and volatility of those situations.

In New York City, as a police officer I wore a uniform and policed protests, taking care to ensure impartial treatment of those who wanted their message to be heard by local, state, federal governments and even the United Nations. To be candid, the issue, cause, or message protestors share at a physical gathering, as well as a virtual one, is irrelevant to nearly everyone in law enforcement. That's what impartiality demands. We teach it in our nation's police academies. And we need it in a constitutional democracy. However, sometimes protesters want their message to be "more effective," "louder" or "disruptive." They use coded words and memes to train the movement to conduct "direct actions" and "wildcat actions." Many carefully planned protests use encrypted communication platforms to direct and target unlawful actions of the participants.

Tension also exists in planning for public safety during these events. That's because pre-operational intelligence is needed for many reasons. For example: Will traffic need to be

³ For example: In May 29 and June 6, 2020 respectively, David Patrick Underwood a Federal Protective Service contract guard and Sheriff Sgt. Damon Gutzwiller were murdered by a boogaloo movement adherent. See also: Urooj Rahman and Colinford Mattis who were arrested and charged by the U.S. Attorney for the Eastern District of New York for allegedly firebombing a NYPD vehicle.

rerouted? will medical responders need to be prepositioned? Will there be counter-protesters? Will protesters engage in unlawful activity and expect to be arrested? How many police will be needed to ensure the safety of all parties? As an intelligence officer we faced these questions routinely in preparation for an event. Intelligence also requires answering the questions about the unknowns: Are the intentions of the group or subgroups to engage in violence? If so, will weapons be involved?

In the past, unrestrained domestic intelligence gathering and activities led to lawsuits and settlements that curtailed egregious intelligence practices. In response, the Attorney General promulgated Guidelines for Domestic FBI Operations, and the FBI has the Domestic Intelligence Operations Guide (last updated in 2016)⁴. The New York City Police Department (NYPD) was sued in the 1970's for investigative overreach⁵. Consequently, the NYPD has operated intelligence capacities under a federal judicial consent decree that was modified several times to ensure effectiveness and to balance civil liberties, most recently in 2016.

Law enforcement a tough task when policing protest events in the best of times; when protesters arrive intent on violence and occupation and are carrying semi-automatic weapons, the stakes grow exponentially. Accelerationists and Militia members know this and seize on those opportunities to amplify their message of revolution through direct confrontation with police.

Complexity of Monitoring Networks of Individuals and Identifying Those Who Will Mobilize to Violence:

There are technology solutions that researchers use to quantify authentic growth of postings, unique events, and to discount those that are generated by bots. Those same technologies can help identify the frequency and intensity of social media postings. However, I'm not aware of any reliable technology that can determine true sentiment of social media postings beyond the stop-gap interventions employed by some surface web social media companies. Some companies use their terms of service and attempt to have users enforce community standards. The larger social media companies have hired people to review offensive posts. The tension between free sharing ideas, debate, community norms and corporate-message control slows social media companies' response. Some companies have taken action when pressured to act, with varying degrees of success. The results resemble a game of whack-a-mole, with content finding its way from one part of the net to another. Despite the companies' efforts to minimize the availability of extremist messages, those messages persist. Ultimately, social media companies are not in the position to identify those who will mobilize to violence.

⁴See: Retrieved July 12, 2020 <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version>

⁵ Handschu v. Special Services Div., 605 F. Supp. 1384 (S.D.N.Y. 1985)

Until someone can, law enforcement must remain vigilant to identify the radicalized before they mobilize. The timeframe for intervention, however, can be remarkably short. Immediately before Robert Bowers attacked the Tree of Life synagogue in Pittsburgh in October 2018, he posted on a website, “I can’t sit by and watch my people get slaughtered. Screw your optics, I’m going in.”

While law enforcement is the last line of defense against extremists who mobilize to violence, it may be their own lives that they save because they have become the ultimate target.

Path Forward:

The problem we face is that social unrest is being effectively organized in the social-cyber domain, into potential insurgencies, on the basis of memes and short messages. This structure is both highly visible on the one hand and fundamentally invisible on the other because though it is ubiquitous. No single entity can contextualize the sheer scale of coded language and memes. Law enforcement certainly must not violate the constitutional protections on citizens' free speech as it tries to distinguish imminent threats from jokes.

America is at a cross roads, the intersection of constitutional rights and legitimate law enforcement has never been more at risk by domestic actors as it is now as seditionists actively promote a revolution. However, I remain confident that America remains strong to its founding principles and recommend the following as possible paths forward.

Social media companies were slow to act during the rise of ISIS message amplification and recruitment activities. These companies cannot be alone in combatting extremist ideologies and accelerationists, but they are part of the solution. And legislation is needed to ensure those companies work collaboratively with civic leaders across the spectrum for a civil society.

Just as the internet is diffuse, the solution cannot reside in singular entity. With regard to extremist actions there needs to be better coordination among law enforcement intelligence capacities, supported by appropriate Department of Justice entities and a social media companies to rapidly respond to hate driven seditious rhetoric where the content and context clearly demonstrates unlawful activity is about to occur, is occurring or is being planned.

The challenges to law enforcement and investigations associated with encrypted communication platforms - the “going dark” issues- must be addressed both technologically and legislatively.

Just as we needed better air-traffic information after 9/11, what is needed is something fundamentally new, both technologically and socially. What is needed technologically is akin to a social media NORAD, a monitoring station that is technologically capable to generate finished intelligence rapidly and at a massive scale that can perceive imminent threats before they emerge, and detail them as the work at Rutgers and the Network Contagion Research Institute seeks to do with such tools.

Powerful technology such as I'm suggesting, must have controls. Socially, we have come to a moment where there is a need for a public trust or neutral third party that can use such technology with credibility to report on threats to democracy and imminent threats to public safety. Such a trust must be one run in partnership with civil society, whose purpose to to further the American civic tradition.

Rather than merely catching the criminal before the next attack, the best use of this public trust would be to fight for our norms at a massive scale. To intercede before radicalization with information civil society led counter-messaging and civic engagement. In other words, we aren't going to censor each other our our problems away on social platforms, and we aren't going to censor one another out of existence through violent insurrection either. We are going to have to use our words. The best use of the solution I propose here is using technology to do that, because that is what furthers and protects democratic traditions.

These are fundamentally the traditions that now find themselves under direct attack by the extreme left and extreme right alike. How we ultimately move forward together as a country, as Americans, depends how we negotiate this moment in history. Thank you.

###