

TESTIMONY OF JOHN COHEN
ADJUNCT PROFESSOR
GEORGETOWN UNIVERSITY
SECURITY STUDIES PROGRAM
BEFORE THE
COMMITTEE ON HOUSE ADMINISTRATION
SUBCOMMITTEE ON ELECTIONS
JULY 27, 2022

“A Growing Threat: Foreign and Domestic Sources of Disinformation”

Introduction

Good morning, Chairman Butterfield, Ranking Member Steil , and members of the Sub-Committee.

Thank you for the opportunity to testify on the current threat facing the United States from foreign and domestic threat actors who use Internet-based communication and information platforms to engage in illicit or other activities harmful to our national security. It is one of the most important national security issues facing our country and I appreciate the opportunity to provide insights.

The observations I will share today are my personal perspectives and informed by my close to forty years of experience working on law enforcement, homeland security, intelligence and counter-intelligence issues. I have had the opportunity to work in both Republican and Democrat administrations and I have worked on these issues at the Federal, state, and local levels of government. I have also worked closely with those in academia, the private sector, and the non-profit community to better understand and address these complex issues.

While the primary focus of this Sub-committee is the threat to our election process, I would like to take a moment to describe the broader threat environment facing the United States, particularly as it relates to the threat of mass casualty attacks and acts of targeted violence. I would also like to describe how our adversaries use information warfare to disrupt our elections, and destabilize and weaken our Nation. This is a threat that has escalated over the past decade and impacts most national and homeland security issues facing the United States.

The Current Threat Environment

Today, the United States is confronting a threat environment that is the most volatile, complex and dynamic of any that I have experienced in my career.

The 2022 mid-term election cycle is taking place at a time when the Nation is experiencing a sustained threat of mass casualty attacks. Far too many communities have experienced tragic

events such as the mass killings in Buffalo, NY, Uvalde, TX, and Highland Park, IL. The tempo of these attacks is increasing and as a Nation we are currently experiencing an epidemic of mass casualty violence.

As repeatedly assessed by both the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), the most significant terrorism-related threat facing the US today comes primarily from lone offenders – who engage in violent activity inspired by extremist beliefs and/or personnel grievances that are in most instances cultivated through the consumption of online content.

It is a trend line that began several years ago and continues to evolve. And while the specific motives behind these attacks vary – analysis tells us that many of the attackers share common behavioral characteristics – in particular they are angry, feel socially disconnected, seeking a sense of life meaning, they spend significant time online and ultimately self-connect with a cause or grievance to justify the use of violence to as a way to express their anger and achieve a sense of social connection and self-worth. They use content they find online to justify, inform, plan and prepare for their attack. They will often discuss their intent to engage in violence online in both open and closed online forums and communities as they prepare to engage in acts of targeted violence.

Their behaviors often do not fit neatly into traditional terrorism, extremism or violent crime related definitional categories. Those who engage in violence often self-connect with a combination of extremist beliefs or a blend of extremist beliefs and personal grievances. This complicates investigative and analytic activities.

Fueling these acts of violence is an online and media eco-system that is saturated with conspiracy theories and other content purposely placed there by foreign and domestic threat actors including foreign intelligence services, international terrorist groups, domestic violent extremists, and criminal organizations.

These threat actors seek to exploit the fractures, anger and discord in our society and our political discourse by using social media and other online communications platforms to spread disinformation, conspiracy theories, extremist rhetoric and other false narratives online. From an information operations perspective, their hope is that once introduced, these carefully chosen socio-political narratives will spread rapidly across social media and the Internet and eventually become amplified by mainstream public figures so that they are consumed by the broadest number of people possible. Their operational objectives include: sowing discord; undermining confidence in government and democratic institutions; diminishing our standing in the global community; destabilizing our society; and at times inspiring violence. Their efforts have and continue to include calls for violence directed at people due to their race, ethnicity, immigration status, sexual orientation, political beliefs, and increasingly government officials from both political parties and law enforcement.

This content will migrate across the online and media ecosystem where it is consumed by a broad cross-section of Americans who see it, believe it, spread it and act on it. In some cases, the reaction to this content may be legal and even constitutionally protected. But in other cases –

the reaction can include targeted attacks, destructive behavior, and other illegal activity by those in our society who believe that violence is an acceptable way to express one's anger or disagreement with government policies and programs.

Recent attacks have targeted a cross section of our society – people and facilities have been targeted because of the faith, political beliefs, race, gender or ethnicity. At other times, attackers have targeted locations where large numbers of people gather such as retail, entertainment or transportation facilities. In other instances, these attacks were directed at law enforcement and government officials.

In 2021, the National League of Cities reported that that 87% of surveyed local officials had observed an increase in attacks on public officials in recent years. The report blamed political polarization, social media, and the spread of misinformation for the increase. Additionally, the Fraternal Order of Police has recently reported that in the first six months of 2022, there have been 35 ambush-style attacks on law enforcement officers—12 of whom died—, and 178 officers have been shot in the line of duty, a 19% jump from 2021. This increase is occurring at the same time we are seeing the spread of graphic content calling for acts of violence directed at law enforcement on a variety of extremist forums. And just last week, Lee Zeldin, while campaigning in New York State, was targeted by a knife wielding attacker. These attacks directed at government officials are occurring as the Nation responds weekly to mass shootings such as those in Buffalo, NY, Highland Park, Illinois and Uvalde, Texas.

Threat to the Election Process

As the 2022 mid-term election draws closer, law enforcement and election officials across the Nation are preparing to address a variety of threat related activities to include:

- **Election Violence** - in 2022, DHS warned that “narratives on other sociopolitical developments – such as claims of election fraud during the 2020 General Election, upcoming 2022 midterm elections, and the emboldening impact of the violent breach of the U.S. Capitol – almost certainly will be used to spur some violent extremist to seek to engage in violence.” Law enforcement authorities are concerned about potential acts of violence at open air, publicly accessible parts of the physical election infrastructure, such as campaign associated mass gatherings, polling places and voter registration events would be the most likely flashpoints for potential violence.
- **Threats Against Election Officials** – we've seen and expect a further increase in threats directed at Republican and Democratic Secretaries of State, and civil servants simply doing their jobs in line with their state's election laws. Perhaps most concerning, election officials and workers' families—their children, their wives, and their parents—have received threats. A Brennan Center report released earlier this year highlighted that, based on a survey of the election community, one in six election officials have received threats and thirty percent of those polled know an election official who quite due to threats.
- **Tampering with Election Equipment** - ballot storage containers, drop-boxes, mail boxes are tampered with, destroyed, removed resulting in ballots not being counted.

- **Voter Suppression/Intimidation** – individuals or groups self-deploying to polling sites - under the guise of poll watching - but who behave in a manner that serves to intimidate other-wise influence voters not to vote or vote a specific way.
- **Disinformation and Cyber Attacks** – in a September 2020, DHS and the FBI warned “Foreign actors and cyber criminals could create new websites, change existing websites, and create or share corresponding social media content to spread false information in an attempt to discredit the electoral process and undermine confidence in US democratic institutions.”
 - In September 2020, DHS further warned that “Russia is likely to continue amplifying criticism of vote by mail and shifting voting processes amidst the COVID-19 pandemic to undermine public trust in the electoral process.”
 - That same month, FBI’s San Francisco office warned of the potential for “cyberattacks against political campaigns and government infrastructure,” secret funding or influence operations to help or harm a person of cause,” and disinformation campaigns on social media platforms that confuse, trick or upset the publics – includes focusing on social issues to provoke and encourage conflict.

Responding to the Threat

Intelligence and Information Sharing - we need to think differently about intelligence and information sharing. Critical pre-incident indicators and other threat-related information may be introduced, amplified and spread broadly on open and closed online forums. Use of highly sensitive Intelligence Community collection tools are not needed to uncover information regarding emerging threats of violence – this information is often publicly available on open source platforms.

Law enforcement operations may benefit through greater access to non-traditional sources of information such as research by academic and non-profit organizations. More can and should be done to understand how foreign and domestic threat actors are using Internet-based communication tools to spread content in furtherance of activity that is illegal and/or harmful to our national security and we need to do more to ensure that information that can inform investigative or other security operations is shared with those who need it.

However, information gathering activities must be guided by clear guidelines and oversight to ensure that the privacy and civil liberties of Americans are protected. Those gathering information from open and closed forums must distinguish between constitutionally protected speech and threat-related activity and be guided by the underlying principle that it is not the role of law enforcement and security officials to police thought – but to prevent violence.

Preventing Acts of Violence - we need to do more to prevent acts of violence. Educating the public regarding the nature of the threat facing the Nation as well as the warning signs of a pending attack they may observe is critical. Ensuring that local communities are prepared to manage the threat posed by those assessed by mental health and/or trained law enforcement professionals to be high risk is vital as well. More support for community-based violence

prevention programs as well as enhanced public education regarding how threat actors use the Internet to purposely spread content would go far in supporting national efforts to address the current threat environment.

We must also take steps to improve media literacy. Everyone, from children to teenagers to adults, need to improve their ability to think critically about information they consume, particularly online, and know where to find trusted sources.

As it relates to those who work within the election infrastructure, we must do all that we can to keep them and our election related facilities safe from violence. To do so, we must ensure that election officials work close with local, state and Federal law enforcement officials to both understand and address emerging threat-related issues. The physical security of our election infrastructure is paramount and Congress can ensure that adequate resources are allocated to election officials to implement physical security measures, such as installing cameras, reinforced doors, and bulletproof glass at their offices.

Closing

Thank you for inviting me to join you today.

We are in the midst of a multi-year threat pattern that has resulted in violence and direct attacks against the very foundation of our Republic. It is a threat environment that manifests itself in both the physical and digital environments.

People shouldn't be scared to go to church, synagogue, school, work or a parade, a mosque, a supermarket or a shopping mall because they fear becoming the victim of a mass shooting. People shouldn't be fearful to serve in public office or work in a polling place, or serve as an election official. Yet they are.

Too many people are angry and view those who hold opposing views as the enemy. Too many people believe conspiracy theories and socio-political content that have been developed and spread specifically by foreign and domestic threat actors to fan the flames of that anger. Our Nation is more vulnerable to information warfare attacks by these threat actors today because of the anger, division, and discord that has become all too common within our political process and public discourse.

Our ability to protect our communities is hampered because often times we cannot even agree on what should be considered a threat. Protecting the people of this Nation must rise above politics and hearings such as this are important because they provide an opportunity for law-makers to better understand the complex, dynamic and evolving nature of the threat facing the United States and take steps to enhance our Nation's ability to address those threats.

And that is a step in the right direction.

I look forward to your questions.

