NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE ROLE OF INTELLIGENCE FUSION CENTERS IN FIGHTING DOMESTIC VIOLENT EXTREMISM

by

Grozdan S. Naydov

December 2022

Thesis Advisor: Erik J. Dahl
Second Reader: Wade L. Huntley

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE THE ROLE OF INTELLIGENCE FUSION CENTERS IN FIGHTING DOMESTIC VIOLENT EXTREMISM	**5. FUNDING NUMBERS**
6. AUTHOR(S) Grozdan S. Naydov	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Over the years, the National Network of Intelligence Fusion Centers, established after the 9/11 attacks, was able to evolve and adapt to new threats and challenges to security environments. Domestic violent extremism became a serious challenge to U.S. security, especially after the development of social media. The most dangerous representatives of violent domestic extremism are the far-right extremists, who have become very active in the last decade. The far-right groups successfully used social media for organization and propaganda by spreading disinformation and conspiracy theories. This thesis tries to understand the role of state and local fusion centers in the fight against violent far-right extremists. To answer that question, this thesis analyses the intelligence fusion centers' actions concerning the Capitol insurrection by far-right extremists on January 6, 2021, and disinformation campaigns during the 2016 and 2020 U.S. presidential elections. The findings are that fusion centers played an important role during the Capitol insurrection by exploiting open-source intelligence. On the other hand, fusion centers are not effective against foreign or, especially, domestic disinformation campaigns. Therefore, more federal support is needed to improve the fusion centers' capacity to help contain the spread of disinformation.

14. SUBJECT TERMS intelligence fusion centers, intelligence, privacy violations, violent extremism, domestic violent extremists, disinformation, conspiracy theories, hate groups, far-right, white supremacists, domestic terrorism, Jan 6, Capitol Insurrection, presidential elections	**15. NUMBER OF PAGES** 135
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE ROLE OF INTELLIGENCE FUSION CENTERS IN FIGHTING DOMESTIC VIOLENT EXTREMISM

Grozdan S. Naydov
Captain, Bulgarian Special Operations Forces
BA, National Military University , 2011

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2022**

Approved by: Erik J. Dahl
Advisor

Wade L. Huntley
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Over the years, the National Network of Intelligence Fusion Centers, established after the 9/11 attacks, was able to evolve and adapt to new threats and challenges to security environments. Domestic violent extremism became a serious challenge to U.S. security, especially after the development of social media. The most dangerous representatives of violent domestic extremism are the far-right extremists, who have become very active in the last decade. The far-right groups successfully used social media for organization and propaganda by spreading disinformation and conspiracy theories. This thesis tries to understand the role of state and local fusion centers in the fight against violent far-right extremists. To answer that question, this thesis analyses the intelligence fusion centers' actions concerning the Capitol insurrection by far-right extremists on January 6, 2021, and disinformation campaigns during the 2016 and 2020 U.S. presidential elections. The findings are that fusion centers played an important role during the Capitol insurrection by exploiting open-source intelligence. On the other hand, fusion centers are not effective against foreign or, especially, domestic disinformation campaigns. Therefore, more federal support is needed to improve the fusion centers' capacity to help contain the spread of disinformation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADL	Anti-Defamation League
DHS	Department of Homeland Security
DOJ	Department of Justice
DVE	domestic violent extremism
FLO	Fusion Center Liaison Officer
GAO	The Government Accountability Office
HVE	homegrown violent extremist
IFC	Intelligence Fusion Center
ILP	intelligence-led policing
IC	Intelligence Community
JIC	Joint Intelligence Center
MDP	Metropolitan Police Department for the District of Columbia
MVE	militia violent extremists
ODNI	Office of the Director of National Intelligence
P/CRCL	privacy, civil rights, and civil liberties
RMVE	racially or ethnically violent extremist
SPLC	The Southern Poverty Law Center
TEWG	Terrorism Early Warning Group
WSE	white supremacist extremist

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First, I want to thank the Bulgarian Joint Special Operation Command, which provided the opportunity and necessary support to study at one of the best military universities. Secondly, I want to thank all my great faculty members at the Naval Postgraduate School for their efforts to teach us how to think critically, to doubt, and always to seek the answers to our questions. I also would like to give special appreciation to my thesis adviser, Professor Erik Dahl, to whom I owe my success because whenever I needed support, he always provided his advice and brought me back on the right track. Thanks to my second adviser, Professor Wade Huntley, who has always been very dedicated and objectively critical of my work. I also want to thank the wonderful writing coaches in the Graduate Writing Center who supported my work throughout my education at NPS. Lastly, I want to say a huge thanks to my wife, Plamena, who was with me the whole time and suffered all my difficulties right next to me. Thank you all!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

Since 9/11, the U.S. structures of homeland security and the Intelligence Community (IC) have changed dramatically. These changes have been driven by the emergence of the international terrorist threat. That new threat led to the understanding that sharing information between intelligence agencies produces more benefits for homeland security than keeping information tightly restricted. This conclusion led to the IC's reforms and the emergence of 80 intelligence fusion centers (IFC) on the U.S. territory. Now we are standing again in a challenging period with a major change in the social, technological, and international arenas which adds new challenges that must be managed. Domestic Violent Extremism (DVE) combined with modern ways of communication presents a significant challenge to the IC. Hence, this thesis asks, what is the role of fusion centers in U.S. homeland security, and can fusion centers address today's problem of the increasing threat from domestic violent extremism?

B. PROBLEM STATEMENT

After the end of the Cold War, the U.S. Intelligence Community failed to adapt to the new situation, and it did not prioritize its efforts toward the emerging threats, such as international terrorism. The cost of this failure was paid by the victims of the 9/11 attacks and by the entire U.S. nation. The events of 9/11 revealed the weaknesses of the U.S. Intelligence structure, and new measures and strategies were adopted. Information sharing has been one of the major failures of the IC, and in this area, there were significant improvements. The creation of a network of IFCs was a significant success. This network had to facilitate a sharing process between federal agencies, state agencies, and local security services. The Fusion Centers play a very important part in the intelligence cycle, and their creation was intended to facilitate the fight against international terrorism so that a failure like 9/11 would never again occur.

There are different opinions about how successful the IFCs have been in the fight against contemporary threats. Despite complaints by some critics, they have largely been

considered as successful. The success of IFCs is evident in that the United States has not had a major attack from an international led terrorist organization and the sharing of intelligence has improved considerably.

Similar to the change in threat environment after the Cold War, the issue that arises 20 years after 9/11 is that nations are facing a new primary threat today: domestic extremism. The Fusion Centers' primary mission is to fight against terrorist threats coming from abroad, yet many assert that the primary threat is coming from homegrown and domestic actors. The main problem is that to address domestic terrorism the IFCs have to collect and analyze information about U.S. citizens, but these actions are very limited because they are regulated by the U.S. Constitution. Further complications arise from the presence of Great Power competitors and technological advancements bolstering the arsenal of adversaries.

Domestic violent extremism is a major threat to homeland security. The main problem now is that the threat is coming from U.S. citizens and that significantly challenges the work of the IFCs. Knowing the lessons of history, we have to ask, "Has the IC learned the lessons of history before 9/11?" In particular, many concerns about the work of the IFCs come from the dilemma regarding how to maintain an accurate balance between providing eligible intelligence without violating civil liberties. According to Amy Zegert, the failure of the IC to adopt to the new threat environment is due to "the nature of the organizations…Government agencies are not built to change with the time."[1] If she is right, this means that in order to adapt to the emerging threats the U.S. has to suffer similar catastrophes as the 9/11 attacks. Is the U.S. in a situation where it has to sacrifice more civil liberties in order to provide the necessary security? Specifically, how can fusion centers adapt to better address today's threats in the face of this dilemma? These are important problems that need to be addressed in order to keep the homeland safe and secure.

[1] Amy B. Zegart, *Spying Blind* (Princeton, NJ: Princeton University Press, 2009), 59.

C. LITERATURE REVIEW

This literature review analyzes what scholars think about the advantages and disadvantages of the IFCs in the U.S. homeland and the emerging threats that come from domestic violent extremists. The first part of the literature review provides scholars' opinions mainly about IFCs' strengths, weaknesses, and privacy concerns. The second part of the literature review will focus mainly on the DVE after the financial crisis in 2008, when digital communications evolved significantly and enhanced the spreading of hate ideology easier than before. There is enough literature about these topics separately, but very little about the role of the IFCs in providing support to law enforcement to counter domestic violent extremists.

1. Intelligence Fusion Centers and Their Role in U.S. Homeland Security

IFCs are one of the new security structures created after 9/11, intended to improve information sharing between state and federal security services. Around their creation and development, there are many contradictions regarding how effective they are and whether they create possibilities for privacy violations. The necessity of an intelligence sharing environment between local and federal security services, however, was one of the conclusions reached after 9/11, and IFCs were developed to fill this gap.

a. Strength of the IFCs

The expectations from the network of fusion centers to boost information sharing and strengthen the U.S. homeland security after their creation were high. According to the Global Justice Initiative, the fusion centers are the main pillar of the collaboration between agencies, and as demand grows and resources shrink, they are becoming an effective tool for maximizing available resources and building trustworthy connections.[2] Many scholars also agree on the benefits of IFCs. Carla Lewandowski and Ray Guidetti suggest that the primary role of fusion centers is to coordinate personnel from different agencies in order

[2] Global Justice Information Sharing Initiative, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," The Bureau of Justice Assistance, 2008, 4, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines0.pdf.

to increase the effectiveness of information sharing.[3] These authors also suggest that this will break down the traditional obstacles of information sharing among agencies. In another piece by Jeremy Carter, Carla Lewandowski, and Gabrielle May, the state-level fusion centers are described as "brick-and-mortar entities comprising representatives primarily from federal, state, and local law enforcement agencies as well as members of the private sector and public works."[4]

According to some authors, the state and local fusion centers not only contribute to homeland security because they maximize the available resources, but they have additional advantages for the country. Donald Kettl investigated three events that defined the new federalism in the United States, and he noticed that during the Cold War, national security was only a responsibility of the federal government, but the age of terror changed that and put the local government as the main responders.[5] Erik Dahl extended this argument and asserted that "the localization of intelligence has had the effect of reducing the central government's authority over intelligence and bringing this important function of government closer to the people it serves."[6] He also found that state and local fusion centers are more effective in prevention than federal intelligence, and they contribute to the community they serve not only with the prevention of terrorism, but also in a way different from that they were originally created to fight against terrorism.[7]

---

[3] Carla Lewandowski and Ray Guidetti, "The Role of Fusion Centers in Homeland Security," in *Homeland Security and Intelligence 2d Ed. by Keith Gregory Logan* (ABC-CLIO Santa Barbara, CA, 2018), 4.

[4] Jeremy G. Carter, Carla Lewandowski, and Gabrielle A. May, "Disparity Between Fusion Center Web Content and Self-Reported Activity," *Criminal Justice Review* 41, no. 3 (September 2016): 336, https://doi.org/10.1177/0734016816651925.

[5] Donald F. Kettl, "Modern Federalism's Big 3 Moments - Potomac Chronicle: There's Been a Sea Change in the Way Levels of Government Deal with Each Other," *Governing Magazine (USA)*, October 1, 2017, http://infoweb.newsbank.com/apps/news/openurl?ctx_ver=z39.88-2004&rft_id=info%3Asid/infoweb.newsbank.com&svc_dat=AWNB&req_dat=0D0CB5FC0F5C3AD5&rft_val_format=info%3Aofi/fmt%3Akev%3Amtx%3Actx&rft_dat=document_id%3Anews%252F169D4DAB7005B380.

[6] Erik J. Dahl, "The Localization of Intelligence: A New Direction for American Federalism," *International Journal of Intelligence and Counterintelligence* 34, no. 1 (January 2, 2021): 3, https://doi.org/10.1080/08850607.2020.1716563.

[7] Dahl, 18.

b. Main Problems for the IFCs

Despite the approval and appreciation for fusion centers from some authors, there are also a lot of critics, debating mainly their effectiveness and raising concerns about the potential privacy violations. Torin Monahan and Neal A. Palmer examined social publications between 2002 and 2008. They concluded that IFCs "have been used for a variety of other purposes, such as basic policing, spying on social movement organizations, or restricting public legal activities such as taking photographs,"[8] but not so much for their primary objective: counterterrorism. They suggest that there are three main areas of concern about these centers: first, their ineffectiveness compared to the expenses; second, the risk of mission creep, in which fusion centers' activities expanded beyond their original intentions; and third, the civil liberty violations, addressing racial or First Amendment violations.[9]

Monahan and Palmer's study was conducted soon after fusion centers became operational, but there is also more recent research showing similar problems. Another critical report came in 2012 from the bipartisan Committee on Homeland Security and Governmental Affairs Senate Investigations Subcommittee. The Subcommittee conclusions were that the collaboration between the Department of Homeland Security (DHS) and fusion centers does not provide sufficient terrorist-related intelligence, the IFC funding is not conducted effectively, and many IFCs have priorities different than counterterrorism.[10] From a federal point of view, this seems to be a problem, but Lewandowski suggested that the expansion of IFCs' mission from counterterrorism to a broader "all-crimes" focus is done to meet the local jurisdictions' needs. She asserts that a

[8] Torin Monahan and Neal A. Palmer, "The Emerging Politics of DHS Fusion Centers," *Security Dialogue* 40, no. 6 (December 2009): 617, https://doi.org/10.1177/0967010609350314.

[9] Monahan and Palmer, 632.

[10] Tom Coburn, "Federal Support for an Involvement in State and Local Fusion Centers," Permanent Subcommittee on Investigations, October 3, 2012, 8.

uniform model for a fusion center is convenient from a federal perspective, but "many state and local agencies would likely prefer a fusion center built around grassroots needs."[11]

The effectiveness of IFCs depends on the personnel who work in them, and some authors connect the low productivity with the absence of high-quality workers. For example, Kevin Jack Riley et al. asserted that it was shocking how poor the analytical capabilities of local law enforcement personnel were, and only bigger police departments have dedicated analysts. This study found that the federal funds regarding human resources commitment have been spent for equipment and consequence management, but not for training in analysis.[12] More than ten years later, Lewandowski and Guidetti reached a similar conclusion about the importance of the human factor. According to them, the training of local law enforcement and private sector personnel is the key to the success of the fusion process.[13]

Other scholars investigated the collaboration between IFCs and stakeholders. The studies were intended to understand the perceptions of policemen toward the centers. After all, the success of the fusion centers depends on mutual information sharing between the officers and the responsible agencies. A study conducted by Cooney et al. in South Carolina, found that many local law enforcement officials find the state fusion centers useful, but still, there were policemen who did not appreciate it. The study showed that those who think that the fusion centers are helpful are policemen who identified themselves as engaging in intelligence-led policing and people who have received training about the fusion center. The findings indicated that fusion centers could increase the collaboration with local structures through more training and adaptation of intelligence-led policing.[14] The idea about a poor understanding regarding fusion centers is also found in the work of

---

[11] Carla Lewandowski and Ray Guidetti, "The Role of Fusion Centers in Homeland Security," in *Homeland Security and Intelligence,* 2nd ed. Keith Gregory Logan, ed. (Santa Barbara, CA: ABC-CLIO 2018), 179.

[12] Kevin Jack Riley and Rand Corporation, eds., *State and Local Intelligence in the War on Terrorism* (Santa Monica, CA: RAND Corporation, 2005), 17.

[13] Lewandowski and Guidetti, "The Role of Fusion Centers in Homeland Security," 17.

[14] Mikaela Cooney, Jeff Rojek, and Robert J Kaminski, "An Assessment of the Utility of a State Fusion Center by Law Enforcement Executives and Personnel," *Journal of Intelligence Analysis* 20, no. 1 (2014): 1.

Lewandowski in 2012. She suggested that local policemen do not understand the role of the fusion centers and they do not know what information to send back to the center.[15] In a more recent study Lewandowski, Carter, and Campbell emphasize the problem that IFCs do not receive feedback from the stakeholders, and due to this, the IFCs cannot satisfy their needs.[16]

c. Privacy, Civil Rights, and Civil Liberties

In the literature, one of the most discussed topics concerning IFCs is the violation of privacy, civil rights, and civil liberties (P/CRCL). The technology development and evolution of the threat environment increases the level of concerns regarding this topic. The problem between P/CRCL concerns and IFCs is widely addressed in federal documents. *The National Strategy for Information Sharing,* published in 2007, addressed privacy protection and other legal rights for information sharing by developing privacy guidelines consisting of twelve core privacy principles that "require specific, uniform action and reflect basic privacy protections and best practices."[17] This strategy established a protection framework for P/CRCL for both federal agencies as well as non-federal agencies. According to the document, the privacy governance is conducted by the Information Sharing Environment Privacy Guidelines Committee, which "seeks to ensure consistency and standardization, as well as serve as a forum to share best practices and resolve agency concerns."[18]

More specifically, the Department of Justice (DOJ) Global addressed the P/CRCL problem directly concerning the IFCs in Guideline 8 of *The Fusion Center Guidelines.* This section "utilize [s], and any fusion center should consider, the Fair Information Practices

---

[15] Carla Lewandowski, "Observations from within a State Fusion Center: Operations and Daily Routines," *IALEIA Journal*, 2012, 1.

[16] Carla Lewandowski, Jeremy G. Carter, and Walter L. Campbell, "The Role of People in Information-Sharing: Perceptions from an Analytic Unit of a Regional Fusion Center," *Police Practice and Research* 18, no. 2 (March 4, 2017): 183, https://doi.org/10.1080/15614263.2016.1250631.

[17] The White House, "National Strategy for Information Sharing," 2007, sec. 7, https://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html.

[18] The White House, 7.

which are the accepted baseline for privacy protection worldwide."[19] More recently *National Strategy for the National Network of Fusion Centers* remarked that all fusion centers will adopt policies for P/CRCL that comply with the Information Sharing Environment Privacy Guidelines. Additionally, "a majority of fusion centers have a designated privacy officer, and many have participated in a compliance verification process to assess how their privacy policy is being implemented and to provide annual training to fusion center personnel."[20]

The P/CRCL problem is widely recognized in the government documents concerning information sharing and IFCs. This problem also concerns many scholars and organizations that have studied the work of FCs and try to reveal problems and violations. One of the well-known issues is noted by Todd Masse and John Rollins, who argue that "[fusion] centers are essentially pre-emptive law enforcement—that intelligence gathered in the absence of a criminal predicate is unlawfully gathered intelligence."[21] They also suggest that the more law enforcement and fusion centers move away from the criminal predicate, the greater the risk of violations toward civil liberties and the potential endangerment of First Amendment protected activities.[22] On the other hand, Dahl suggested that local fusion centers are more easily readjusted and suited to the local requirements and specifics.[23] This means that if there is a problem with a privacy violation, it could be fixed more easily.

Other authors like Monahan and Palmer argue that there is a connection between the expansion of the mission creep in order to meet local communities' needs and liberties violations. They suggest that it is very possible that in order to respond and to adapt to the

---

[19] Global Justice Information Sharing Initiative and DHS's Homeland Security Advisory Council, "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," 2006, 41.

[20] National Fusion Center Association, "National Strategy for the National Network of Fusion Centers 2014–2017 | Public Intelligence," 2015, 19, https://publicintelligence.net/national-fusion-center-strategy-2014-2017/.

[21] Todd Masse and John Rollins, *A Summary of Fusion Centers: Core Issues and Options for Congress,* CRS Report No. RL34177 (Washington, D.C.: Congressional Research Service, September 19, 2007), 4, https://crsreports.congress.gov/product/details?prodcode=RL34177.

[22] Masse and Rollins, 4.

[23] Dahl, "The Localization of Intelligence," 15.

local threat environment, IFCs lend themselves to P/CRCL violations.[24] Other important concerns made by the authors were mainly connected with the "role of third parties and their access to information [and T]he centralization of information and intelligence into single databases."[25] On the other hand, in more recent research, Carter et al. assert that violation of civil liberties is not necessarily connected with an increased rate of threat detection. They suggest that when IFCs implement the correct privacy infrastructure, which includes privacy policy, training personnel on privacy guidelines, and having a privacy review board, it will safeguard the civil rights of individuals while maintaining the high effectiveness of the fusion center.[26]

One of the biggest critics of the IFCs and advocators for preserving the P/CRCL is the Electronic Privacy Information Center (EPIC). In one recent report, EPIC suggested that DHS should consider "whether fusion centers as an enterprise are justifiable in light of the limited intelligence value they produce and magnitude of privacy harms they create."[27] In April 2022, EPIC published another critical report where they identified the "fusion centers as particularly dangerous and wasteful outgrowths of counterterrorism policy that are now being used to investigate domestic terrorism."[28] The main argument they provided was that FCs exist in the space between state and federal regulations, and this position allows them to choose the most tolerant privacy regulations and the least effective oversight practices.[29]

---

[24] Monahan and Palmer, "The Emerging Politics of DHS Fusion Centers," 633.

[25] Monahan and Palmer, 631.

[26] Jeremy G. Carter et al., "Law Enforcement Fusion Centers: Cultivating an Information SharingEnvironment While Safeguarding Privacy," *Journal of Police and Criminal Psychology* 32, no. 1 (March 2017): 24, https://doi.org/10.1007/s11896-016-9199-4.

[27] Jeramie Scott and Jake Wiener, "Comments of the EPIC to the Department of Homeland Security Data Privacy and Integrity Advisory Committee," *EPIC - Electronic Privacy Information Center* (blog), October 2020, 9, https://epic.org/epic-again-urges-dhs-advisory-committee-to-investigate-fusion-centers/.

[28] Alan Butler, Jeramie Scott, and John Davisson, "Comments of the EPIC to the Privacy and Civil Liberties Oversight Board on Notice of Public Forum on Domestic Terrorism," *EPIC - Electronic Privacy Information Center* (blog), April 2022, https://epic.org/documents/epic-comments-agenda-for-pclob-may-2022-meeting-on-domestic-terrorism/.

[29] Butler, Scott, and Davisson, 5.

2. Domestic Violent Extremism

According to the last Homeland Threat Assessment report, the Department of Homeland Security (DHS) in 2020 pointed out that lone-wolf or small groups of extremists are the main terrorist threat in the United States.[30] These extremists are divided into two main categories: domestic violent extremists and homegrown violent extremists (HVEs).[31] Domestic violent extremists are people who use violence to achieve domestic ideological ends, and racial prejudices and anti-government beliefs usually influence these objectives.[32] Homegrown violent extremists are individuals who do not usually receive direct operational guidelines from any foreign terrorist organization, but they have been motivated by foreign terrorist organization ideology.[33] From a security perspective, that difference allows the security services more tools to respond against citizens inspired by a foreign terrorist, but in regard to domestic violent terrorists, that freedom does not exist.

The agencies responsible for preventing domestic terrorist attacks on the U.S. soil are the FBI and DHS. According to Liam McHugh and Tobias Armour "the first challenge…policymakers and leaders must overcome in order to successfully confront the threat of DVE is to define the problem"[34] Even though almost every federal agency has its own definition for "terrorism," DHS, FBI, and Office of the Director of National Intelligence(ODNI) agree to define domestic terrorism as "activities involving acts dangerous to human life that are a violation of the criminal laws of the U.S. or any State; appearing to be intended to: intimidate or coerce a civilian population, influence the policy of the government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination or kidnapping, and occurring primarily within the territorial

[30] Department of Homeland Security, "Homeland Threat Assessment October 2020," October 6, 2020, 17, https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.

[31] Department of Homeland Security, 17.

[32] Department of Homeland Security, 18.

[33] Department of Homeland Security, 17–18.

[34] Liam McHugh and Tobias Armour, "Trends in Domestic Violent Extremism," Lobo Institute, 2021, https://www.loboinstitute.org/trends-in-domestic-violent-extremism/.

jurisdiction of the U.S."[35] The definition for a domestic violent extremist, according to the FBI, is "an individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals wholly or in part through unlawful acts of force or violence."[36] Many scholars and officials have agreed that lack of connections with foreign organizations contributes to the challenges facing the FBI and DHS as they tackle the problem of domestic violent terrorists.

The threat from domestic violent extremists is not a new phenomenon in the United States. According to Robert O'Harrow, Andrew Tran, and Derek Hawkins the deadliest domestic violent extremism attack in U.S. history remains the Oklahoma City bombing in 1995.[37] Over the years the threat has remained active and has continued evolving. According to Muhlhausen and McNeill from the Heritage Foundation's analysis of RAND data, there were ninety-one homegrown terrorist attacks on the U.S. territory between 2001 and 2009.[38] O'Harrow et al. suggest that the right-wing extremists started gathering fresh power after the election of the first African-American president, and after that they concentrated efforts into recruiting members, mobilizing supporters, and spreading ideology through propaganda. They also found that more than 330 plots or attacks have been conducted by right- and left-wing extremists.[39]

Even with the large number of attacks and plots conducted by domestic terrorists and other associated warnings, this threat did not significantly attract the attention of the policymakers until January 6, 2021. Domestic violent extremists and especially right-wing extremist groups became a bigger concern for the domestic security services, after the

---

[35] Federal Bureau of Investigation Department of Homeland Security, "Strategic Intelligence Assessment and Data on Domestic Terrorism," 2021, 3.

[36] Federal Bureau of Investigation Department of Homeland Security, 2.

[37] Robert O'Harrow Jr, Andrew Ba Tran, and Derek Hawkins, "The Rise of Domestic Extremism in America," *Washington Post*, accessed May 26, 2022, https://www.washingtonpost.com/investigations/interactive/2021/domestic-terrorism-data/.

[38] David Muhlhausen, "Terror Trends: 40 Years' Data on International and Domestic Terrorism," The Heritage Foundation, accessed May 26, 2022, https://www.heritage.org/terrorism/report/terror-trends-40-years-data-international-and-domestic-terrorism.

[39] O'Harrow, Tran, and Hawkins, "The Rise of Domestic Extremism in America."

Capitol Breach. An unclassified summary from ODNI identified that the most lethal branches of the domestic violent terrorists are racially or ethnically violent extremists (RMVE) which promote the superiority of the white race and predominantly attack civilians; and militia violent extremists (MVE) who ordinarily attack law enforcement and government personal. According to the summary, the RMVEs are the most persistent and concerning actors due to the shared similarities in ideology internationally and because these actors frequently exchange ideas and influence each other.[40] Department of Homeland Security Secretary Chad Wolf, during his confirmation hearing in 2020, pointed out that among all extremist organizations, "white supremacist extremists, from a lethality standpoint over the last two years, particularly when you look at 2018 and 2019, are certainly the most persistent and lethal threat when we talk about domestic violent extremists"[41]

a. Inspiration of Individuals to Become Domestic Violent Extremists

It is very important to understand why and how the radicalization of individuals occurs in order to build proper measures for countering this process. There is much information in the literature about the radicalization of international terrorists based on religious ideology, but when we talk about lone-wolf and far-right extremists, we need to further our understanding. There are different approaches used to understand domestic violent extremists. There are scholars who choose "top-down" approach, and they are focusing on groups, organizations, and social structural issues. These types of studies aim to reveal how the violent extremist groups disseminate their ideology, how they recruit and radicalize individuals, and the impact these groups experience when they are cut off from access to social media or finance. On the other hand, the opposite approach is "bottom-up." These types of approaches aim to understand how people can be attracted to extremist

[40] The Office of the Director of National Intelligence, "Unclassified Summary of Assessment on Domestic Violent Extremism" (Office of the Director of National Intelligence, March 2021), 2, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2194-unclassified-summary-of-assessment-on-domestic-violent-extremism.

[41] Savannah Behrmann, "Acting DHS Secretary: White Supremacy Is 'Most Persistent and Lethal Threat' Internally to US," *USA Today*, September 23, 2020, https://www.usatoday.com/story/news/politics/2020/09/23/dhs-secretary-white-supremacy-poses-persistent-and-lethal-threat/3511913001/.

activities, and researchers aim to understand what kind of vulnerabilities cause people to have extreme ideas.

The financial flow stimulating the domestic violent extremists is an important issue that concerns security agencies and some scholars. Even though there is insufficient information on how different groups obtain their money, most studies agree that the internet and social media facilitate the process of gathering finances. The Anti-Defamation League (ADL) conducted a study examining white supremacy groups in the United States, which threw light on the digital environment. The study concluded that these kinds of groups are decentralized and not well funded, as they usually rely on crowdfunding, and they use Bitcoin as an alternative to bank cards or wire transfers. The study underlines the importance of social media, online lending platforms, and crypto currencies for white supremacists.[42] The importance of the digital environment was also the subject of a study by Seth Jones. He claims that "right-wing extremists are increasingly using the internet and social media to issue propaganda statements, coordinate training, organize travel to attend protests and other events, raise funds, recruit members, and communicate with others."[43] In a recent study, Timothy Canady provided a similar conclusion. He also recommended to security services that "federal, state, and local law enforcement and intelligence agencies need to continue to monitor social networking and Internet sights to be able to identify those that pose a threat. In addition, monitoring will also reveal possible strategies and tactics which can be countered factual information and the operational development plans to detect, deter and defeat violent extremist."[44]

An extensive study conducted by Allison Smith, with sponsorship from the National Institute of Justice, has used four different research projects to examine radicalization. The examined actors were a wide range of groups and individuals, they were

[42] Anti-Defamation League, "Funding Hate: How White Supremacists Raise Their Money," Anti-Defamation League, 2017, https://www.adl.org/resources/report/funding-hate-how-white-supremacists-raise-their-money.

[43] Seth G Jones, "The Rise of Far-Right Extremism in the United States," Center for Strategic & International Studies, 2018, 3, https://www.csis.org/analysis/rise-far-right-extremism-united-states.

[44] Timothy M. Canady, "Rise of Domestic Violent Extremism and Law Enforcement's Ability to Effectively Investigate Seminar Research Paper," University of Wisconsin-Platteville, May 2021, 44.

either supporters or executers. The results showed that their actions were based on political, social, or religious goals, including "left-wing," "right-wing," and "single-issue" terrorists. Despite the differences in the methods and findings of these four different research-projects, Smith found collective "evidence of the importance of several facilitators of radicalization to terrorism that occur within individuals, in interaction with other individuals, and at the broader community or societal level."[45] Other conclusions from the research were that the radicalization of individuals often includes embracing a terrorist narrative that identifies "the others" as the enemy. The findings also showed that with appropriate measures, this process is reversible. Furthermore, the research indicated that some specific events could trigger personal or political grievances that could push individuals into extremist movements, and sometime any trigger event connected with these grievances could inspire an attack.[46]

Other authors choose to focus their attention on another direction. Instead of answering *why* and *how* the radicalization happens, Cynthia Miller-Idriss tried to understand *where* and *when* the radicalization of far-right and white-supremacist individuals happens. The importance of this approach is to understand where normal people could face far-right extremist ideas in their daily routine before any ideological commitment, and how important are these cultural spaces and places in shaping extremist commitment. In Miller-Idriss's book, she examined this process and found that "over the past several years, a new range of cultural spaces and places cultivating far-right and white-supremacist ideology —not only in the fringes but also within the mainstream—has gradually changed the cultural landscape of the far-right"[47] She asserted that in the cultural mainstream spaces and places such as clothing companies' marketing, veterans' fight

[45] Allison G. Smith, *How Radicalization to Terrorism Occurs in the United States: What Research Sponsored by the National Institute of Justice Tells Us* (Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 2018), 18.

[46] Smith, 18.

[47] Cynthia Miller, *Hate in the Homeland: The New Global Far Right.* (Princeton, NJ: Princeton University Press, 2020), 162, https://muse.jhu.edu/book/77540.

clubs, MMA gyms, and college campuses the radicalization, exposure, and recruitment all happen faster.[48]

b. Disinformation, Misinformation, and Conspiracy Theories as a Fuel for Domestic Violent Extremists

Disinformation and conspiracy theories have become an essential part of the motivation for domestic terrorism. The transition from print media sources to online sources and the emergence of social media provide a significant advantage to extremist groups. In the last several years the literature regarding disinformation and conspiracy theories has enlarged significantly, especially after the presidential election in 2016, where the focus was on foreign state influence. Following the events of January 6, 2021, however, the focus has changed toward RMVEs.

The scholars are aware that disinformation and conspiracy theories play the main role in spreading extremist ideology from all extremist groups. Miller-Idriss argues that the rise of populist parties, the spread of disinformation and conspiracy theories, and the weaponization of youth culture disseminate extremist ideas.[49] In his article, the homeland security expert Charles Allen, and e-CIA official, suggests that "today, domestic threats come from right-wing extremist groups that have fed off rampant conspiracy theories, misinformation campaigns, and a fringe media and internet community that has become self-sustaining and detached from the broader American society."[50] He also suggests that the information campaigns and conspiracy theories, sometimes backed by foreign states such as Russia or other near-peer competitors, have led to the extremist violence experienced in Charlottesville, Va.; Portland, Ore.; and at the U.S. Capitol. Another scholar, Bharath Ganesh, also observes the important role of disinformation in the digital

[48] Miller-Idriss, 162.

[49] Miller-Idriss, 47.

[50] Charles Allen, "State of Terrorism Intelligence: Confronting Foreign and Emergent Domestic Threats," *HSToday*, September 15, 2021, 3.

environment, and he suggests that "digital hate culture is fueling hate crimes and, in more limited cases, terrorist attacks."[51]

There is an important overlapping tendency about the use of disinformation from far-right groups. According to the last threat assessments from the DHS and the IC, far-right groups, especially white supremacists, present the biggest lethal threat to the United States. This first-rank position overlaps with the significant amount of research conclusions about which groups gain the most from disinformation and conspiracy theories. The research from the Cybersecurity for Democracy group, which has studied online misinformation, wanted to know how different types of news sources engaged with their audiences on Facebook.[52] According to the researcher, the accounts with far-right affiliations are much more successful than far-left accounts. Additionally, those far-right accounts that spread misinformation have 65 percent more engagement than other far-right accounts.[53] Miller-Idriss points out that disinformation and conspiracy theories, especially within the far-right, "clearly inspire violence by fringe actors who believe the conspiracy is truth and move from fantasy to direct action and real-life violence."[54]

Although, scholars share a common opinion about the important role of disinformation and conspiracy theories among hate groups, they do not have a consensus opinion about how law enforcement could contain the spread of disinformation that sparks violence. Some scholars believe that censorship is an appropriate way to decrease violent extremism, and they emphasize the example of fighting against ISIS propaganda on social media. According to Ganesh, what is needed is a global discussion on free speech and an effort toward reconsidering the censorship of digital hate culture.[55] He also suggested that "rather than focus on content moderation, governments, technology companies, and civil

---

[51] Bharath Ganesh, "The Ungovernability of Digital Hate Culture," Journal of International Affairs 71, no. 2 (Spring/Summer 2018): 42.

[52] Laura Edelson et al., "Far-Right News Sources on Facebook More Engaging," Medium, *Cybersecurity for Democracy* (blog), March 4, 2021, https://medium.com/cybersecurity-for-democracy/far-right-news-sources-on-facebook-more-engaging-e04a01efae90.

[53] Cybersecurity for Democracy.

[54] Miller-Idriss, *Hate in the Homeland: The New Global Far Right.*, 61.

[55] Ganesh, "The Ungovernability of Digital Hate Culture," 43.

society should cooperate to focus on disrupting individuals, accounts, and movements that use emotive messaging and extreme worldviews."[56] On the other hand, Allen's approach is toward the role of the IC. He suggested that "the IC needs to focus on the monitoring of social media and other channels for evidence of planned attacks as well as longer-term investigations of extremist groups…. federal law enforcement and intelligence agencies must also build stronger relationships with state and local authorities to help address domestic extremism…. especially through the operation of fusion centers [which] are better positioned to know which groups pose the greatest threat and conduct investigations into organizations focused in a narrow geographic area."[57]

Another moderate approach comes from the Combatting Targeted Disinformation Campaigns team, which includes public and private members. Their paper was based on the opinion of subject matter experts and open-source material. The approach that they recommended would impact both supply and demand. They believe that disinformation cannot be fully stopped, but it could be managed by building the resilience of information consumers to disinformation.[58] They suggested that that resilience could be built by "giving information consumers more tools with which they can verify the information they consume online, identify the threat actors behind disinformation campaigns, verify the claims of imposters hiding behind fake persona and credentials, and control their content feeds is essential."[59]

D. RESEARCH DESIGN

This thesis analyzes how state and local intelligence fusion centers can better address the problem of domestic violent extremism. In order to do that, this thesis explores three main topics: Intelligence Fusion Centers, Domestic Violent Extremism, and Disinformation and Conspiracy Theories as fuel for violent extremists' propaganda. The

---

[56] Ganesh, 44.

[57] Allen, "State of Terrorism Intelligence: Confronting Foreign and Emergent Domestic Threats," 3.

[58] The Public-Private Analytic Exchange Program, *Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue Part Two* (Washington, DC: Department of Homeland Security, 2021), 43, https://publicintelligence.net/dhs-combatting-disinformation-2021/.

[59] The Public-Private Analytic Exchange Program, 43.

examination of these topics focuses on intersection points between them. This thesis uses mainly historical analysis, applying qualitative and quantitative methods to answer the research question. It relies on scholarly research, government documents and strategies, official testimonies, and newspaper and magazine articles to build a clear understanding about the role of the fusion centers and threat coming from DVE.

The emergence of the DVE in the United States is a recent phenomenon but in the past decade, there have been a significant number of attacks that have happened on the U.S. territory. Examining domestic violent extremists' attacks and events provides an understanding of what kind of problems IFCs have, what could have been done to prevent such attacks, and how to improve the work of the IFCs. This thesis seeks also patterns and vulnerabilities in multiple examples of successful attacks on domestic violent extremists. The disinformation and conspiracy theories are the tissue that connects the majority of domestic violent extremists and hate groups. Understanding how violent extremists think, how they feed their grievances, and, most importantly, how to disrupt this process is important for fighting against DVE. To answer these questions, this research looks for answers in several domestic case studies and searches for similarities and opportunities for taking part in this fight with the use of IFCs. It shows that this is simultaneously a federal phenomenon, but also a local problem that state and local intelligence fusion centers could take part in against tackling this threat.

E. CHAPTER OVERVIEW

This thesis comprises five chapters. The first chapter presents general problems that IFCs have faced and information about DVE as a new threat to U.S. homeland security. The first chapter introduces the problem. The introduction aims to see what the other scholars think about these problems and what gaps exist. Chapter II discusses how IFCs work and their role in protecting local communities. This chapter provides information about the differences between domestic and foreign intelligence and the historical background of creating the first domestic intelligence agency. It also discusses the main challenges in front of IFCs and how to improve their role in the security infrastructure. Chapter III presents an overview of far-right ideology in the United States and examines

case studies about the Capitol insurrection on January 6. This chapter focuses on far-right case studies because these groups are very active, and they present one of the biggest threats to homeland security. Chapter IV examines the importance of spreading disinformation and conspiracy theories for far-right movements and how the disinformation works. It also examines the role of the federal security services and IFCs in countering far-right disinformation campaigns. To do that, the chapter examines the election interference in 2016 and what measures had been taken during the 2020 elections. Chapter V concludes the state and local fusion centers' role against the far-right threat. It also provides recommendations on how IFCs can better address domestic violent extremism and highlights gaps that this thesis does not address for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. ORIGINS AND CHALLENGES OF THE STATE AND LOCAL IFC

The fusion of information is a concept that had proven itself successful in military operations and against domestic threats years before 9/11. More recently, trans-national threats such as terrorism and organized crime drove the creation of a system of intelligence fusion centers (IFCs), which allow better information sharing and better prevention of such threats. This chapter reviews the basic historical steps in the development of IFCs and how they have changed from strictly counterterrorism efforts to all-hazards fusion centers. The chapter also provides insight into the main challenges facing fusion centers and what must be done to ensure their success.

A. UNDERSTANDING INTELLIGENCE

The word "intelligence" usually is associated by regular people with international scandals or with violations of civil liberties. Talking generally about intelligence introduces difficulties and usually imposes doubts in the mind of the regular reader because he or she not understanding what we mean with this term. On the other hand, intelligence could be seen only as a process for gathering and analyzing information about certain national security topics. Intelligence has a variable definition, and very often, each intelligence service has its own definition due to its particular specifics and areas of service. One possible explanation for these variations comes from Bimfort, who suggests that "each expert tends to view the term through the spectacles of his specialty."[60] Distinct definitions are important for the services and those who work in them because the definitions provide a legal framework for certain intelligence services; therefore, each service should have a definition that is best suited to the tasks the service must perform.

1. Defining Intelligence

One of the most comprehensive and very often cited definitions of intelligence comes from Mark Lowenthal. He sees intelligence in three ways: a process, a product, and

[60] Martin T. Bimfort, "A Definition of Intelligence," CIA Historical Review Program, 1994, 1.

an organization; sometimes, these three dimensions are combined altogether.[61] Intelligence as a process means the activities in that specific information is "required and requested, collected, analyzed, and disseminated and as the way in which certain types of covert action are conceived and conducted."[62] When we think of intelligence as a product, it refers to the results from the intelligence process. Lastly, when we think of intelligence as an organization, it refers to the units that conduct all these functions.[63]

Regular people's understandings about intelligence is very often limited. The primary division line about the understanding of intelligence depends on whether the term has IC or law enforcement origins, and whether it was developed before or after the events of 9/11. According to Lowenthal, most people conceive intelligence as a piece of military information, such as troops' movement, weapons capabilities, or plans for mission execution.[64] In the context of law enforcement, Taylor at al. suggests that "intelligence" is information "significant or relevant to an impending event and that will be a contribution to the positive outcome of that specific incident."[65] The focal point for the beginning of changing perceptions of intelligence was 9/11. Since then, we can assume that the Cold War style of thinking about intelligence started to change. After 9/11, people have become more affected by intelligence activities because the Patriot Act provided greater freedom and capabilities to the intelligence services to collect information domestically on American citizens connected with terrorist organizations or terrorists. This law significantly changed the Americans' perceptions for intelligence because now the intelligence services received more legal rights to collect information.

The second important law that changed the understanding of national intelligence is the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. According to the Act, national intelligence is "all intelligence, regardless of the source from which

---

[61] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2022), 9.

[62] Lowenthal, 9.

[63] Lowenthal, 9.

[64] Lowenthal, 6.

[65] Robert W. Taylor and Jennifer Elaine Davis, "Intelligence-Led Policing and Fusion Centers," in *Critical Issues in Policing: Contemporary Readings*, 6th ed. (Long Grove, IL: Waveland Press, 2010), 225.

derived and including information gathered within or outside the United States."[66] According to Lowenthal, the purpose of combining foreign and domestic intelligence was to overcome the past division between them, which was conceived as the main obstacle to information sharing, especially on problems that overlap both branches, like terrorism.[67] Breaking the mental model of "secrecy" and "stove piping" in intelligence services was very important for countering terrorism. Uniting domestic and foreign intelligence in one term as "national intelligence" provides a legal reason for separate intelligence services to share information more freely due to the perception that by sharing information with other services, your service contributes to national intelligence.

The IFCs are an essential segment in the complete spectrum of national intelligence. According to DHS Intelligence and Analysis Strategic Plan, there are three types of intelligence—anticipatory, strategic, and operational.[68] According to the document, "anticipatory Intelligence addresses new and emerging trends, changing conditions, and underappreciated developments. Strategic Intelligence addresses issues of enduring national security. Operational intelligence supports planned and ongoing operations."[69] The IFCs play a major role in operational intelligence, but they also support the other two types of intelligence. For example, with the contribution for anticipatory intelligence, the state and local fusion centers are in the best position to analyze and provide information regarding recorded trends or to alert local communities about emerging threats because their focus is toward said local communities. These centers are best aware about the problems of the state, and they can provide the most accurate information about the changing conditions in their area of operation. In terms of strategic intelligence, the IFCs

66 Peter Hoekstra et al., "Intelligence Reform and Terrorism Prevention Act of 2004," Conference Report (Washington, D.C.: House of Representative, 2004), 29, https://books.google.bg/books?id=NC1heYaq9NMC&printsec=frontcover&dq=intelligence+reform+and+terrorism+prevention+act&hl=bg&sa=X&redir_esc=y#v=onepage&q=intelligence%20reform%20and%20terrorism%20prevention%20act&f=false.

67 Lowenthal, *Intelligence: From Secrets to Policy*, 5.

68 "The Office of Intelligence and Analysis FY 2020–2024 Strategic Plan – Homeland Security," 6, accessed July 18, 2022, https://www.dhs.gov/publication/office-intelligence-and-analysis-fy-2020-2024-strategic-plan.

69 "The Office of Intelligence and Analysis FY 2020–2024 Strategic Plan – Homeland Security," 6.

provide opportunities to produce comprehensive assessments in the era of terrorist threat and transnational organized crime.

2. The Intelligence Cycle

The intelligence cycle was originally implemented in the U.S. IC in 1947, and it was intended to "provide essential information to the president, policymakers, federal organizations, and military communities."[70] Today the political situation and threat environment is very different, and this led to an expansion of the IC beyond the federal level. This expansion includes state, local, tribal, nongovernmental, and private sector entities with the purpose to strengthen domestic intelligence capabilities.[71]

The intelligence cycle is a process by which the different intelligence services produce and disseminate intelligence. The DNI defines the intelligence cycle as "a process of collecting information and developing it into intelligence for use by IC customers. The steps in the process are direction, collection, processing, exploitation, and dissemination."[72] Each intelligence agency determines the steps in its particular cycle. According to Stocks, the range of the steps in the different IC services varies from four to seven.[73] The intelligence cycle in terms of law enforcement and criminal intelligence is "the process of developing raw information into finished intelligence for consumers, including policymakers, law enforcement executives, investigators, and patrol officers. These consumers use this finished intelligence for decision-making and action. Intelligence may be used, for example, to further an ongoing investigation, or to plan the allocation of resources."[74]

---

[70] Roger L. Stokes, "Employing the Intelligence Cycle Process Model Within The Homeland Security Enterprise" (master's thesis, Naval Postgraduate School, 2013), 4.

[71] Stokes, 4.

[72] "What Is Intelligence?" Office of the Director of National Intelligence, accessed July 15, 2022, https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

[73] Stokes, "Employing the Intelligence Cycle Process Model Within The Homeland Security Enterprise," 7.

[74] "The Intelligence Production Cycle," Iowa Department of Public Safety, accessed July 17, 2022, https://dps.iowa.gov/divisions/intelligence/intel-cycle.

Intelligence fusion centers employ a version of the intelligence cycle called the Intelligence Process, which outlines the standards and capabilities necessary for fusion centers to perform correctly.[75] The Fusion Process Capabilities are as follows:

- Planning and Requirements Development—during this step, the centers' leadership should decide what information to collect or what they want to understand.

- Information Collection and Recognition of Indicators and Warnings—during this step, raw information is gathered from many sources, including open sources and confidential sources.

- Processing and Collation of Information—this step includes validation and appreciation of reliability. After that, the information is sorted, combined, categorized, and arranged so relationships can be determined.

- Intelligence Analysis and Production—this step converts the gathered material into real intelligence. The end state of this step is to develop an intelligence report which includes logical conclusions based on information that is possessed.

- Intelligence/Information Dissemination—it must be timely and credible. It also must be executed based on the "right to know" rule.

- Reevaluation—identify previously identified flaws in the fusion process, identify potential weak spots and threats, and review existing and new information.[76]

From a military or traditional IC perspective, the intelligence cycle is intended to resolve military and national policymaker information gaps. This is also called the "top-

[75] Global Justice Information Sharing Initiative, *Baseline Capabilities for State and Major Urban Area Fusion Centers*, (Washington, DC: U.S. Department of Justice, 2008), 9, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf.

[76] Global Justice Information Sharing Initiative, 9.

down" approach.[77] This means that top-level military or national leaders request information about foreign capabilities or threats from the intelligence services, and through the implementation of the intelligence cycle, the intelligence services provide the requested information. The opposite approach is "bottom-up," and it provides "state and local decision-makers, public safety officials and the private sector the ability to influence and shape national interest through fusion centers operating within the National Network at the state and local level."[78] It is necessary for IFCs to implement both approaches in their fusion cycles because they are multi-threat oriented. IFCs must train and maintain two types of approaches in order to adequately address contemporary threats such as domestic violent extremists, which is a threat that has purely domestic roots, and to continue facilitating counterterrorism efforts, which involve foreign influence.

B. DEVELOPMENT OF FUSION CENTERS BEFORE 9/11

Fusion of information is a concept with a long history starting with WWII, and this section reviews the development of fusion centers leading up to the 9/11 attacks. "A relatively stable threat environment,"[79] throughout The Cold War, coming primarily from foreign state actors and an intelligence culture conscious of the need for secrecy, defined the slow implementation of the fusion concept in domestic intelligence. After the Cold War, the threat environment began significantly changing, but the Intelligence Community had difficulties adapting to the new challenges. The benefits of fusion centers slowly began to become visible to decision makers, the military and law enforcement's efforts and experience with intelligence gathering began to naturally develop the first domestic fusion centers.

[77] Stokes, "Employing the Intelligence Cycle Process Model Within The Homeland Security Enterprise," 71.

[78] Stokes, 72.

[79] James Thomson, *Conflict and Cooperation in Intelligence and Security Organisations: An Institutional Costs Approach*, 1st ed. (London: Routledge, 2021), 198, https://doi.org/10.4324/9781003107231.

1. The Military Experience

The beginning of the fusion center concept started during WWII, and it happened very similarly to the creation of a contemporary network of IFCs after 9/11. The first military fusion center was called the Joint Intelligence Center (JIC), created in Pearl Harbor, Hawaii, after the proposal by the Commandant of the U.S. Marine Corps.[80] One of the motives for creating this center was the intelligence failure with the Pearl Harbor attack. According to Dahl, the Japanese attack happened because "sufficient intelligence indicators had been available, but they were misunderstood or ignored as a result of faulty analysis."[81] The faulty analysis was a result of fragmented national intelligence, which at that point produced products without coordination. This lack of coordination and capabilities to "connect the dots," similar to 9/11, led military officials to undertake the reform in military intelligence.

Another reason for creating the JIC was the need for cooperation with different services due to the complicated character of war. It was complicated because the U.S. military had to conduct operations simultaneously in multiple theaters. According to Marchio, "the conduct of the war in the Pacific and Europe during 1943 and 1944 drove the push for joint intelligence. As U.S. military forces transitioned from largely defensive to multiservice offensive operations, it became clear that extensive interservice cooperation was required."[82] Marchio also suggests that the JIC was the result of the increasing number of new intelligence sources, which led to new problems such as duplication, delays or inappropriate dissemination, and competition over collection resources.[83] The creation of the first fusion center in U.S. intelligence was the solution to the complicated situation management and intelligence coordination processes necessary in multiple offensive operations. After all, the Pearl Harbor attack exposed the flaws of military intelligence, and

---

[80] James D. Marchio, "The Evolution and Relevance of Joint Intelligence Centers," *Studies in Intelligence* 49, no.1 (March 2005): 2, https://www.cia.gov/resources/csi/studies-in-intelligence/volume-49-no-1/the-evolution-and-relevance-of-joint-intelligence-centers/.

[81] Erik J. Dahl, *Intelligence and Surprise Attack : Failure and Success from Pearl Harbor to 9/11 and Beyond.* (Washington, DC: Georgetown University Press, 2013), 46.

[82] Marchio, "The Evolution and Relevance of Joint Intelligence Centers," 2.

[83] Marchio, 2.

senior military leaders had to make reforms. Still, the real reason is that the characteristics of war have changed, and the JIC was a good solution for better coordination and maximizing the U.S. military intelligence.

2. Law Enforcement Fusion Efforts

The major cause for creating a network of IFCs after 9/11 was countering terrorism, however, one of the first successful models of law enforcement intelligence fusion centers was focused on countering drug proliferation. The idea for creating such a fusion center was because "[they] have been one of the key instruments used by the U.S. government to adopt a more networked approach to national security."[84] According to Puyvelde, fusion centers provide the necessary coordination to fight against transnational criminals, who take advantage of the limitations of government authorities in regards to jurisdictions and borders.[85] Indeed, most of the first intelligence fusion centers were developed around the High-Intensity Drug Trafficking Area Center's model, which served as an example of a successful structure.[86]

The first domestic fusion center was established in 1974 and is called the El Paso Intelligence Center (EPIC). This fusion center is a result of the U.S. Department of Justice study about the problems involving the U.S.–Mexican border, and it is considered as the first successful attempt to create law enforcement interagency operability.[87] The EPIC aims to provide strategic, operational, and tactical information needed for interdiction of narcotics, weapons trafficking, and smuggling along the Southwest border.[88] The EPIC is a successful model of a fusion center oriented toward a specific threat. Over the years,

---

[84] Damien Van Puyvelde, "Fusing Drug Enforcement: A Study of the El Paso Intelligence Center," *Intelligence and National Security* 31, no. 6 (September 18, 2016): 889, https://doi.org/10.1080/02684527.2015.1100373.

[85] Van Puyvelde, 889.

[86] David L. Carter and Jeremy G. Carter, "The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement," *Criminal Justice and Behavior* 36, no. 12 (December 1, 2009): 1324, https://doi.org/10.1177/0093854809345674.

[87] DEA Museum, "An Overview of the El Paso Intelligence Center," DEA Museum, 2011, https://museum.dea.gov/video-archive/el-paso-intelligence-center.

[88] Van Puyvelde, "Fusing Drug Enforcement," 890.

EPIC has enlarged organizationally due to the widening of its scope from the Southwest border to the Western hemisphere. This center is considered as a successful example and model for the future centers under the initiative of DHS.[89] Using the model of EPIC as an example of a counterterrorism center has its reasons. There are many similarities between international drug trafficking organizations and terrorist threats. These similarities make EPIC a successful model for the DHS and the DOJ to use if they choose to create new state and local fusion centers.

While the EPIC naturally transformed from an anti-drug to an all-threat intelligence center, the Terrorism Early Warning Group (TEWG) was created for the first time specifically for counterterrorism intelligence. The TEWG concept was originally created in Los Angeles in 1996, and according to Sullivan and Lester, it is "a way to bridge the gaps in traditional intelligence and security structures."[90] The main idea behind this center was to support strategic and tactical users through the creation of connections between criminal and operational intelligence.[91] The TEWG's goal was to anticipate, prevent, disrupt, or mitigate the consequences of any possible terrorist attack. In order to do that, it is necessary for different agencies to participate in collaborative efforts to produce intelligence, which is called the co-production of intelligence.[92] Contemporary IFCs conduct exactly that. By collaborative efforts from different agencies and partners, they provide a better understanding of specific threats. Without such collaboration, a complete understanding of a particular threat would be much harder.

The combination of the law enforcement and military's experience is the base of the creation of the current contemporary state fusion centers. This combination is expressed by a collaboration of operational and criminal intelligence in one center. Criminal intelligence is connected more with law enforcement, and it is intended for criminal suppression and prosecution. On the other hand, operational intelligence is more connected

89 Van Puyvelde, 892.

90 John Sullivan and Genevieve Lester, "Revisiting Domestic Intelligence," *Journal of Strategic Security* 15, no. 1 (April 2022): 88, https://doi.org/10.5038/1944-0472.15.1.1976.

91 Sullivan and Lester, 88.

92 Sullivan and Lester, 88.

with military experience. It aims to "understand the current and future situation, including the capabilities and intentions of an adversary in order to conduct operational missions at all phases of response."[93] The blending of both types of experience increases the intelligence capabilities of the centers and provides a better foundation for success in supporting security providers.

C. BUILDING FUSION CENTERS AFTER 9/11

Since 9/11, the IC in the United States has changed significantly. There were many debates about how this catastrophe happened and the role of intelligence could have played in preventing such attacks. Many officials have concluded that one of the biggest reasons for the success of this terrorist attack was the absence of communication between the intelligence services. This conclusion led to the creation of multiple state and local intelligence fusion centers, which had to support intelligence sharing from federal and state services and provide new capabilities to the local law enforcement to fight against terrorism.

Similarly, like the creation of JIC after the Pearl Harbor attack, other factors initially pushed for conceiving the idea of an information-sharing environment. According to Rollins, beyond the effects of the 9/11 attack, there were also other important impacts such as "the increasing favor of the Intelligence-Led Policing model."[94] He also suggests that the success of the High-Intensity Drug Trafficking Area (HIDTA) center's structure and the agreement amongst Governors that each state should have a fusion center established the favorable foundation for developing the network of IFCs.[95] The initial understanding of the necessity of structures like fusion centers was present before 9/11. This development was a logical step considering the evolving threat conditions after the Cold War. The tragedy of 9/11 gave more freedom to the U.S. authorities to conduct big reforms, but the ideas were already present. This reveals that the creation of IFCs was not

[93] A. Bauer et al., *Terrorism Early Warning: 10 Years of Achievement in Fighting Terrorism and Crime* (Los Angeles, CA: Los Angeles California County Sheriff's Department, 2008), 108, https://books.google.com/books?id=pWU6mwEACAAJ.

[94] Masse and Rollins, "Fusion Centers: Issues and Options for Congress," 15.

[95] Masse and Rollins, 15.

unreasonable or an impulse decision, but it was an act driven by the necessity for a better security system. The IFCs are a very important element of the information sharing environment, and their role in homeland security is essential.

1. Creation of the Fusion Center Network

The final idea for establishing an IFC network began several weeks after 9/11, and it emerged from the need to implement intelligence-led policing (ILP). The beginning of the idea started in an annual meeting of the International Association of Chiefs of Police, where it was discussed how to redesign state, local, and tribal law enforcement intelligence capabilities.[96] According to Carla Lewandowski and Ray Guidetti, in order to adopt ILP, law enforcement "need [s] to develop an information collection framework as well as an organizational infrastructure to support ILP."[97] Basically, this organizational infrastructure presents organized IFCs which provide the necessary environment in which ILP efforts function properly.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) started the program of contemporary IFCs. This document addressed the conclusions and recommendations of the 9/11 Commission, and it said that "the biggest impediment to a greater likelihood of 'connecting the dots' was the resistance to information sharing, and recommended a new, government-wide approach to information sharing."[98] It also required the U.S. president to establish an Information Sharing Environment(ISE) in order to "facilitate the sharing of terrorism information among all appropriate Federal, State, local, tribal and private sector entities, through the use of policy guidelines and technologies."[99] The ISE "consists of the people, projects, systems, and agencies that

[96] Lewandowski and Guidetti, "The Role of Fusion Centers in Homeland Security," 178.

[97] Lewandowski and Guidetti, 178.

[98] Susan M. Collins, "Summary of Intelligence Reform and Terrorism Prevention Act," Summary (United States Senate Committee of Government Affairs, 2004), 6.

[99] Collins, 6.

enable responsible information sharing across the national security enterprise,"[100] and the IFC network is the backbone of this environment, along with 36 other partners.

The next important step in developing the IFC network was establishing standards. These standards for IFCs are the results of a joint work of the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) and the DHS's Homeland Security Advisory Council. These two organizations "collaborated with numerous law enforcement experts and practitioners from local, state, tribal, and federal agencies, as well as representatives of public safety and private sector entities across the country."[101] This work was intended to provide guidelines for developing similar capabilities and information-sharing processes. The result of their work was the creation of "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," in 2008, which addressed the problems involved in standardization. According to Lewandowski and Guidetti, this document provides "guidance to the personnel of fusion centers for how to develop policies, manage resources and establish an information-sharing environment."[102] The creation of the guidelines in 2008 is an important document for developing the network of fusion centers because, until then, there was no clear framework for its establishment. After issuing this document, we can assume that fusion centers finally have the first level of standardization necessary to be recognized as one system. On the other hand, this standardization was not overly specified, allowing sufficient flexibility for the fusion centers.

2. Evolution of Fusion Centers

Broadening the mission's scope of the networked fusion centers is the main characteristic of the evolution of the fusion centers. After 9/11, the main intention of the centers was to share information to facilitate counterterrorism, but soon after that they

100 "About the Information Sharing Environment," Office of the Director of National Intelligence, accessed May 7, 2022, https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise.

101 Global Justice Information Sharing Initiative, "Fusion Center Foundational Guidance on Homeland Security," U.S. Department of Homeland Security, accessed May 18, 2022, https://www.dhs.gov/fusion-center-foundational-guidance.

102 Lewandowski and Guidetti, "The Role of Fusion Centers in Homeland Security," 179.

started to reorient and to adapt to the needs of the local security services. According to Lewandowski and Guidetti, most of the fusion centers have become all-crime or all-hazards oriented due to meeting their stakeholders' requirements.[103] The adaptation process was led by demand, which differed from the fusion centers' productions. When we talk about all-crime centers, we must know that they also have different priorities. Some of them are focused on any crime, large or small, but some of them support only larger criminal cases.[104] On the other hand, all-hazards centers seek "to act as a force multiplier and support structure for existing Emergency Operations Centers, which remain responsible for coordinating the response to large-scale incidents and disasters."[105] The all-hazard approach originally emerged from the Federal Emergency Management Agency, but in 2003 it was promoted as the preferred approach for homeland security agencies, which includes preparedness for domestic terrorist attacks, major disasters, and other emergencies.[106]

The expansion of the mission scope is a good indicator that the IFCs are adaptive structures that react to the environment around them. According to Rollins, three factors initiated this evolution: "Appearance of a national trend, need for local and non-law enforcement buy-in, and need for resources."[107] He found that some of the leaders of the fusion centers followed the trend in the states, which was going in all-hazard or all-crime oriented models. Other leaders, however, have adapted to the needs of the local security services due to most of the local problems being connected with gangs, narcotics, and street crime.[108] According to him, the third factor behind the adoption of adaptive structures stemmed from operational finance concerns. According to the last National Network of

[103] Lewandowski and Guidetti, 179.

[104] Masse and Rollins, "Fusion Centers: Issues and Options for Congress," 22.

[105] Masse and Rollins, 23.

[106] Masse and Rollins, 22.

[107] Masse and Rollins, 21.

[108] Masse and Rollins, 21.

Fusion Centers Final Report, 37 percent of the operational cost is paid by state funds,[109] which it additionally explains that fusion centers are willing to expand their mission in order to satisfy their biggest financial provider - the state. This evolution of fusion centers could be analyzed as a positive feature necessary for a contemporary intelligence structure. In order to meet the challenges of contemporary threats, fusion centers have to have the freedom to improve and to be able to adjust their capabilities in order to maximize the effects of their products. When fusion centers can orient their product towards the preferences of the local's needs, they will be more able to adequately adjust to the needs of the specific area of operation.

The Fusion Center Liaison Officer (FLO) program is another step in their evolution, as it provides an increase in the fusion centers' productivity. The FLO are utilized to provide the necessary flow of information needed between the fusion center and local and federal services.[110] According to JP Burt from the Colorado Information Analysis Center, the liaison officers are the most important tool of the fusion centers. Consisting of people from all kinds of services, this liaison network is the most robust information network which provides the best information collectors because the liaisons come from the local communities where they understand what the threat is.[111] Carter et al. also suggest that IFC will be effective if two-way information sharing mechanisms improve, and the best way to do that is by adopting the FLO program, which will improve local law enforcement connections.[112] The IFCs need to maintain connectivity with different partners such as law enforcement, health services, fire stations, and other public and private partners. Maintaining and training liaison officers provides increased effectiveness and connection between the different services in the information-sharing environment.

---

[109] Departmnet of Homeland Security, "National Network of Fusion Centers Final Report," 2018, 2, https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf.

[110] Lewandowski and Guidetti, "The Role of Fusion Centers in Homeland Security," 9.

[111] "Fusion Center Liaison Officer (FLO) Programs," National Fusion Center Association, video, 8:54, accessed July 27, 2022, https://nfcausa.org/video/.

[112] Carter et al., "Law Enforcement Fusion Centers," 24.

The liaison officer program provides flexibility and a less expensive way to maintain a reliable connection with fusion centers' partners. Lewandowski and Nestel found that personal contact is the most frequent way of seeking information, and budget cuts made it more difficult to participate in the inter-department meetings to build professional networks.[113] Training and maintaining at least one person to facilitate the information-sharing process is necessary. According to Stone, depending on the geographic region or the specifics of the agency the number of the liaisons can vary.[114] He also suggests that "[a]n agency's involvement in the liaison officer program is much less resource-intensive than dedicating personnel directly to a fusion center but provides significant benefits to both the fusion center and participating agencies."[115] The main goal of the liaisons is to connect their agency with the IFCs network. This is a very simple and easy method to maintain a reliable connection with the partners of the IFC. This connection provides relevant information in both directions and benefits the IFC and the agencies that share information with IFCs. As Lewandowski et al. suggest, "local police departments may be able to survive without sharing information with other departments, but they will not be able to thrive."[116]

3. The Intelligence Fusion Centers Today

More than 21 years after 9/11 there are 80 IFCs, divided into 54 primary and 26 recognized fusion centers.[117] The Primary Fusion Centers, also known as state fusion centers, normally provide information sharing and analysis for the whole state. These centers typically "are the highest priority for the allocation of available federal resources, including the deployment of personnel and connectivity with federal data systems."[118] The

---

113 Carla Lewandowski and Thomas J. Nestel, "Police Communication at the Local Level: An Exploratory Study," *Journal of Policing, Intelligence and Counter Terrorism* 11, no. 1 (January 2, 2016): 54, https://doi.org/10.1080/18335330.2016.1161224.

114 Kelley Edmonds Stone, "Creating an Information Sharing and Analysis Center: A Case Study of The North Central Texas Fusion Center," (PhD diss., University of Texas - Dallas, 2014), 46.

115 Stone, 46.

116 Lewandowski and Nestel, "Police Communication at the Local Level," 61.

117 "Fusion Center Locations and Contact Information – Homeland Security."

118 "Fusion Center Locations and Contact Information – Homeland Security."

second type of centers are Recognized Fusion Centers. They usually deliver "information sharing and analysis for a major urban area.".[119] Before 9/11, there were fusion centers, but they were focused only on specific regions, or they had specific tasks. The big change after 9/11 was developing the state fusion centers whose main idea was to provide local communities with federal information. This connectivity is an important condition for the further development of intelligence-led policing. This connectivity will benefit both state and federal intelligence services because now fusion centers can add a different perspective to federal intelligence by fusing "a broader range of data, including nontraditional source data, to create a more comprehensive threat picture"[120]

D. CHALLENGES

The challenges in front of the state and local fusion centers are many. Since their creation and development, these challenges have been forming the future of the centers' information sharing and analytical capabilities. Struggles like effectiveness, privacy issues, and budgeting are the main problems that fusion centers have to encounter. Fusion centers have even harder struggles with social digitalization and the social media revolution. Technology developments available to the population often outpaces intelligence services existing strategies, and this allows criminal groups and terrorist groups to outmaneuver the security services. According to Zegart, now the threat environment is different than 2001, and new technologies supercharge these threats through the acceleration of information sharing on a huge scale, and this make intelligence much more important and challenging.[121] Using social media and forms of free encrypted communication allows these criminal individuals relative freedom, and it has started challenging fusion centers to collect and analyze intelligence without violating civil liberties.

To summarize the fusion centers' challenges, we can divide them into two main categories. The first category is how to build and maintain trust in the fusion centers'

119 "Fusion Center Locations and Contact Information – Homeland Security."

120 Masse and Rollins, "Fusion Centers: Issues and Options for Congress," 3.

121 Amy Zegart, "In the Deepfake Era, Counterterrorism Is Harder," *The Atlantic*, September 11, 2019, https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/.

partners. The second, is how to work effectively while simultaneously maintaining the trust of U.S. citizens.

1. Building Trust between the IFCs and Their Partners

Building trust between the IFCs and their partner organizations is a continuing process that depends on the IFCs maintaining proper communication with their partners and the effectiveness of the IFCs. The main role of the IFCs is to be a hub for information and analysis between other agencies. According to Lewandowski and Guidetti, "to become the true analytical centers…[IFCs] need better to communicate their resources and abilities to the stakeholders as well as communicate their information needs to local agencies."[122] According to Cooney et al. who made a study about the South Carolina Intelligence and Information Center, "without a high degree of communication, the flow of information and intelligence between these centers and the agencies they serve will be minimal, which will result in the fusion center concept becoming a very expensive initiative that falls short of its intended purpose."[123] Increasing communication with the security agencies is extremely important for building trust in fusion centers. If the IFCs do not communicate properly, the chances for sharing information significantly decrease, which undermines the main purpose of the fusion centers.

Maintaining good communication with the fusion centers' partners also depends on what concept of investigation they have adopted. For example, Cooney's findings suggest that partners of the South Carolina Intelligence and Information Center "who placed a high priority on ILP were more likely to provide a very useful rating of the center…[and] those who had used the center's services in the past year or who had attended training on the fusion center's operations and services were more likely to provide a very useful rating of the center compared to those who did not."[124] With these results in mind, we can conclude that building trust between fusion centers and their partners could be improved if fusion

[122] Lewandowski and Guidetti, "The Role of Fusion Centers in Homeland Security," 190.

[123] Cooney, Rojek, and Kaminski, "An Assessment of the Utility of a State Fusion Center by Law Enforcement Executives and Personnel," 13.

[124] Cooney, Rojek, and Kaminski, 14.

centers focused more on the training of law enforcements and other partners. In particular, education on how to use the services of the fusion centers and promoting ILP as a concept for policing among agencies that do not currently use it could greatly improve trust building efforts.

It will be challenging, however, to build trust between IFC and their partners with the current budget spending for training and exercises. The budget spendings from the last public reports show that training is not a priority for the fusion centers (see Figure 1).

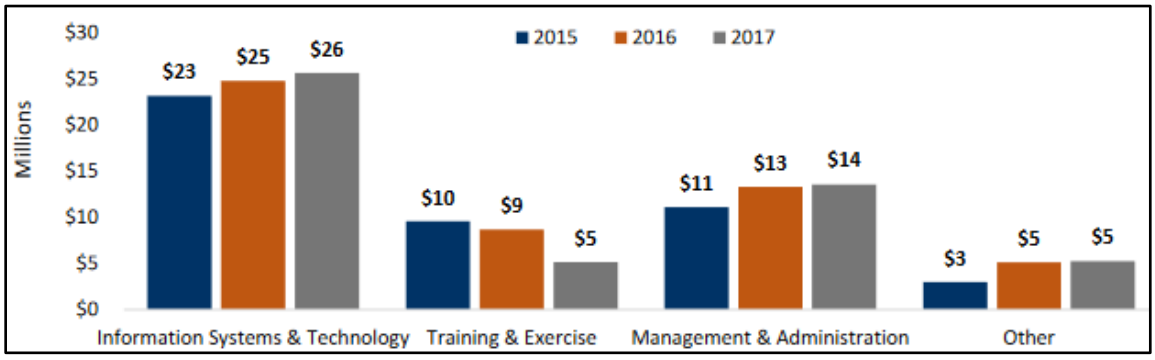

Figure 1. Non-staff spending (2015–2017).[125]

Figure 1 represents non-staff spending of the annual fusion centers' budget. The result shows that there is a tendency for non-staff spending, and the tendency is to spend less money on training. For 2017, the budget for training and exercise was 50 percent lower compared with 2015, which shows that fusion centers' executives focused their efforts in other directions. The lowering training and exercise budget negatively affects the fusion centers' ability for collaboration and hampers approval from their partners, and this decreases the trust between fusion centers and their partners. A good example is the Final Report from 2018, where a Key Stakeholder Survey shows a decrease in customer satisfaction from 83 percent in 2016 to 77 percent in 2018.[126] Additionally, it is noticeable from the 2017 report that there are also "decreases in participation from key disciplines,

[125] Source: "2017 National Network of Fusion Centers Final Report," 2017, 16.

[126] Department of Homeland Security, "National Network of Fusion Centers Final Report," 2018, 5.

including fire service (-19%), emergency management (-17%), critical infrastructure (-22%), and cybersecurity (-19%)."[127] The decline in participation of the liaison officers results in a decline in the capabilities of the fusion centers to share information with their stakeholders. This negative decline matches the decrease in the budget for training and exercise.

2. Building Trust between IFCs and Citizens

Building trust between the IFCs and citizens is important. After all, trust in the public services providing security is one of the most important conditions for IFCs to function. As state and local actors, the fusion centers depend greatly on budgeting coming from state and local funds. According to the most recent Final Report, roughly 64 percent of the budget for the IFCs comes from state and local funding.[128] Consequently, fusion centers have to work to attract people's positive appreciation in order to keep receiving funds from local and state accounts. The biggest obstacle in front of the IFCs is attempting to maintain a good level of trust while avoiding the issue of violating privacy, civil rights, and civil liberties (P/CRCL).

The trust in the fusion centers is affected by the legacy of the local and federal law enforcement. According to Lewandowski and Guidetti, "fusion centers are on the front lines balancing freedom and security within the state and local threat landscapes."[129] The problem is that local and federal law enforcement working with domestic intelligence inclines the violation of P/CRCL. The fusion centers act as a frontline of domestic intelligence and succeed in the bad narrative from law enforcement experience. For example, the notorious operations conducted by the FBI's counter-intelligence program, COINTELPRO, which targeted Black Americans fighting against segregation and structural racism, remains a painful example of a P/CRCL violation.[130] The FBI was not

[127] Department of Homeland Security, "National Network of Fusion Centers Final Report," 2017, 20.

[128] Department of Homeland Security, "National Network of Fusion Centers Final Report," 2018, 2.

[129] Lewandowski and Guidetti, "The Role of Fusion Centers in Homeland Security," 187.

[130] Dia Kayyali, "The History of Surveillance and the Black Community," Electronic Frontier Foundation, February 13, 2014, https://www.eff.org/deeplinks/2014/02/history-surveillance-and-black-community.

the only agency that was involved in the scandal, as the NSA together with the FBI also was involved in spying on Dr. King to find "avenues of approach aimed at neutralizing King as an effective Negro leader."[131] The Church Committee was created in response to these and other public scandals, but the bad feeling about American intelligence spying on its own citizens remains and fusion centers as front liners in domestic intelligence bear the burden.

Similar to the FBI, the fusion centers have been involved in the surveillance of protesters too. The most recent example of a violation of the protesters' rights is from the Black Lives Matter protest in 2020. The revelation about irregular activities came from the poorly secured Northern California Regional Intelligence Center (NCRIC) website. According to Micah Lee, the NCRIC has provided daily lists of protestors from Black Lives Matter events, and it performed other actions which violated protestors' rights protected by the First Amendment.[132] The provided lists from the NCRIC to the local law enforcement were intended for Situational Awareness or planning/staffing purposes because there was evidence that there were planned looting, vandalism, and threats of violent activities.[133] Even though these inappropriate surveillances were not conducted for political or racial reasons like in the case of COINTELPRO, these revelations generated significant disapproval and debates from some civil organizations, and this led the criticizing the work of all fusion centers.

The lack of a unified model and a generous reading of the mission creep from most of the fusion centers led to concerns among the population and some civil societies about privacy violations. Privacy violations are sensitive issues that concern many civil society organizations and social groups. According to Palmer and Monahan, "[t]he range of people who now have access to sensitive information, and the expansion of access to people who previously did not have access to files without concurrent ethics guidelines, particularly at local and state levels, provides further credence to fears of intelligence abuse and privacy

131 Kayyali.

132 Micah Lee, "How NCRIC Keeps Tabs on Black Lives Matter Protesters," The Intercept, August 17, 2020, https://theintercept.com/2020/08/17/blueleaks-california-ncric-black-lives-matter-protesters/.

133 Lee.

violations" Because of the widening of the range of the missions of the fusion centers, the number of people involved in managing private information has also necessarily increased. From the information provided by the 2018 Final Report, barely 67 percent of the people who need permission for classified information have it.[134] Still, around 33 percent of the staff has to comply with the requirement for receiving classified information access, but they do not yet have the required permission. This discrepancy is challenging the trust of the people, especially in state fusion centers. Additionally, Monahan and Palmer noticed that there are many analysts who are contractors with a lesser degree of accountability.[135] There are also concerns about the access to information from third-party organizations.[136] Collaboration between private companies and fusion centers provides effective results, but there are many citizens who worry that these companies do not have proper mechanisms for privacy protection. Fusion centers must address these problems and work more closely with civil liberties organizations for more transparency in order to build trust in IFCs from the citizens.

Another challenge in building trust between fusion centers and the people is how to maximize effective intelligence productivity while simultaneously safeguarding privacy, civil rights, and civil liberties (P/CRCL). The main efforts of the fusion centers are intended to provide better protection for the citizens, and to do that they are trying to adopt a variety of contemporary technologies for collection and analysis. Unfortunately, using contemporary technologies for surveillance generates opposing opinions among the people and civil societies. According to EPIC, one of the civil liberties advocate organizations, "[IFCs] provide state and local police with access to a wide range of surveillance technologies including facial recognition, nationwide automated license plate reader databases, and social media monitoring services."[137] These situational awareness systems are considered helpful and innovative from a law enforcement point of view, but civil-liberties advocates do not agree. For example, camera surveillance systems helped in the

[134] Department of Homeland Security, "National Network of Fusion Centers Final Report," 2018, 2.

[135] Monahan and Palmer, "The Emerging Politics of DHS Fusion Centers," 629.

[136] Monahan and Palmer, 631.

[137] Butler, Scott, and Davisson, "EPIC Comments," 5.

detention of the terrorist suspects from the Boston Marathon Bombing and in detaining a suspect who tried to conduct an attack on Times Square.[138] The New York Police Department's Domain Awareness System facilitated the arrest of Ahmad Khan Rahimi, who was convicted of attempted bombings in New York and New Jersey.[139] The Domain Awareness system is useful and adequate for the threat environment. Such a system will increase the fusion centers' capabilities to find and track suspects, especially in domestic terrorism. The efforts of the fusion centers must be concentrated on convincing the citizens that such a kind of system is used properly and is not threatening the civil rights of the citizens.

Technology is changing, and now criminal groups take advantage of the shrinking technology gap that exists between them and intelligence centers. Amy Zegart's conclusion is that in the future, "intelligence will increasingly rely on open information collected by anyone, advanced code and platforms that can be accessed online for cheap or for free, and algorithms that can process huge amounts of data faster and better than humans."[140] She also suggests that there is a need for strategic efforts to understand how "intelligence agencies can gain and sustain the edge while safeguarding civil liberties in a radically different technological landscape."[141] If fusion centers do not maintain contemporary tools, their effectiveness will decrease. The fact that IFCs are not centralized under the federal government makes them more adaptive to the people's needs. As Dahl suggests, "[fusion centers] offer a flexible tool of government that can be calibrated to meet local needs and thus is more likely to be acceptable to the public."[142]

---

138 "Surveillance Cameras and the Times Square Bombing.," Slate, accessed August 9, 2022, https://slate.com/technology/2010/05/surveillance-cameras-and-the-times-square-bombing.html.

139 "New York's 8,000 Cameras Helped Snare Bomb Suspect Ahmad Rahami," NBC News, accessed August 9, 2022, https://www.nbcnews.com/storyline/ny-nj-bombings/more-8-000-cameras-helped-snare-bomb-suspect-ahmad-rahami-n650891.

140 Zegart, "In the Deepfake Era, Counterterrorism Is Harder."

141 Zegart.

142 Dahl, "The Localization of Intelligence," 12.

E. CONCLUSION

The concept of the fusion of information has a long history in supporting military operations and intelligence services fighting against state actors or foreign non-state actors. That experience shows both benefits and good results in tackling these foreign threats. Applying that concept to domestic threats and actors, however, is challenging for fusion centers. Collecting and disseminating information on American citizens is strictly defined and constrained in The First Amendment, which challenges the fusion centers' preemptive efforts.

Fusion centers must also increase investments in the education of their employees, with the education aimed both in preserving civil liberties and in minimizing mistakes made by unprepared employees. Fusion centers are on the frontline of domestic intelligence, and they are in the crosshairs of civil society organizations. Every failure in preserving the civil rights and civil liberties of the American citizens has great consequences and affects the people's trust.

Fusion centers must improve the trust they receive from citizens. Being in the frontline of domestic intelligence, IFCs have to be more open in front of the citizens and civil societies. Currently, there are established mechanisms for mitigating civil liberties violations, but citizens are unaware and unconvinced. There is a need for more information campaigns about the fusion centers' work and how they contribute to the safety of local communities. IFCs have to develop very robust practices that will guarantee to the public that preserving civil liberties is a priority. Still, at the same time, they have to maintain a high level of effectiveness and capability to adapt swiftly to the new threats from domestic terrorism.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DOMESTIC VIOLENT EXTREMISM AND IFCS IN THE U.S.

Domestic violent extremist threats evolved significantly during the last decade and started challenging U.S. security more seriously. According to the Department of Homeland Security (DHS) threat assessment in 2020, "ideologically motivated lone offenders and small groups pose the most likely terrorist threat to the Homeland, with Domestic Violent Extremists presenting the most persistent and lethal threat"[143] According to the report, among all domestic violent extremists, racially and ethnically motivated white supremacist extremists (WSEs) will continue to pose the most serious and deadly threat to the homeland.[144] Another intelligence report provided by The Office of The Director of National Intelligence reached a similar conclusion two months after the Capitol insurrection.[145] In the last decade, DVE became a real threat to U.S. security. Among all violent extremists with left or right ideology, the far-right extremists are the most dangerous, and intelligence services have begun to recognize this growing problem.

This chapter focuses on the rise of far-right extremism in the U.S and the work of the Intelligence Fusion Centers (IFCs) to address that threat. The first part of the chapter covers the common far-right ideology and the distinctions between the different groups. The chapter continues with a historical overview of the rising far-right extremism in the United States. It continues by characterizing the white supremacist movement as one of the most dangerous hate movements in the United States. The last part of the chapter focuses on the contribution of the IFCs in countering violent extremism. This part examines the Capitol insurrection on January 6 and the intelligence warnings that IFCs were able to analyze and disseminate with local and federal security services.

[143] Department of Homeland Security, "Homeland Threat Assessment October 2020," 18.

[144] Department of Homeland Security, 18.

[145] The Office of the Director of National Intelligence, "Unclassified Summary of Assessment on Domestic Violent Extremism," 2.

A. THEORETICAL FRAMEWORK

Understanding the problem is an important step in the fight against any threat. In the case of DVE, however, understanding the problem is challenging. The focus here is toward far-right ideology. There are many different types of groups in the United States that can be classified as far-right domestic violent extremists. Recently terms such as the far right, the radical right, or the extreme right are used constantly, but the understanding of what they cover exactly is confusing. There are also differences between concepts like extreme-right violence, extreme-right terrorism, and hate crime.[146] For example, on May 14, 2022, Payton Gendron allegedly shot 13 people in a Buffalo supermarket, most of them black. It was reported that the killer had made a statement before the attack supporting racist theories and that he had the intention to kill black people.[147] The DOJ and FBI Director Wray stated that the incident is a "hate crime and an act of racially-motivated violent extremism."[148] On the other hand, President Biden defined the incident as an act of domestic terrorism.[149] Such kinds of division in the decision-makers and services shows the complexity of the problem and how difficult it is to define the roots of that problem. Without clearly framing the specifics of a violent act, it is difficult to address the problem with appropriate measures.

1. The Far-Right Ideology

There is no clear line between the different far-right groups, which makes it more difficult to track them. The far-right have additional internal divisions into radical and extreme wings.[150] Bjørgo and Ravndal try to classify the different far-right groups.

---

[146] Tore Bjørgo and Jacob Aasland Ravndal, "Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses," International Center for Counter-Terrorism, September 2019, 1.

[147] Carolyn Thompson, "Grand Jury Indicts Man In Buffalo Supermarket Shooting," HuffPost, May 19, 2022, https://www.huffpost.com/entry/buffalo-supermarket-shooting-payton-gendron-indicted_n_62864ecce4b00685b66a4d44.

[148] Lisa N. Sacco, *Sifting Domestic Terrorism from Domestic Violent Extremism and Hate Crime*, CRS Report No. IN10299 (Washington, DC: Congressional Research Service, June 1, 2022), 3.

[149] Sacco, 3.

[150] Bjørgo and Ravndal, "Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses," 2.

According to them, the radical groups seek change within the democratic framework. Extreme groups, in contrast, reject democracy and are willing to use violence or other unconventional methods to further their objectives.[151] According to the authors, the radical right does not necessarily seek to eliminate democracy itself, but it does wish to eliminate liberal elites. Extreme right groups not only legitimize assaults against these elites but want to tear down democracy.[152]

There is another distinction between cultural nationalist groups, ethnic nationalist groups, and racial nationalist far-right groups. Bjorgo and Ravndal suggest that cultural nationalists are represented by radical-right populists and normally are anti-Islam and anti-immigration, but they are not as driven by anti-racial ideology.[153] Ethnic nationalists believe that people from different ethnic groups must not be blended, and that different ethnic groups should be expelled from the state.[154] And finally, racial nationalists believe that the white race is superior and that subordinated races must be deported or exterminated.[155] According to Bjorgo and Ravndal, "their worldview is typically based on anti-Semitic conspiracy theories, claiming that Jews promote immigration, egalitarianism, and racial mixing to destroy the white race."[156]

In the United States, far-right groups are composed of a seemingly mixed ideology. Some scholars argue that in the United States the far-right groups are represented by ethno-nationalist divisions, but many of their members gravitate around the ideas of the white supremacists, and they often call themselves white nationalists.[157] Joshua Freilich et al. provide a definition about American far-right extremism, where they define it as "fiercely nationalistic, anti-global, suspicious of centralized federal authority, reverent of individual liberty, believe in conspiracy theories that involve a grave threat to national sovereignty

[151] Bjørgo and Ravndal, 2.

[152] Bjørgo and Ravndal, 3.

[153] Bjørgo and Ravndal, 3.

[154] Bjørgo and Ravndal, 3.

[155] Bjørgo and Ravndal, 3.

[156] Bjørgo and Ravndal, 5.

[157] Bjørgo and Ravndal, 4.

and/or personal liberty…, and a belief in the need to be prepared for an attack either by participating in, or supporting the need for, paramilitary preparations and training or survivalism."[158] Overall we cannot describe a clear pattern of any extremist group and separate them into different categories. Very often, one specific group that could be described as ethno-nationalist could include members with different beliefs, or the group may have partners and connections to other extremist groups with different ideologies. All these differing ideologies and beliefs create difficulties for the security services attempting to analyze and target the problem.

2. Classification of Far-Right Extremists' Attacks

Far-right extremism differs from the well-known Islamic terrorism in the type of attacks both groups commit. According to Ravndal and Bjørgo, Islamist terrorism seems to follow a low frequency but high-intensity trend, with sporadic attacks that inflict many fatalities. In contrast, the far right's brand of terrorism exhibits a pattern of high frequency but low severity, with many assaults that result in just one or two fatalities.[159] This difference created the perception that Islamic terrorism is a major threat, and until recently, the problem with far-right extremism was neglected.

In order to better understand the complexity of the right-wing extremist attacks, this thesis will use the explanation of right-extremist attacks presented by Bjørgo and Ravndal. According to the authors, right-wing attacks could be divided into three categories: right-wing violence, right-wing terrorism, and hate crimes.[160] Right-wing violence is considered as a grouping of more broad attacks conducted by people with certain right-wing beliefs, and the selection of their targets are usually immigrants, minorities, political opponents, or governments officials, and the attacks are motivated due to their far-right perceptions.[161]

---

[158] Joshua D. Freilich et al., "Patterns of Fatal Extreme-Right Crime in the United States," *Perspectives on Terrorism 12*, no. 6 (December 2018): 39.

[159] Jacob Aasland Ravndal and Tore Bjørgo, "Investigating Terrorism from the Extreme Right: A Review of Past and Present Research," *Perspectives on Terrorism* 12, no. 6 (December 2018): 5.

[160] Bjørgo and Ravndal, "Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses," 5.

[161] Bjørgo and Ravndal, 5.

Right-wing terrorism is when an assault is prepared and designed to spread fear among more people in order to influence political outcomes.[162]

The third category, hate crimes, makes the understanding blurrier and confusing. The problem is that those hate crimes could overlap with violence and terrorism, but they could also be classified separately. One example of the overlap between hate crimes and terrorism is the Charleston church attack that killed of nine black people in 2015.[163] Bjørgo and Ravndal suggest that hate crimes are "motivated by bias or hatred against certain categories of people, such as religious, racial, or sexual minorities or people with disabilities"[164] The hate crimes are frequently committed by nonpolitical youths acting alone, not in accordance with a structured hate group, and only for the thrill of it, and the perpetrators' personal bias drives them to commit these crimes.[165] All these blurry lines between the different groups and the types of attacks that they conduct create difficulties for the legal authorities and security services in attempts to track and intercept the perpetrators. It is also difficult to count on accurate statistics because there is no clear picture of the situation.

Lone-wolf actors are a real challenge for intelligence services due to their limited social connections and their lack of affiliation to a particular group. According to Ellis et al., lone-wolf actors usually plan, prepare, and execute their attacks without any direct support from an organization or person, and their decision is not guided by anybody and is instead inspired by cause or ideology.[166] Although, there is evidence that "most lone actors maintain social ties, which are critical to the development of their motivations and

[162] Bjørgo and Ravndal, 5.

[163] "Hate Crimes, Explained," Southern Poverty Law Center, accessed September 14, 2022, https://www.splcenter.org/hate-crimes-explained.

[164] Bjørgo and Ravndal, "Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses," 6.

[165] "Hate Crimes, Explained."

[166] Clare Ellis et al., "Analysing the Processes of Lone-Actor Terrorism: Research Findings," *Perspectives on Terrorism* 10, no. 2 (2016): 33, https://www.jstor.org/stable/26297551.

capabilities to complete their acts of extreme violence."[167] A study shows that prior to the attack, often the lone actors exhibit "leakage behavior" intended for spreading their extreme objectives.[168] This leakage behavior is in the form of some type of manifesto and it is the only good opportunity for the intelligence services to detect the imminent attack. The problem is that the time is very short, and the reaction of the security services is delayed.

B. THE RISE OF THE FAR-RIGHT EXTREMISM

Far-right ideology in the United States is not new, and it usually is not illegal until it becomes extreme. In the United States, these movements started gaining significant popularity during the Obama administration and increased during the Trump administration. The rise of far-right extremism became more obvious after 2016, when there was a significant increase in the number of the incidents connected with far-right groups. According to the ADL, the leading anti-hate organization, in 2015 there were 76 registered hate incidents which include Extremist Murder, Terrorist Plot/Attack, Extremist/ Police Shootout, White Supremacist Event, White Supremacist Propaganda, and Antisemitic Incident.[169] The following year the registered incidents of far-right activity rose to 1330, and it continued rising until the peak of 7751 reported incidents in 2021.[170] Of all different categories registered during the years, two thirds of the incidents are connected with white supremacist groups and the other one-third are anti-Semitism oriented. According to many experts, one of the reasons for that abrupt increase was the newly elected President Trump and his noticeable support for far-right people.[171] The

[167] Joshua D Vitali, "Fueling The Fire: An Examination of Right-Wing Extremism in The United States Over The Last Decade" (master's thesis, Monterey, Naval Postgraduate School, 2020), 29, https://calhoun.nps.edu/handle/10945/65460.

[168] Bart Schuurman et al., "Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis," *Journal of Forensic Sciences* 63, no. 4 (2018): 1195, https://doi.org/10.1111/1556-4029.13676.

[169] "HEAT Map," ADL, accessed August 31, 2022, https://www.adl.org/resources/tools-to-track-hate/heat-map.

[170] "HEAT Map."

[171] Vitali, "Fueling The Fire: An Examination of Right-Wing Extremism in The United States Over The Last Decade," 57.

President's support to the members of the far-right provided encouragement and legitimacy, which indirectly resulted in more activities and extremism.

1. The Evolution of the Far-Right in the United States—from Rallies to Terror

The far-right wave in the United States spread significantly between 2016 and 2018. Over this period of time The Southern Poverty Law Center (SPLC) registered "125 rallies, marches and protests nationwide, which were organized and attended by far-right extremists, including white nationalists, neo-Nazis, Klansmen, the alt-right, and right-wing reactionaries."[172] Along with the marches and rallies, the homicides allegedly committed by far-right extremists tripled from 47 during the last three years of the Obama administration to 147 during the first three years of the Trump administration.[173] According to Seth G. Jones , the biggest concern comes from "white supremacists and anti-government extremists, such as militia groups and so-called sovereign citizens interested in plotting attacks against government, racial, religious, and political targets in the United States."[174]

The organization of rallies and clashes with other protesters was the initial tactic enabling far-right extremists to gain support. The origins of this tactic were marked in Charleston, South Carolina in 2015. Dylann Roof, who was self-radicalized and did not belong to any white supremacist group, killed nine black worshipers in a church in Charleston.[175] After this attack, South Carolina removed the Confederate flag from its Capital in order to show support and respect, which led to the removal of other such flags from monuments in the state.[176] This act of removing the racist symbol provided fuel to

---

[172] Cassie Miller and Graves Howard, "When the 'Alt-Right' Hit the Streets: Far-Right Political Rallies in the Trump Era," Southern Poverty Law Center, accessed September 15, 2022, https://www.splcenter.org/20200810/when-alt-right-hit-streets-far-right-political-rallies-trump-era.

[173] David Neiwert, "Domestic Terror in the Age of Trump," Reveal, July 9, 2020, http://revealnews.org/article/domestic-terror-in-the-age-of-trump/.

[174] Jones, "The Rise of Far-Right Extremism in the United States," 1.

[175] "Dylann Roof Wrote White Supremacist Manifestos: Prosecutors," *Reuters*, August 22, 2016, sec. U.S. News, https://www.reuters.com/article/us-south-carolina-shooting-idUSKCN10X29A.

[176] "Confederate Flag Taken down from South Carolina Capitol," *BBC News*, July 10, 2015, sec. U.S. & Canada, https://www.bbc.com/news/world-us-canada-33483415.

the right-wing narratives and grievances. According to the SPLC, six months after removing the Confederate flag, there were 364 pro-Confederate rallies, some of which gathered more than 4000 people.[177] These rallies built connections and attracted conservative supporters united around the idea of preserving the Confederate symbols. Additionally, Trump's anti-Muslim and anti-immigration statements strengthened the far-right narratives among the supporters of these ideas.

The more violence of far-right supporters against counter-protesters reflects more recruitment for new sigmatisms. The common tactic of far-right groups is to announce a rally a month prior to the event providing the chance for Antifa supporters to organize anti-protests. Then on the day of the protest, the far-right extremists escalate the situation and began clashes with the Antifa members. All these scenes were captured on videos and uploaded on social media. These videos of violence serve as a recruitment tool for new sympathizers. According to the SPLC, the Berkeley rally in April 2017 marked the change in the far-right because they realized that violence on videos brings more supporters, and law enforcement did nothing to remove the videos from the open social platforms.[178] After 2017 the counter protests outnumbered the far-right rallies significantly, and this tactic did not work anymore. Since this period, the far-right started focusing more on retreating to the internet and spreading far-right propaganda there.[179]

Stepping back from the rallies and focusing on internet propaganda changed the pattern of the aggression of far-right extremists, and white supremacists became the main players. Spreading propaganda on the internet influences lone wolf actors to conduct violence. David Neiwert estimates that "incidents involving people who were exposed to violent extremist ideologies almost entirely online—rather than through contact in real-world settings—rose substantially starting in 2015, amounting to nearly 1 in 5 incidents during the Trump years."[180] One of the most significant attacks that inspired many white

[177] Miller and Howard, "When the 'Alt-Right' Hit the Streets."

[178] Miller and Howard.

[179] Miller and Howard.

[180] Neiwert, "Domestic Terror in the Age of Trump."

supremacists was the killing of 51 Muslim people in New Zealand. This attack was used by many as an example and inspiration for attacks in the United States. According to Neiwert, the recent attackers "are not ideologically identical, but they tap into similar ideological strains and modes of attacks that bind them together and help one terrorist act fuel another, and another after that."[181] Every next attack is an inspiration for lone-wolf actors who are not members of any particular organization, but who do share the same violent extremist ideologies and grievances. The fact that these people are self-radicalized and lack connections with other people significantly hardens the work of the security services to prevent any attack.

The lack of understanding of the problem from law enforcement and the focus on Islamic terrorism provided freedom for far-right movements to grow. During the Obama and Trump administrations, the U.S. security services were focused on Islamic terrorism and threats coming from ISIS. The data shows, however, that in the United States, far-right extremists conducted much more deadly attacks on American citizens than Islamic terrorism. According to Ankrom and Neiwert's database in Figure 2, the right-wing extremist attacks are much more frequent, and the success of law enforcement in foiling the far-right plots is significantly lesser than the Islamic attacks.[182] The fact that law enforcement was more focused on other issues provided relative freedom for far-right movements to spread their ideology, to execute violence and attacks, and to attract more supporters. The threat from the far-right extremists became obvious after 2017 when the attacks became more deadly.

[181] Neiwert.

[182] "Domestic Terrorism Database," Domestic Terrorism Database, accessed September 17, 2022, https://apps.revealnews.org/domestic-terror-int/index.html.

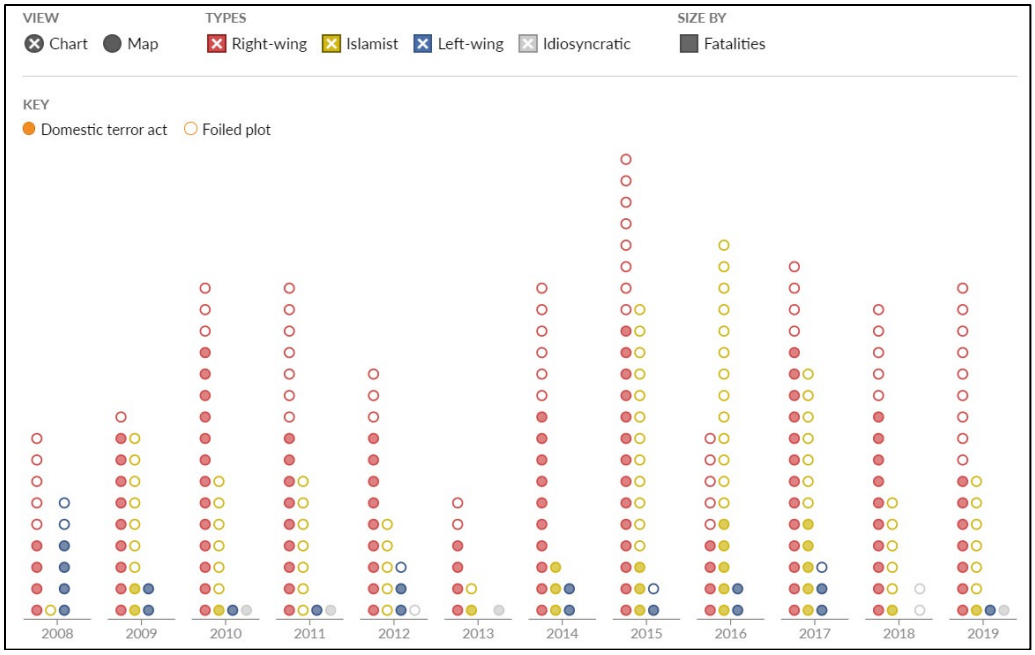

Figure 2. Domestic terror attacks in the United States.[183]

Here we are discussing violent far-right extremism as one entity, but it is divided and very nuanced. According to McHugh and Armour, the U. S. far-right consists of three main pillars: white supremacists, anti-government movements, and Christian fundamentalists.[184] The development of communication technologies allowed conspiracy theorists, like the QAnon movement, to influence the far-right's development and become the fourth pillar.[185] To complete the picture of the violent far-right extremism, we have to add lone-wolf actors who do not participate in any movement, but who still gain inspiration from the ideas and propaganda of the far-right. This challenging threat environment is represented not only by the far-right, as there is also violent extremism from the left. Far-left extremism is not as dangerous and active as far-right extremism, but it still presents challenges for intelligence services to maintain a clear understanding.

[183] Source: "Domestic Terrorism Database."

[184] McHugh and Armour, "Trends in Domestic Violent Extremism."

[185] McHugh and Armour.

2. Strategy and Concepts of White Supremacy Extremism

The main concept of the white supremacy movement is a race war. The acronym "RAHOWA," which means "racial holy war" is a widespread slogan among white supremacist internet social groups and platforms. Daniel Byman suggests that white supremacists believe that the racial holy war is already ongoing, and all believers of white supremacy are warriors defending the white race.[186] Believing in such a theory provides legitimacy to the actions of all lone-wolf actors because they believe that white people are being attacked, and those who are killing non-white people are defenders of the cause. In order to win that race war, white supremacists count on violence to attract more people to the cause. According to Byman, violence is the main form of propaganda, and through wide media coverage it will ensure the accumulation of money, people, and other resources necessary for further attacks.[187]

Sometimes when there are not enough overt activities involving white supremacists, the violence may be stoked and accelerated by provocateurs, enabling white supremacists to maintain the motivation for violence against their enemy. These activities can include false-flag operations, in which provocateurs pose as their opponents to initiate violence. According to the hearing of the Subcommittee on Intelligence and Counterterrorism Committee on Homeland Security, several days before the anti-gun control rally in Richmond, Virginia, where there were left and right supporters of the rights to possess guns, the FBI arrested three members of the neo-Nazi group known as the Base, in July 2020.[188] They were arrested due to accusations of planning and preparation to shoot into the crowd with the intention to inflict fear and outrage, which would be blamed on their leftist political enemies.[189] This example supports the idea that to maintain the

186 Daniel Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism* (New York & London: Oxford University Press, 2022), 129.

187 Byman, 130.

188 "Assessing the Threat from Accelerationists and Militia Extremists" (Washington, D.C.: Subcommittee on Intelligence and Counterterrorism Committee on Homeland Security, July 16, 2020), 7, https://www.congress.gov/event/116th-congress/house-event/110911.

189 "Assessing the Threat from Accelerationists and Militia Extremists," 7.

movement, it has to continue the violence. The acceleration of violence provides more supporters, and these supporters will ensure even more violence.

The decentralized organization of the white supremacists presents a significant challenge to law enforcement and IFCs to prevent a deadly attack. In 2015 Dylann Roof killed nine worshipers at a Black church in Charleston; in 2018 Robert Bowers killed 11 worshipers at the Tree of Life synagogue in Pittsburgh; and in 2019 an even deadlier attack occurred at a Walmart in El Paso by Patrick Crusius, where 23 people were murdered. According to Daniel Byman, these are the deadliest white supremacist attacks in recent years, but none of the three perpetrators are representatives of a particular group or organization.[190] He suggests that the online culture of hate and white supremacy significantly shaped their behavior.[191] The inspiration of violence is the main strategy of the white supremacy movement. In such a strategy, the survivability of the movement increases, and the chances of preventing the attack diminish significantly due to a lack of direct interaction with a particular organization or people.

Embracing a leaderless organization has advantages and disadvantages. When we talk about advantages, secrecy and sustainability are the most important. Any hierarchical organization is vulnerable to infiltration and disruption from law enforcement. According to Byman, many white supremacist organizations in the past have disappeared after the arrest of their chief leaders, which led to the arrests of their followers or bankruptcy due to legal fees or lawsuits.[192] In order to safeguard the movement from such possibilities, the white supremacists embraced leaderless organizations. This kind of organization has a significant advantage in terms of operational security, and it is used when there is a strong government.

On the other hand, leaderless organizations are a sign of weakness, as it also has many disadvantages. Byman suggests that "too decentralized a process means that believers all go in different directions, reducing their overall impact, and the actions of the

[190] Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism*, 123.

[191] Byman, 123.

[192] Byman, 137.

undisciplined members…can lead to government crackdowns"[193] He also suggests the ability to organize and conduct a major attack on well-secured targets decreases due to the lack of support from the movement.[194] The pressure from law enforcement keeps the white supremacy movements decentralized, and that keeps the growth of the movement low. In order to pressure such kinds of far-right extremists, the intelligence role becomes even more of a major factor that could provide additional suppression.

Raising funds for the cause of white supremacy is another challenge that decreases the movement's capabilities to organize attacks. This is also an opportunity for the IFC to track and facilitate disruption of these fundraisings. According to Rena Miller, the white supremacy groups are poorly funded, and most of the extremists are self-funded.[195] This again creates difficulties for the security services to intercept the potential attack, but it also shows the weaknesses of the movement. According to Anti-Defamation League, "because of the comparatively small size of the white supremacist movement and the relative lack of wealth within it, the movement is limited in the amount of money that it can generate."[196] The poorly funded groups cannot count on a financial flow that is necessary for buying weapons, paying operatives to be members, covering legal defenses for those members who are arrested, and so on. This weakens any organization because the members of the group have to take care of themselves and the connections between the members and the group become less important. This creates opportunities for law enforcement to put more pressure on the members by making them informants to earn rewards from the government.[197]

The white supremacists are only one side of DVE, but it is important to explore this ideology because it remains the most common cause of lethal domestic attacks in the

[193] Byman, 140.

[194] Byman, 140.

[195] Rena S. Miller, *A Persistent and Evolving Threat: An Examination of the Financing of Domestic Terrorism and Extremism*, CRS Report No. TE10056 (Washington, DC: Congressional Research Service, January 15, 2020), 4.

[196] Anti-Defamation League, "Funding Hate," 14.

[197] Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism*, 157.

United States. The white supremacists, like other far-right extremists, use violence to maintain popularity and recruit. The funding problem for white supremacists presents a significant disadvantage due to their limitation in collecting money, leading to restricted operational capabilities. The neglect of the problem by the political elite and the security services provided a comfortable environment for far-right extremism to grow undisturbed, but the focus of the DHS and the FBI on DVE may start to significantly pressure far-right extremists.

C. THE ROLE OF THE INTELLIGENCE FUSION CENTERS IN SUPPORTING THE FIGHT AGAINST DVE

Domestic violent extremism (DVE) is not a new threat, and the intelligence services have techniques to fight against it. According to Jones, the FBI and local law enforcement agencies successfully infiltrated and destroyed some right-wing terrorist organizations throughout the 20th century, including the Order and the Covenant, Sword, and Arm of the Lord.[198] The basic ideology of the violent extremists has not significantly changed, but the means of communication and ways of reaching more people is easier than before. These new tools challenge the Intelligence services and create difficulties in providing the necessary support security services need to continue holding DVE down to a manageable level while also preventing violent attacks with significant consequences.

IFCs are not the primary organizations responsible for dealing with DVE, but their role is important for managing the threat level and as a mechanism preventing a major attack. The DHS, FBI, and some state and local services are the primary entities tasked with the collection of information about domestic violent extremists, and the IFCs provide the necessary connection between these security entities. That connection could flow both ways through mutual information exchanges such as from federal entities to local police departments and from grassroots entities to federal agencies. The IFCs work as a connector of the local and federal intelligence services, and they can provide tactical intelligence necessary for the prevention of high intensity attacks organized by domestic violent extremists. Dealing with extremists requires tactical intelligence and a better understanding

198 Jones, "The Rise of Far-Right Extremism in the United States," 6.

of the local situation in order to effectively connect the dots, and IFCs can efficiently satisfy this need.

Learning how far-right extremists communicate and organize themselves provides opportunities for the IFCs to obtain understanding about intentions and the atmosphere in state and local situations. In a testimony in 2021 to the House Homeland Security subcommittee on counterterrorism, John Cohen underlined the importance of social media for far-right extremists, and he claimed that the DHS planned "increased analytic focus to more comprehensively assess how violent extremist actors and other perpetrators of targeted violence exploit and leverage social media and other online platforms."[199] Adam Schiff, chairman of the Intelligence Committee stated that "it appears that probably some of the best intelligence prior to January 6 was open source."[200] Open-source information is important to the operation of IFCs, and January 6 provides a good examples of the role IFCs served and how they were able to exploit open-source information to build a clear picture about the intentions and preparations involved in the of storming the Capitol.

1. Case Study: The Capitol Insurrection and the Role of the IFCs

In order to better understand the importance of IFCs in countering DVE, this section examines the IFCs' role in one of the most significant events against democracy in the United States: the Capitol insurrection. This event was not an ordinary far-right extremist attack or rally because it combined all the different aspects of the far-right groups in one place. It combined anti-government, white supremacist, neo-Nazi groups, and many ordinary supporters of the far-right ideology. This mass organization is important, because it illustrates the IFCs' role and how the information coming from state and local agencies provided understanding and early warnings for the preparation and execution of an attack against U.S democracy. Furthermore, it shows how when the primary agencies responsible for fighting against DVE failed to raise a proper warning regarding the attack, the IFCs served as a secondary warning system independent from political biases.

199 "DHS Is Gathering Intelligence on Security Threats from Social Media," NBC News, accessed September 27, 2022, https://www.nbcnews.com/politics/national-security/dhs-launches-warning-system-find-domestic-terrorism-threats-public-social-n1266707.

200 "DHS Is Gathering Intelligence on Security Threats from Social Media."

a. Events Leading to the Capitol Insurrection

The January 6 attack is arguably the highest level of mobilization the far-right extremists achieved in the United States in the last several decades. The far-right movements have slowly grown since the Obama administration, and they have significantly raised their popularity during the Trump presidency. According to an interview made by A.C. Thompson with Brian James, one of the leaders of a Proud Boys group, the people on the right see former President Trump as a supporter of their far-right ideology, and they now see the biggest hope for change in a direction palatable to the far-right.[201] A.C. Thomson, who was tracking the far-right movement for years, asserts that on January 6, among the regular supporters for Trump, there were groups like Proud Boys, who are an ultranationalist street fighting group; militias groups like the Oath Keepers, the Three Percenters, and the Boogaloo Boys who believe in overthrowing the U.S. government; white nationalists; and also QAnon followers believing in conspiracy theories.[202] President Trump's influence and indirect messages toward the far-right led to the culmination of the anti-government event of the January 6 Capitol Breach, including far-right groups blended in with regular Trump supporters who played an important role in driving the mob towards violence.

The attack against election certifications could be traced back to the planting of the seeds of doubt regarding the lawfulness of the election. According to Alan Feuer et al., disinformation about the fake election results was encouraged by Trump, which led to the motivation of his followers to dispute the election results.[203] Doing this, intentionally or not, President Trump received the attention of many far-right movements that already believed that he, as the President, supported them, and they moved to support him.

---

201 *American Insurrection* (Frontline Film, 2022), PBS, sc. 18.36, https://www.pbs.org/wnet/exploring-hate/films/american-insurrection-a-frontline-film-2022/.

202 *American Insurrection*, 1.01.

203 Alan Feuer et al., "Jan. 6 Timeline: Key Moments From Before the Attack on the Capitol to Now," *The New York Times*, June 9, 2022, https://www.nytimes.com/interactive/2022/us/politics/jan-6-timeline.html.

In 2020, far-right groups became more active than usual due to being influenced by conspiracy theories surrounding Covid-19. A number of rallies were organized by far-right groups, and some of these rallies hosted significant numbers of people. In Virginia on January 20, more than 20,000 gun rights activists, many of them armed, gathered to protest. Among the protestors were Proud Boys members.[204] On April 30, after Trump tweeted "Liberate Michigan," armed protesters stormed the Michigan State House. Two of the protesters involved were charged for planning to kidnap the governor of Michigan and to bomb the state Capitol.[205] According to A.C. Thompson, there were many others who targeted and threatened public officials at a state and local level.[206]

On December 19, several weeks after losing the elections, Trump tweeted, asking support from his followers for disputing the results of the election on January 6.[207] The reactions after this tweet were immediate, and it stirred a huge magnitude of support among far-right movements. According to Feuer et al., on a forum called "The Donald win" people started posting information about bringing arms to the protests and shared plans for the tunnel infrastructure under the Capitol. The most active and violent among these commenters were far-right extremist groups like the Proud Boys, the Oath Keepers and the Three Percenters militia movement.[208] Other interesting groups that planned to participate at the rally were Latinos for Trump and the Virginia Freedom Keepers, which both oppose vaccines and occupied the Virginia State House.[209] According to the Feuer et al. the common thing between all these groups was that they were "participants in a private group chat on the encrypted app Signal called F.O.S. or Friends of Stone, a reference to Roger J.

204 Lois Beckett, "Virginia: Thousands of Armed Protesters Rally against Gun Control Bills," *The Guardian*, January 20, 2020, sec. U.S. news, https://www.theguardian.com/us-news/2020/jan/20/virginia-gun-rally-activists-richmond.

205 Kathleen Gray, "In Michigan, a Dress Rehearsal for the Chaos at the Capitol on Wednesday," *New York Times*, January 9, 2021, sec. U.S., https://www.nytimes.com/2021/01/09/us/politics/michigan-state-capitol.html.

206 *American Insurrection*, 16.44.

207 Alan Feuer et al., "Jan. 6 Timeline: Key Moments From Before the Attack on the Capitol to Now."

208 Feuer et al.

209 Feuer et al.

Stone Jr., Mr. Trump's longtime adviser."[210] On the day of the protests things are well known that after the speech of Mr. Trump, the mob headed to the Capitol and stormed the building.

b. Intelligence Warnings and IFCs Contribution

There are two fusion centers responsible for covering the security of Washington, D.C., The DC Fusion Center is part of the D.C. Homeland Security and Emergency Management Agency, and it is in close coordination with the Maryland and Virginia fusion centers and federal security services.[211] The DC Fusion Center is part of the National Network of Fusion Centers that work with DHS and is responsible for sharing information regarding terrorism, crime, and other hazards.[212] Another fusion center in the district is the Northern Virginia Regional Intelligence Center, which is more focused on the fusion processing of terrorism.[213]

The January 6 Capitol Breach is a good example of how IFCs provide sufficient situational awareness and warnings about the threats coming from DVE. The DC Fusion Center's contributions regarding domestic violent extremists could be assessed as sufficient for concluding that far-right groups would target the election certification and there would be a potential threat to security during this event. Hendrix et al. were able to provide information about the sequence of the activities of the D.C. Fusion Center. According to them, on December 14, the DC Fusion Center started sharing open source intelligence regarding January 6 with local and federal services.[214] On December 21, the DC Fusion Center provided information to the Metropolitan Police Department for the District of Columbia and the DHS Office of Intelligence and Analysis about extremist

---

[210] Feuer et al.

[211] Justin Hendrix et al., "Capitol Attack: Federal Agencies' Use of Open Source Data and Related Threat Products Prior to January 6, 2021," Report to Congressional Requesters (The Government Accountability Office, May 5, 2022), 8, https://www.justsecurity.org/81384/facebook-provided-warning-to-fbi-before-january-6-gao-report-reveals/.

[212] Justin Hendrix, 8.

[213] Justin Hendrix et al.

[214] Justin Hendrix, 36.

groups preparing to bring weapons to the protest in Washington and sharing instructions on how to avoid detention by security services.[215] On December 29 information from a neo-Nazi-affiliated telegram channel regarding the march on January 6 was shared again with local law enforcement and FBI.[216] On January 4th 2021, the DC Fusion Center warned U.S. Park Police about coordination between far-right groups like Proud Boys, QAnon, and other militia groups.[217]

The Northern California Regional Intelligence Center (NCRIC) also contributed to the fusion process by processing many signals received from some social media companies in Silicon Valley. According to the director of the NCRIC, Mike Sena, the reports from the social media companies were so numerous that his office was unable to process all the information and he had to retranslate it to the FBI directly.[218] Sena also requested information from other fusion centers for similar activities of the far-right groups in their regions, and on that request he received around three hundred replies from all 80 fusion centers in the United States.[219]

2. DISCUSSION

From an intelligence perspective, most scholars do not consider the January 6 attack a major intelligence failure, but still, there were significant flaws. The organization of this insurrection produced a lot of intelligence warnings, and the U.S. IC collected many of them. According to Dahl, the intelligence warnings and reports that came before the Capitol insurrection "represent a remarkable example of what we call the 'intelligence cycle'—how it works, or in this case, how it doesn't work."[220] In this case, the intelligence cycle or the fusion process of the IFCs had not failed, because they provided very valuable

[215] Justin Hendrix, 37.

[216] Justin Hendrix, 37.

[217] 38.

[218] Phoebe Connelly et al., "Warnings of Jan. 6 Violence Preceded the Capitol Riot," *Washington Post*, accessed October 4, 2022, https://www.washingtonpost.com/politics/interactive/2021/warnings-jan-6-insurrection/.

[219] Connelly et al.

[220] Erik Dahl, "January 6th Intelligence Failure Timeline," *Just Security*, June 7, 2022, https://www.justsecurity.org/81806/january-6-intelligence-and-warning-timeline/.

information in a timely manner. The intelligence cycle failure happened in the upper-level federal agencies responsible for DVE. According to Mitchell Silber, the intelligence collection did not fail, but "the failure was in the analysis of the intelligence and the failure of senior government officials to issue warnings based on that intelligence."[221]

The collection part of the intelligence cycle for the Capital insurrection was complete and sufficient to conclude that there would be violence during the certification of the elections. A significant part of this information collection came from the contribution of the IFCs' information. According to a report from The Government Accountability Office, the most important information about the potential for an attack on January 6 came from social media and open-source information.[222] The IFCs have the capacity to observe social media platforms, and because of their local focus they were able to collect a more complete body of information that they then were able to analyze correctly.

The collection of information from social media is a very controversial issue in the United States, due to the blurry line between free speech rights and what may be seen as potentially organizing a conspiracy against the government. As we understood from the previous chapter, far-right extremists use social media and the digital environment as very important tools and they use these tools widely. According to Silber, "one of the most common refrains when discussing the challenge of collecting intelligence against domestic violent extremists is that, without a catchall domestic-terrorism statute, government authorities can do little to intervene preemptively without evidence of a planned violent act or other crime"[223] The protection of the First Amendment and the protection of free speech significantly obstruct the work of the IFCs when they have to collect information about domestic violent extremists, but they still have legal opportunities to obtain information.

The IFCs can legally collect information from social media in specific conditions without causing a violation of civil rights and civil liberties. The First Amendment protects

221 Mitchell D. Silber, "Domestic Violent Extremism and The Intelligence Challenge," Atlantic Council, May 2021, 1.

222 Justin Hendrix et al., "Capitol Attack: Federal Agencies' Use of Open Source Data and Related Threat Products Prior to January 6, 2021," 1.

223 Silber, "Domestic Violent Extremism and The Intelligence Challenge," 12.

all U.S. citizens' rights to peacefully protest and their freedom of speech. According to The Government Accountability Office, "executive branch agencies that maintain a system of records shall maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute"[224] The IFCs have the capabilities and permission to collect open-source information from social media without violating the First Amendment, but only in specific circumstances. These circumstances are described in the 2013 Social Media Policy Guide and in the 2017 Real-Time and Open-Source Analysis Resource Guide. According to GAO, these two guidelines permit IFCs to lawfully use open-source information, if there is risk to public safety.[225] Still, the opportunity to use social media as a source of information raises many concerns in the organizations protecting civil liberties, but in attacks such as the one on January 6, IFCs are able to use these assets to achieve a better understanding of the intentions of far-right movements.

The collaboration with local companies and partners is another advantage of IFCs that could provide valuable intelligence information. We see that the close work of the The Northern California Regional Intelligence Center with companies based in Silicon Valley provided valuable indications necessary to activate the fusion process. From there, the information provided from local companies could be shared among all fusion centers and federal services. This sharing of information speeds up the fusion process and provides information directly from the local environment to the federal intelligence agencies. Information from social media companies is very important because social media is crucial for far-right extremist networks. Because of this, maintaining communication between IFCs and social media companies is essential.

D. CONCLUSION

The information about fusion centers' activities regarding January 6 is limited and insufficient to generate a clear picture of their capabilities and activities during this attack.

[224] Justin Hendrix et al., "Capitol Attack: Federal Agencies' Use of Open Source Data and Related Threat Products Prior to January 6, 2021," 9.

[225] Justin Hendrix, 10–11.

In the future, we will probably have access to additional information about the IC's activities, which will provide a clearer picture of the IFCs' contributions. Even with these limited facts, it is noticeable that the fusion process works, and with the capabilities to gather information from social media, it could provide valuable information to federal intelligence services leading to better decision making.

Far-right extremism is constantly adapting, and we see that the development of new technologies plays a major role in that. Another factor that played an important role for the United States was the interactions between policy rhetoric similar to the ideology of many far-right movements, which make far-right sympathizers to think that they are represented in political life in the United States. These two factors provided power to far-right extremists, and it led to the emergence of a "plethora of groups and ideologies, including armed militias and committed conspiracy theorists, neo-Nazis and isolated anti-government militants with few common denominators beyond hate and propensity for violence."[226]

The steady development of violent far-right extremism led to the ultimate culmination and attack that summarizes all far-right groups and movements: the Capitol insurrection on January 6. The IFCs in the United States showed that they could be productive in fighting against domestic violent extremism by exploiting open-source information collected from social media and collaborating with private companies. Even though the Capitol breach was successful for the far-right groups, the open-source collection from IFCs must be considered more seriously in the future.

[226] Homeland Security Today, "'This Is Our House!' A Preliminary Assessment of the Capitol Hill Siege Participants," Program on Extremism (George Washington University, March 2021), 10, https://www.hstoday.us/subject-matter-areas/counterterrorism/this-is-our-house-a-preliminary-assessment-of-the-capitol-hill-siege-participants/.

IV. THE FAR-RIGHT CONSPIRACY THEORIES AND FUSION CENTERS

Disinformation campaigns and the spreading of conspiracy theories are essential for right-wing movements. According to Kamy Akhavan, the Executive Director of USC Dornsife Center for the Political Future, "conspiracies have been around as long as there have been human beings around. It is a way to explain the unexplainable."[227] After the development of Facebook, Twitter, and YouTube, right-wing extremists received platforms that allowed them to spread propaganda much faster, and this led to the easy radicalization of new recruits. Spreading false information can be very dangerous for society and democracy, especially when false information has been used for the mobilization of extremist groups or for other dangerous political purposes.

Spreading disinformation and conspiracy theories is not illegal according to U.S. laws. On the other hand, we are witnessing more and more examples of the weaponization of disinformation through social media platforms, and the U.S. Intelligence Community (IC) is not able to respond properly. Disinformation campaigns create conspiracy theories leading to division in the United States and the undermining of democracy. Spreading disinformation is a simultaneously federal and local problem, and state intelligence fusion centers (IFCs) have to address this problem in order to be more productive in countering domestic violent extremism (DVE). IFCs, however, need federal institutional support in order to develop better capabilities for disrupting disinformation.

This chapter begins by examining the use of disinformation and the spreading of conspiracy theories by far-right groups. After the development of social media platforms, spreading disinformation became far easier for many far-extremist groups. After that, the chapter examines a model for spreading disinformation by foreign-state actors, particularly through exploiting existing far-right internet platforms. The last part of the chapter explores the government measures taken against disinformation during the 2016 and 2020 elections.

227 *The Surprising Origins of the Modern Conspiracy Theory*, Documentary (BBC Real, 2022), sc. 0:41, https://www.bbc.com/reel/video/p0chchj8/the-surprising-origins-of-the-modern-conspiracy-theory.

It concludes with discussion about the involvement of IFCs in countering disinformation campaigns.

A. FAR-RIGHT EXTREMISM AND THE DIGITAL ENVIRONMENT

Disinformation and conspiracy theories fuel far-right movements' propaganda and grievances, and they often influence lone-wolf actors who are inspired by far-right beliefs to commit hate crimes or deadly attacks. According to a RAND report by Williams et al., "contemporary right-wing extremism–related violence is, in large part, orchestrated and carried out by lone-wolf actors, many of whom are inspired by previous terrorist attacks."[228] Miller-Idriss and Hughes suggest that, far-right movements have been shifting to a post-organization paradigm through the use of online disinformation. The propaganda and extremist ideas disseminated online lead to the radicalization of many nonaffiliated individuals to far-right ideas without participation in any specific organization.[229] Like any other terrorist organization, far-right extremists adapt to the contemporary technologies available to survive and be more successful. In this case, the spread of false messages and ideas, and the possibility of disconnecting people from reality by using disinformation and conspiracy theories, provided a very cheap way to recruit people for the cause even though these people do not participate in any organization officially.

The post-organizational paradigm significantly changes the approach taken by the IC against right-wing extremism. Williams et al. suggest that the post-organizational approach emphasizes the importance of online connections among right-wing extremists.[230] For example, some of the most high-profile attacks in Norway, New Zealand, the United States, and Germany were unaffiliated to any far-right group, but the

---

[228] Heather J. Williams et al., *Mapping White Identity Terrorism and Racially or Ethnically Motivated Violent Extremism: A Social Network Analysis of Online Activity* (Santa Monica, CA: RAND Corporation, 2022), 14, https://doi.org/10.7249/RRA1841-1.

[229] Cynthia Miller-Idriss and Brian Hughes, "Blurry Ideologies and Strange Coalitions: The Evolving Landscape of Domestic Extremism," Lawfare, December 19, 2021, https://www.lawfareblog.com/blurry-ideologies-and-strange-coalitions-evolving-landscape-domestic-extremism.

[230] Williams et al., *Mapping White Identity Terrorism and Racially or Ethnically Motivated Violent Extremism: A Social Network Analysis of Online Activity*, 15.

perpetrators maintained online connections with extreme right-wing networks.[231] The post-organization paradigm also allows for a deeper decentralized mode of operation, which provides the far-right movement more security against infiltration.[232] This evolving transformation to the online environment is possible thanks to the cheap and secure means of communication and digital media that define the supply and demand of ideological content.[233] These factors create additional challenges for intelligence services because the regular method like surveillance used in counterterrorism, are not very suitable here because violent extremists do not maintain many physical connections. Moreover, the U.S. citizen's right to free speech is protected by the U.S. Constitution and security services are restricted from enforcing their full surveillance capabilities.

1. Social Media Effect

In terms of using digital technology, white supremacists could be considered as one of the most proactive of all other far-right groups in utilizing digital means for the purpose of spreading far-right ideology. According to the Southern Poverty Law Center (SPLC), the notorious figure of the radical right, Louis Beam, and two others, were among the first white supremacists who used computers for their propaganda as they created the first white supremacist computer bulletin, the Aryan Nations Liberty Net, in 1984.[234] Another study suggests that at the end of 2000, there were already several hundred white supremacist websites, and that most major extremist organizations had their own website.[235] The authors of the study concluded that the internet compensates the lack of people with similar thinking around the physical proximity of white supremacists, as "the internet has the capacity to facilitate a sense of community for white supremacist in rural….suburbs"[236]

---

231 Williams et al., 15.

232 Williams et al., 16.

233 Miller-Idriss and Hughes, "Blurry Ideologies and Strange Coalitions."

234 "Louis Beam," Southern Poverty Law Center, accessed October 16, 2022, https://www.splcenter.org/fighting-hate/extremist-files/individual/louis-beam.

235 Val Burris, Emery Smith, and Ann Strahm, "White Supremacist Networks on the Internet," *Sociological Focus* 33, no. 2 (2000): 216, https://www.jstor.org.libproxy.nps.edu:2048/stable/20832076.

236 Burris, Smith, and Strahm, 232.

The creation of a cyber white supremacy community has a long tradition. We can conclude that at this time, white supremacists, as one of the most dangerous factions of far-right ideology, had a very innovative approach dictated by their need to create their own community, which was further developed in the twenty-first century.

Access to social media changed the landscape of white supremacy. This change resulted in the decline of some old organizations, like the Klan, that were unable to fully embrace social media. This has led to the rise of other new organizations or figures that had never been known before.[237] A good example of the power of social media for the far-right movements is the Nazi Feuerkrieg Division case from Estonia. When Estonian police organized an intervention against the neo-Nazi Feuerkrieg Division, it turned out that the commander of the group was a 13-years-old boy who used the anonymity of social media platforms on the internet to become the "commander" of the extremist group.[238] This example shows that social media provides a different ecosystem for white supremacists and other extremists that differs from traditional environments. This ecosystem allowed actors hidden behind anonymous profiles to spread their ideas in the form of disinformation and conspiracy theories. The internet also made it easier for extremists to attract followers, which has led to further white supremacy digitalization and the expanded use of disinformation.

White supremacists use social media because they can easily and freely send their messages and maintain their network. According to Byman, before social media, the radicalization of people took face-to-face contact, but especially after 2015, this has changed significantly, and now recruitment needs almost only online interaction.[239] He also suggests that the current digital technologies provide a platform for free to upload propaganda videos or manifestos, secure communications with sympathizers, and the

[237] Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism*, 101.

[238] Colin Drury, "'Commander' of Feuerkrieg Far-Right Terror Group Unmasked by Police as 13-Year-Old Boy," *The Independent*, April 30, 2020, https://www.independent.co.uk/news/world/europe/far-right-terror-group-commander-teenage-boy-fire-war-division-estonia-a9460526.html.

[239] Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism*, 105.

ability to build organizational networks.[240] For example, white supremacist followers of James Masons' ideology which advocating violence against the minority and neo-Nazi cult, created social media accounts dedicated to his book *Siege* on Facebook, Twitter, YouTube, and another platform named Gab.[241] Another example is the far-right conspiracy theory movement known as "QAnon," which started its development on the 8chan platform. QAnon gained so much popularity among President Trump's supporters that it had several representatives running for office.[242]

Another benefit of free and secure social media platforms extremists use is that they provide access to shape their own narratives by inventing and spreading false or misleading information. For instance, in 2020, white supremacists framed a Black Lives Matter peaceful protest in Harrison, Arkansas, as a left-wing violence protest intending to "burn Harrison to the ground."[243] White supremacists maintained a Twitter account with the misleading name "@Antifa-US," where they posted information on May 31 2020, that "tonight's the night … we move into the residential areas … the white hoods … and we take what's ours."[244] Such methods aiming to create a narrative that the far-right is attacked by the far-left or sparking tensions in peaceful protest against the right-wing is commonly used by right-wing extremism. The main goal is to create violence and that violence is to be exploited as propaganda for their supporters. This tactic would be less successful without fairly free and unrestricted social media platforms.

The white supremacist communication strategy can be divided into two stages. The first stage is built on spreading disinformation and propaganda on open websites and social media channels, where the intention is to feed their supporters and attract new recruits with

---

[240] Byman, 101.

[241] "James Mason's Siege: Ties to Extremists," Counter Extremism Project, accessed October 18, 2022, https://www.counterextremism.com/james-masons-siege-ties-to-extremists.

[242] Charles Levinson, "With Super PAC, QAnon's Con Chases Mainstream — and Money," Protocol, March 3, 2020, https://www.protocol.com/qanon-conspiracy-new-super-pac.

[243] Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism*, 102.

[244] Nicholas Kristof, "When Antifa Hysteria Sweeps America," *The New York Times*, June 17, 2020, sec. Opinion, https://www.nytimes.com/2020/06/17/opinion/antifa-protests.html.

more moderate propaganda.[245] White supremacists use more open platforms like Facebook and Twitter, because in this way the propaganda achieves wider coverage in mainstream audiences. Extremists use cheerful propaganda like humor and satire to reach more people because these conventional platforms use content moderation.[246] The aim is to get the attention of more people who may then be redirected to more closed and unrestricted platforms. The second stage of communication strategy follows the redirection to secure channels. In this stage, new recruits are exposed to more radical content using hate speech, videos, and conspiracy theories. According to Williams et al., the less-conventional platforms used by right-wing extremists, such as Telegram, Gab, and 8Chan, are preferred "to avoid restrictions on hate speech and carry on discussing and disseminating various conspiracy theories, posting content, spreading false narratives, and raising money."[247]

Among non-conventional social media platforms, Telegram is one of the most important for violent extremists. According to Megan Squire, the technical features of Telegram have converted the app into the "perfect hybrid tool for hate."[248] She underlines two main features that are of great importance for many violent extremists. First, in the application, a user can create a group or channel that can contain 200,000 users. Second, Telegram allows one-way communication from the channel's owner to the channel's followers.[249] Recently, new features have been added that facilitate even more dangerous actions from radical groups. For example, file storage capability can be used for literature, instructions, manuals, and propaganda videos storage; Telegram channels can be operated by humans and software; and it provides a very slow process for reporting extremist content

[245] Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism*, 104.

[246] Williams et al., *Mapping White Identity Terrorism and Racially or Ethnically Motivated Violent Extremism: A Social Network Analysis of Online Activity*, 21.

[247] Williams et al., 21.

[248] Megan Squire, "Alt-Tech & the Radical Right, Part 3: Why Do Hate Groups and Terrorists Love Telegram?," Center for Analysis of the Radical Right Analysis, 2020, https://www.radicalrightanalysis.com/2020/02/23/alt-tech-the-radical-right-part-3-why-do-hate-groups-and-terrorists-love-telegram/.

[249] Squire.

and channels.[250] Another important characteristic is that the company heavily advocates free speech rights. The company advertises itself as a secure space for free speech, and resists government cooperation in terms of banning content or channels.[251] All these useful features convert Telegram into an encrypted "loudspeaker" of propaganda that securely hosts all necessary information and communications for extremist groups.

2. Conspiracy Theories, Lies, and Disinformation Spreading into the Homeland

Conspiracy theories and disinformation are an important part of the far-right extremists' propaganda. According to Gregory Rousis et al., who concentrated their research on terrorist organizations such as ISIS, Al Qaida, and Neo-Nazi groups, they figured out that "groups that seek to achieve their goals using violence tend to use more conspiracy theories than those that advocate political action."[252] Still, it is unknown whether extremist groups use conspiracy theories only to recruit new members and sustain the old ones or if the conspiracy theories are the reason for violence. The importance of this question is that targeting far-right conspiracy theorists and disinformation sources could be a useful strategy that could lead to containing the violence.

The recruitment of new members is very important for extremist organizations. There are different methods for recruitment, and every extremist group chooses methods based on availability and suitability. Conspiracy theories are used by almost the entire spectrum of ideological extremist organizations. According to Jamie Bartlett and Carl Miller, for the far-right groups, "the concept of Zionist Occupied Government – that a small cabal of Jews controls world governments—is central to both ideology and

[250] Squire.

[251] Hannah Gais and Megan Squire, "How an Encrypted Messaging Platform Is Changing Extremist Movements," Southern Poverty Law Center, accessed October 19, 2022, https://www.splcenter.org/news/2021/02/16/how-encrypted-messaging-platform-changing-extremist-movements.

[252] Gregory J. Rousis, F. Dan Richard, and Dong-Yuan Debbie Wang, "The Truth Is Out There: The Prevalence of Conspiracy Theory Use by Radical Violent Extremist Organizations," *Terrorism and Political Violence*, November 19, 2020, 13, https://doi.org/10.1080/09546553.2020.1835654.

propaganda."[253] This theory is universal for many far-right movements because it involves well-known enemies of the far-right identity, the Jews, and it creates the perception of a direct threat.[254] Different studies suggest that almost half of all American citizens consider at least one conspiracy theory as true, and trying to change the minds of these individuals is very hard.[255] Another important fact is that there are many different conspiracy theories that find cross-sectional overlap in believers, and it is often possible to observe people from different ideological spectrums who believe in similar theories.[256] One of the reasons far-right extremists exploit conspiracy theories is because they provide a huge pool of believers that could be recruited and controlled easily. Most people among the far-right do not participate in an organization, but instead support the ideas of the movement. The support very often means sharing ideas and propaganda, likes, trolling, and other virtual support.

The conspiracy theories serve to organize extremist groups and indirectly push them toward more extreme activities. According to Bartlett and Miller, this is happening in three ways:

> First, conspiracy theories create demonologies of 'the other' or 'the enemy' that the group defines itself against. Second, they delegitimize voices of dissent and moderation by casting them as part of the conspiracy. Finally, they can encourage a group to turn to violence, acting as rhetorical devices to portray violence, both to the group itself and their wider supporters, as necessary to 'awaken' the people from their acquiescent slumber.[257]

Conspiracy theories and disinformation are essential parts of mainstreaming far-right ideas. According to Miller-Idriss, mainstreaming of the far-right in a democratic society happens when an extreme idea becomes more acceptable than before.[258] She

---

253 Jamie Bartlett and Carl Miller, *The Power of Unreason: Conspiracy Theories, Extremism and Counter-Terrorism* (London: Demos, 2010), 3, https://www.demos.co.uk/files/Conspiracy_theories_paper.pdf?1282913891.

254 Rousis, Richard, and Wang, "The Truth Is Out There," 14.

255 Rousis, Richard, and Wang, 2.

256 Bartlett and Miller, *The Power of Unreason: Conspiracy Theories, Extremism and Counter-Terrorism*, 4.

257 Bartlett and Miller, 5.

258 Miller-Idriss, *Hate in the Homeland: The New Global Far Right.*, 46.

argues that mainstreaming is essential for the far-right because it is directly connected with the growth of the movement and diminishes the probability of a negative public response because the public is used to the far-right ideology.[259] She claims that conspiracy theories entering mainstream society creates a moral obligation to act against the clear and distinguished enemy, and it becomes perceived that a lack of action against this enemy is wrong.[260] An example of the effect of such moral obligation is the attack on the Washington Comet Ping Pong pizza restaurant by a 28-years old father of two, who was influenced by a conspiracy theory about a pizza restaurant that is used by a child-abuse ring orchestrated by Hillary Clinton.[261] Mainstreaming far-right ideology increases the possibilities of lone-wolf attacks, and it makes predicting and preventing violent attacks harder. It also provides favorable conditions for manipulators to influence certain social groups into committing actions that damage society and democracy. Maintaining an informed society, competing ideas, and a willingness to compromise are all key factors for democracy, and the act of spreading disinformation creates unfavorable conditions for the health of said democracy.[262]

B. HOW DO THE DISINFORMATION CAMPAIGNS WORK, AND WHERE CAN IFCS HELP?

There are a variety of disinformation campaigns, and their characteristics mainly depend on factors like motivation and attribution of the threat actor. Understanding the motives behind the campaign is important in order to build a proper strategy to counter it. According to a DHS report about countering disinformation campaigns, the motives usually are financial, political, ideological, legal, or a combination.[263] For example, far-

[259] Miller-Idriss, 46.

[260] Miller-Idriss, 55.

[261] Cecilia Kang and Adam Goldman, "In Washington Pizzeria Attack, Fake News Brought Real Guns," *The New York Times*, December 5, 2016, sec. Business, https://www.nytimes.com/2016/12/05/business/media/comet-ping-pong-pizza-shooting-fake-news-consequences.html.

[262] The Public-Private Analytic Exchange Program, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue Part Two," 10.

[263] The Public-Private Analytic Exchange Program, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 11, https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

right propaganda falls under ideological causes, but often the ideological causes are paired along with financial motives. Attribution is also important in understanding the intent of the actor, but it is almost always very difficult. Disinformation campaigns can be created domestically or in foreign countries. According to the DHS report, the location of the disinformation's initial creation leads to the campaign's intention.[264] For example, a campaign originating in Mississippi is most likely targeting racial tensions, and such a campaign will have different aspects involved compared to a campaign started in Russia. A campaign started in Russia, on the other hand, targets far-right groups in order to create dislike for political figures, and an example would be propaganda targeting Hilary Clinton during the 2016 election. Also, disinformation campaigns can be state or non-state sponsored. The DHS report suggests that state-sponsored campaigns possess more resources, and the response against them falls under national security matters and international relations. Contrary to this, non-state sponsored campaigns possess fewer resources to operate, but are addressed by the more limited criminal justice department.[265]

It is also important to distinguish between the different actors involved in spreading disinformation. According to the DHS, actors supporting disinformation campaigns could be witting or unwitting.[266] Unwitting actors are far-right people who spread anti-Democratic propaganda that originated in Russia without knowing that, by this way, they support the goals of the foreign state against their own. Unwitting actors are the resource that foreign states rely on and need in order to spread disinformation. Such people in the United States could be far-right groups because they believe heavily in conspiracy theories, and their ideology is continuously fueled by disinformation, and they are more likely to respond to and to share the disinformation.

264 The Public-Private Analytic Exchange Program, 14.

265 The Public-Private Analytic Exchange Program, 14.

266 Kate Starbird, "Disinformation's Spread: Bots, Trolls and All of Us," *Nature* 571, no. 7766 (July 2019): 14, https://doi.org/10.1038/d41586-019-02235-x.

1. Disinformation Kill Chain Model

The disinformation kill chain model is presented by DHS officials, and it explains how a disinformation campaign works. This model is based on the cyber kill chain model developed by Lockheed Martin.[267] The disinformation kill chain model presented in Figure 3, describes the steps that the threat actors follow in order to conduct a disinformation campaign, and it could be applied to foreign and domestic actors.[268]

Figure 3. Disinformation kill chain model.[269]

The beginning of a disinformation campaign starts with the creation of an objective or end state such as changing public opinion on a specific topic.[270] Examples for that could be making far-right ideas mainstream, promoting an anti-government narrative, or shifting public opinion toward a specific presidential candidate during an election campaign. According to the DHS report, after an objective is set, the campaign usually follows these steps:

[267] The Public-Private Analytic Exchange Program, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 15.

[268] The Public-Private Analytic Exchange Program, 15.

[269] Source: The Public-Private Analytic Exchange Program, 16.

[270] Starbird, "Disinformation's Spread," 16.

1. Reconnaissance: This phase analyzes the target audience and the environment, based on the preparation of the campaign plan.

2. Build: This phase includes assembling of campaign infrastructures like computing assets and staff, the creation of accounts, the preparation of bots, and establishing the necessary websites.

3. Seeds: The initial misleading products or materials that will serve as the original source must be developed; then through online forums and social media that content needs to be delivered to the initial seeds locations.

4. Copy: This phase includes developing many supporting materials that refer to the original source, including written articles, blogs, posts on social media, and other items that spread the main idea.

5. Amplify: This phase includes the use of bots and inauthentic accounts, and the idea is to accelerate the spreading of the story to the targeted audience's communication channels. The spreading of the information happens not only through software but also by witting and unwitting agents. The main purpose of this phase is to push misleading ideas into the mainstream media.

6. Control: This includes manipulation of the audience by creating discussion about the content aiming to inspire conflict or to align the argument.

7. Effects: This phase evaluates the desired effects and the behavior of the targeted group.[271]

2. Case Study—Seth Rich Murder

Seth Rich was low-level employee in the Democratic Party of the United States. On 10 July 2016, he was walking on the way to his home when he was shot dead by an

[271] The Public-Private Analytic Exchange Program, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 16.

unknown perpetrator.[272] The case remains open because the Washington police suspected it was a street robbery that ended wrong and never found any suspect.[273] Soon after Rich died, WikiLeaks published thousands of emails of Democratic National Committee representatives obtained by an anonymous source, which caused turmoil in the U.S. presidential election.[274] In a Dutch TV interview, Julian Assange, the WikiLeaks owner, refused to say precisely how he got the Democratic National Committee representatives emails or who his source was, but he dropped a tip saying that "there's a 27-year-old who works for the Democratic National Committee representatives who was shot in the back, murdered, just a few weeks ago, for unknown reasons as he was walking down the street in Washington."[275] After this interview, the conspiracy theory about Rich being murdered for political reasons went viral and made its way to the mainstream media after that.

This case study is an example of a state-sponsored disinformation campaign about spreading a conspiracy theory in the U.S. population. The following information connects with spreading disinformation in the United States. The case examines how the murder of Seth Rich was exploited by Russian Foreign Intelligence Services (SVR) in order to cast doubts against one of the major political parties in the United States and to redirect the suspicions away from Russia's involvement in leaked Democratic National Committee emails in WikiLeaks. The narrative of this campaign is that Seth Rich was the WikiLeaks' source; he was planning to reveal the information about violations committed by Hillary Clinton, and because of that Clinton had ordered Rich's assassination.[276] Table 1 illustrates the steps used by Russian Intelligence to spread disinformation about Seth Rich's case.

---

[272] Charlie Mole, "Seth Rich: How a Young Man's Murder Attracted Conspiracy Theories," *BBC News*, April 21, 2018, sec. BBC Trending, https://www.bbc.com/news/blogs-trending-43727858.

[273] Mole.

[274] Andy Kroll, "Will Julian Assange and WikiLeaks Finally Tell the Truth About Seth Rich?," *Rolling Stone* (blog), November 26, 2019, https://www.rollingstone.com/politics/politics-news/will-julian-assange-and-wikileaks-finally-tell-the-truth-about-seth-rich-918946/.

[275] Kroll.

[276] Michael Isikoff, "Exclusive: The True Origins of the Seth Rich Conspiracy Theory. A Yahoo News Investigation.," Yahoo News, July 2019, https://news.yahoo.com/exclusive-the-true-origins-of-the-seth-rich-conspiracy-a-yahoo-news-investigation-100000831.html.

Table 1. Application of disinformation kill chain model.[277]

DISINFORMATION KILL CHIN MODEL—Seth Rich Murder			
PHASE	**PRIMARY SOURCE**	**DESCRIPTION**	**ACTORS**
Seed	SVR bulletin; whatdoesitmean.com	Three days after the murder, SVR circulated a fictitious intel report about the assassination, using a website known as a frequent vehicle for Russian propaganda, citing SVR in an article asserting that Rich was killed by Clinton's kill squad.[278]	threat actor
Copy	Reddit; 4Chan; Twitter; RT; Sputnik; Facebook	Sputnik and RT start spreading the story;[279] meanwhile in the United States, Rich conspiracy stories started being posted on Reddit, 4Chan, and other far-right platforms on Twitter and Facebook, but not exclusively.[280]	threat actor; witting agents; unwitting agents
Amplify	Twitter; Facebook; YouTube; Infowars; America First Media; Fox News	IRA bots repost the story; witting and unwitting agents retweet it; far-right websites aggressively push the story; the story goes viral on mainstream through far-right affiliated media Fox News and America First Media.[281]	threat actor (bots); witting agents; unwitting agents
Control	Twitter comments; Fox News; YouTube; far-right sites; RT; Sputnik	Bots and trolls start posting in order to spark division; Julian Assange suggests Seth Rich was the source for Wikileaks; Fox News continues to spread the story; After Yahoo News revelation about Russian origins for the story, a new counternarrative begins circulation.[282]	Threat actor (bots, trolls); witting agents; unwitting agents

277 Adapted from: The Public-Private Analytic Exchange Program, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 21.

278 Isikoff, "Exclusive: The True Origins of the Seth Rich Conspiracy Theory."

279 Isikoff.

280 Mole, "Seth Rich."

281 Isikoff, "Exclusive: The True Origins of the Seth Rich Conspiracy Theory."

282 Isikoff.

As Table 1 shows, the disinformation campaign was well- orchestrated by the Russian Foreign Intelligence Service. This operation could not have achieved the same magnitude without the involvement and unwitting support of far-right sympathizers. From the information provided by Yahoo News, it is noticeable that immediately after the SVR bulletin, the far-right social media groups and websites connected with spreading far-right propaganda began spreading the story. Foreign state disinformation campaigns are so successful because there is an existing and fertile environment that helps spread conspiracy theories. Far-right movements use conspiracy theories for recruitment and their target audiences and members tend to believe and respond to such news more readily than most typical American citizens. Therefore, by exploiting the willingness of far-right social media groups, Telegram's channels, and some television programs to share conspiracy theories, foreign intelligence services possess easy access to American mainstream media.

Audiences of far-right media outlets are more receptive to conspiracy theories and thus are often objects of disinformation campaigns, and this problem hasto be addressed more seriously by the U.S. authorities. According to Larry Luxner, after the U.S. presidential election in 2016 and the outbreak of the Covid 19 pandemic, the focus shifted from foreign to domestic actors that spread disinformation.[283] Richard Stengel suggests that the spreading of disinformation by domestic actors is more dangerous than such campaigns organized by foreign-state actors.[284] Moreover, disinformation campaigns will not disappear. This is not a problem that can be permanently solved; rather, it should be thought of as a problem that can be treated.[285] Disinformation in the United States is not only coming from foreign state actors. It also comes from domestic far-left and far-right groups. There are many examples of disinformation campaigns with economic goals, too. However, many researchers suggest that far-right groups are more likely to share

[283] Larry Luxner, "Ahead of the 2020 U.S. Elections, the Disinformation Threat Is More Domestic than Foreign," *Atlantic Council* (blog), September 23, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/ahead-of-the-2020-us-elections-the-disinformation-threat-is-more-domestic-than-foreign/.

[284] Richard Stengel, "We Should Be as Worried About Domestic Disinformation as We Are About International Campaigns," *Time*, accessed October 21, 2022, https://time.com/5860215/domestic-disinformation-growing-menace-america/.

[285] The Public-Private Analytic Exchange Program, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue Part Two," 6.

conspiracy theories and fake news than other groups.[286] The danger coming from the far-right disinformation is that there is a convenient overlapping with the agendas between far-right groups, such as anti-government groups, and foreign state actors, which endangers democracy and national security. This contemporary problem is very broad, and it needs a comprehensive approach to solving it.

C. GOVERNMENT RESPONSE TO DISINFORMATION CAMPAIGNS AND THE ROLE OF THE IFCS

The Intelligence Fusion Centers' participation in countering disinformation is not well coordinated, and their involvement is not clear. Disinformation campaigns are a complex problem due to the rapid development of social media, the ability of users to shift from one platform to another, and the huge amount of information available on the internet.[287] This complexity needs a multiagency approach, which means that IFCs could participate more seriously in this problem. Creating conditions that restrict the spread of disinformation in general will also decrease the spread far-right disinformation, which will indirectly weaken right-wing extremism and its influence on U.S. citizens.

Fighting against disinformation campaigns is another approach to mitigating the effects of DVE. Creating an environment with a lower supply and demand for disinformation is essential for stifling far-right extremism. This can happen when information consumers increase their ability to distinguish facts from fiction.[288] The role of IFCs in this struggle seems blurry because this problem is encountered and has to be addressed on a federal level, mainly by the FBI and by private companies. Most IFCs are all-hazards oriented, and they engage in a variety of state and local problems; hence, they could support countering disinformation campaigns, too. While reducing the supply of disinformation is largely a federal responsibility, the IFCs could address the demand part. They can use their ability to share information from federal agencies to local services,

[286] Stengel, "We Should Be as Worried About Domestic Disinformation as We Are About International Campaigns."

[287] The Public-Private Analytic Exchange Program, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," 21.

[288] The Public-Private Analytic Exchange Program, 21.

partners, and institutions in order to better educate local structures and communities about disinformation campaigns and, in this way, decrease the demand side of disinformation campaigns.

1. Lessons Learned from U.S. Elections

The 2016 U.S. presidential election showed how unprepared the U.S. government and private companies were to protect the American people from the effects of disinformation campaigns on social media. According to Molly Montgomery, "the 2016 U.S. presidential election … and potential effects of Russian disinformation on U.S. democratic institutions provided an important wake-up call for [social media] platforms."[289] Since 2013 the Russian Internet Research Agency had employed social media platforms in order to conduct a disinformation campaign aiming to affect the 2016 U.S elections.[290] According to Elvis Chan, the Internet Research Agency utilized three lines of effort before the 2016 presidential campaign in order to influence the American public during the election.[291] First, many fake social media accounts and pages addressing a variety of political subjects were created and operated by the Internet Research Agency.[292] Second, to boost already existing information, Internet Research Agency workers deployed social media bots or computer programs that managed social media accounts.[293] Third, to improve their organic content and increase internet traffic to their websites, Internet Research Agency workers secretly bought online advertisements from social media firms.[294] According to Philip Howard, the goal of this disinformation campaign was to encourage extreme right-wing voters to support Trump and to make left-

[289] Molly Montgomery, "Disinformation as a Wicked Problem: Why We Need Co-Regulatory Frameworks," Brookings, 2020, 5, https://www.brookings.edu/research/disinformation-as-a-wicked-problem-why-we-need-co-regulatory-frameworks/.

[290] Elvis M. Chan, "Fighting Bears and Trolls: An Analysis of Social Media Companies and U.S. Government Efforts to Combat Russian Influence Campaigns During the 2020 U.S. Elections" (master's thesis, Naval Postgraduate School, 2021), 29, https://calhoun.nps.edu/handle/10945/68309.

[291] Chan, 30.

[292] Chan, 30.

[293] Chan, 30.

[294] Chan, 30.

wing people not vote by "spreading sensationalist, conspiratorial, and other forms of junk political news and misinformation."[295] The far-right groups were the main target audience, as evidenced by more than half of the Russian fake accounts leveraging topics connected with race, ethnicity, and self-identity.[296]

The conclusion from the 2016 elections was that Russia executed a disinformation campaign on U.S. soil, inflicting arguably some divisions in U.S. society. According to Chan, the Internet Research Agency had almost unrestricted access to social media platforms, and American security services and private companies were unable to detect and deter the Russian disinformation campaign.[297] One of the major factors that allowed the Internet Research Agency to have such success was social media platforms' inability to detect from the start that their platforms were being used for a disinformation campaign.[298] From there, communication with federal services was not present, and the government's response also was dissatisfactory.

During the 2020 presidential campaign, the tactics of the Research Internet Agency changed a little but remained active. About Russian tactics during the 2020 elections, Chan concluded that the Internet Research Agency continued "using alternative communication platforms, artificial intelligence to generate false personas, and unwitting agents co-opted to avoid detection by the social media companies and the U.S. government."[299] In order to influence voters' attitudes, they used proxy organizations like Eliminating Barriers for the Liberation of Africa to deal with racial issues such as "police brutality, displays of anger towards white people, and black empowerment."[300] The Internet Research Agency

295 Philip N. Howard et al., "The IRA, Social Media and Political Polarization in the United States, 2012–2018," Propaganda Computational Research Project, Oxford University, 2018, 3, https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

296 Chan, "Fighting Bears and Trolls: An Analysis of Social Media Companies and U.S. Government Efforts to Combat Russian Influence Campaigns During the 2020 U.S. Elections," 32.

297 Chan, 55.

298 Chan, 55.

299 Chan, 63.

300 Chan, 59.

continued targeting far-right groups primarily using social media platforms, but they also used right-wing dedicated platforms like Gab and Parler.[301]

The U.S. government's response to Russian attempts to influence public opinion during the 2020 presidential campaign was more robust than it was in the 2016 election. Gabriel Cederberg et al. concluded that there are three possible types of measures for fighting against disinformation: security, transparency, and resiliency.[302] The security measures include "prevention of disinformation or data breaches, deterrence of damaging actions or operations, and punishment of criminal or other harmful actions."[303] Transparency measures include building trust and confidence in official institutions by sharing necessary information with society.[304] Finally, resiliency measures are intended to build the public's ability to recognize disinformation and ignore it.[305] According to Chan, the collaboration between the FBI with the relevant social media companies, which led to the shutting down of many troll accounts, played a key role for securing the 2020 election.[306] The FBI also provided cyber security training to national-level political parties and presidential campaign personnel. The FBI, along with the Department of Homeland Security and the Director of National Intelligence, initiated Protected Voices Initiatives, which provided online resources that "explain the nature of foreign influence and social engineering, highlight common areas of vulnerability, and offer cybersecurity measures to help campaigns, companies, and individuals protect themselves against common Internet-

301 Graphika Team, *Step Into My Parler; Suspected Russian Operation Targeted Far-Right American Users on Platforms Including Gab and Parler, Resembled Recent IRA-Linked Operation That Targeted Progressives* (New York: Graphica, 2020), 16, https://graphika.com/reports/step-into-my-parler/.

302 Gabriel Cederberg et al., *National Counter-Information Operations Strategy* (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2019), https://www.belfercenter.org/publication/national-counter-information-operations-strategy.

303 Chan, "Fighting Bears and Trolls: An Analysis of Social Media Companies and U.S. Government Efforts to Combat Russian Influence Campaigns During the 2020 U.S. Elections," 95.

304 Gabriel Cederberg et al., *National Counter-Information Operations Strategy*, 12.

305 Cederberg et al., 17.

306 Chan, "Fighting Bears and Trolls: An Analysis of Social Media Companies and U.S. Government Efforts to Combat Russian Influence Campaigns During the 2020 U.S. Elections," 86.

enabled crimes."[307] The collaboration between the FBI and the NSA to combat cybersecurity threats by Drovorub malware, the most advanced cyber weapon of Russia, provided additional support to the election organization to better prepare against it.[308]

Other federal organizations were involved in protecting the elections. The Cyber and Infrastructure Security Agency, established within the Department of Homeland Security, also supported election protection. The agency established an Elections Interference Information Sharing and Analysis Center to work with election officials and security officers to improve the overall cybersecurity posture of state, local, and government organizations.[309] U.S. Cyber Command was also involved by training National Guard cyber operators on how to provide support to state and local officials in stopping any interference.[310]

Overall, the government's response to securing the 2020 elections appeared adequate, and there is evidence that the government utilized most federal capabilities in order to block foreign disinformation campaigns. Nevertheless, according to Chan, during the 2020 elections, the U.S. government and social media companies concentrated their efforts only on security and transparency measures and did not do much for public resilience, which is most crucial in the long term.[311] Due to the First Amendment, which obliges the government not to interfere with freedom of speech, and the Fourth Amendment, which stipulates privacy rights, the approach to combating disinformation is constrained. This is especially true when trying to counter the spread of disinformation by

307 "Protecting Every Voice: FBI Expands Resources on Election Security," Homeland Security Today, October 23, 2019, https://www.hstoday.us/subject-matter-areas/cybersecurity/protecting-every-voice-fbi-expands-suite-of-resources-on-election-security/.

308 Dan Goodin, "NSA and FBI Warn That New Linux Malware Threatens National Security," Ars Technica, August 13, 2020, https://arstechnica.com/information-technology/2020/08/nsa-and-fbi-warn-that-new-linux-malware-threatens-national-security/.

309 "Elections Infrastructure Information Sharing & Analysis Center," Center for Information Security, accessed October 30, 2022, https://www.cisecurity.org/ei-isac/.

310 Terry L. Thompson, "No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions," *Georgetown Journal of International Affairs* 21, no. 1 (2020): 183, https://doi.org/10.1353/gia.2020.0033.

311 Chan, "Fighting Bears and Trolls: An Analysis of Social Media Companies and U.S. Government Efforts to Combat Russian Influence Campaigns During the 2020 U.S. Elections," 94.

far-right extremists, who are American citizens; the security measures that were used against foreign state actors are not fully applicable against domestic actors. This narrows the window of opportunity. Building a society that resists fake news and conspiracy theories is essential for democracy. The federal government has a major role in countering foreign disinformation, but this problem must also be addressed by local institutions. The IFCs must support federal efforts in countering disinformation, but they need federal support in doing so.

2. The Role of IFC in Countering Disinformation

IFCs are in a difficult position to counter disinformation. According to Montgomery, the pernicious character of disinformation needs a "multi-stakeholder approach that requires governments and platforms to increase collaboration among themselves."[312] The IFCs, as part of state and local institutions, know their area of responsibilities better and could also be part of this multi-stakeholder approach. Toward this goal, they must be supported by the federal government. In 2015, a Cyber Integration for Fusion Centers Appendix to the *Baseline Capabilities for State and Major Urban Area Fusion Centers* was published. This document "identifies recommended actions and guidance for state and major urban area fusion centers to integrate information technology, cybercrime prevention intelligence and analytic capabilities."[313] This document does not automatically create new capabilities for the fusion centers, and it serves only as guidance for those who are willing to develop cyber capabilities.[314] Developing cyber capabilities is essential for fusion centers to better contribute to the countering of disinformation campaigns. Yet not every state will provide additional finances for these capabilities for their fusion centers. Therefore, the federal government should provide funds and efforts to

[312] Montgomery, "Disinformation as a Wicked Problem: Why We Need Co-Regulatory Frameworks," 1.

[313] The Global Advisory Committee, "Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers" (Global Justice Information Sharing Initiative, 2015), 1, https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/cyber_integration_for_fusion_centers.pdf.

[314] The Global Advisory Committee, 1.

develop all fusion centers equally, to ensure consistent and continuous coverage across the United States.

The IFCs need to be better integrated to counter the disinformation fight. Cederberg et al. recommend the creation of "an interagency fusion cell to combat IO [information operations] modeled on the National Counter Terrorism Center."[315] This center would provide better coordination among the government, federal agencies, the private sector, and state and local fusion centers.[316] Moreover, this model is essential because it can provide state and local fusion centers with better integration and would provide more opportunities for support against disinformation. This step would be inclusive for local fusion centers, integrating their role in sharing intelligence analysis with federal services and receiving intelligence about disinformation trends and methods from the federal services.

U.S. decision makers appreciate the idea of such a center. However, its implementation has created much debate, and to date, such a center is not functioning. According to Nomaan Merchant, the creation of an intelligence center targeting foreign influence was approved by Congress in 2019, and the Office of the Director of National Intelligence was ordered to create it.[317] Three years later, the debates around its creation are still ongoing. According to Merchant, one of the important questions hindering the center's implementation is who will be in charge of the center. Furthermore, previous history of federal services spying on U.S. citizens raises the concerns that after the establishment of such a center, it could be used politically, or it could violate citizens' First Amendment rights. These are among the concerns that constrain the rapid creation of such a center.[318] Nevertheless, creation of such a center is essential because it will provide better

315 Gabriel Cederberg et al., *National Counter-Information Operations Strategy*, 16.

316 Cederberg et al., 16.

317 Nomaan Merchant, "US Delays Intelligence Center Targeting Foreign Influence," U.S. *News & World Report*, accessed October 14, 2022, //www.usnews.com/news/politics/articles/2021-12-23/us-delays-intelligence-center-targeting-foreign-influence.

318 Merchant.

coordination and connections between federal security services and state intelligence fusion centers.

Building resilience in the American public is also essential for decreasing the negative effects of disinformation. When local communities are informed and aware of disinformation campaigns in general, they will become more skeptical of the far-right groups' fake information and propaganda. The IFCs are in a convenient position to support these disinformation countermeasures because their focus is on local communities; they maintain close connections and collaboration with state and local structures; their reach to the local communities is easier than federal institutions, and they know better the local atmosphere. However, they need support from the federal government in order to be successful.

Through IFCs, state and local institutions and communities can be informed and knowledgeable about disinformation campaigns. The IFCs could identify trends in ongoing disinformation campaigns circulating in the digital environment. According to the Department of Homeland Security, an effective approach against disinformation is "building resilience to disinformation narratives by raising awareness of the threat and of techniques to reenforce digital literacy."[319] For example, Cybersecurity and Infrastructure Security Agency, which "leads the national effort to understand, manage, and reduce risk to [the U.S.] cyber and physical infrastructure,"[320] started an informational campaign explaining how to recognize disinformation and how disinformation takes advantage from users' attention.[321] Similarly, DHS started promoting digital literacy among other federal institutions.[322] IFCs could be helpful in fostering digital literacy in local communities, and more specifically, among those at greater risk to being exposed to disinformation

319 Jamie Gorelick and Michael Chertoff, *Final Report from Disinformation Best Practices and Safeguards Subcommittee* (Washington, DC: Homeland Security Advisory Council, Department of Homeland Security, August 24, 2022), 11, https://www.dhs.gov/homeland-security-advisory-council.

320 "About CISA," Cybersecurity and Infrastructure Security Agency, accessed November 2, 2022, https://www.cisa.gov/about-cisa.

321 Gorelick and Chertoff, *Final Report from Disinformation Best Practices and Safeguards Committee*, 11.

322 Gorelick and Chertoff, 11.

campaigns. For example, towns like Harrison, Arkansas, are at greater risk because they are known as being home to white supremacists, where far-right narratives are readily received.[323] The fusion center efforts in Arkansas need to be more robust in Harrison than in towns where far-right narratives are not appreciated or are even rejected. Having local connections and an understanding of the environment can help fusion centers better guide the federal efforts toward groups at higher risk of being targeted by disinformation campaigns.

The IFCs could support the Office of Intelligence and Analysis under DHS in connecting the dots. Through the fusion process, the IFCs can identify the possible spread of disinformation narratives from domestic extremists in their area of responsibility. In this way, the Office of Intelligence and Analysis will have a clearer understanding of the different levels of disinformation narratives being spread in the United States. After the intelligence reports are completed by federal intelligence services, the IFC could share these reports with state, local, tribal, and territorial institutions and, in this way, the IFCs can facilitate "building resilience to disinformation narratives"[324] within state and local communities.

D. CONCLUSION

Containing the spread of disinformation in a democratic state is a challenging endeavor. This problem involves not only physical communities and groups but also the digital environment. These characteristics require a solution built around a multi-stakeholder approach which involves the federal services and the IFCs. The involvement of the IFCs in these challenges needs more federal support for developing and upgrading the centers so they can meet the requirements for addressing cyber threats. In order to be more effective, these cyber capabilities need to be developed consistently in all states, which points to the need for federal support.

[323] Byman, *Spreading Hate: The Global Rise of White Supremacist Terrorism*, 102.

[324] Gorelick and Chertoff, *Final Report from Disinformation Best Practices and Safeguards Subcommittee*, 11.

Far-right disinformation campaigns and conspiracy theories aim to create grievances. The proliferation and persistence of such narrative can ultimately radicalize people and drive them to take violent action. Disinformation is used by far-right groups for recruiting new supporters and keeping these supporters involved. Such groups are a potential danger for "smuggling" foreign state-sponsored disinformation campaigns into the United States and endangering democracy. By fully engaging IFCs in the effort to prevent the spread of disinformation, the United States will increase its capabilities to fight this threat.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

After 9/11, the intelligence structure in the U.S. homeland changed significantly. This change led to the development of a network of intelligence fusion centers intended to support the Intelligence Community's efforts to tackle contemporary challenges threatening U.S. national security. Domestic violent extremism is an increasingly challenging threat, especially in the social media era. The Biden administration acknowledges the pernicious problem of domestic violent extremism, and in the newly published National Security Strategy in October 2022, this problem is addressed.[325] The strategy emphasizes the importance of federal agencies sharing information with state, local, territorial, and tribal partners on domestic violent extremist threats.[326] The strategy also recognizes the problem of disinformation and misinformation coming from social media platforms that can create extreme divisions in society, can fuel people's grievances, and on some occasions, can spark violence.[327] Meanwhile, government responses to these threats need to be addressed properly by protecting the democratic principles and civil rights and liberties.

This thesis has analyzed the role of the National Network of Fusion Centers in the protection of U.S. homeland security and how they can support the efforts of the other federal and state security services in countering domestic violent extremism. The threat from domestic violent extremism in the United States is coming mainly from far-left and far-right movements. This thesis has focused only on domestic violent extremism coming primarily from right-wing extremists because the far-right is more organized than the far-left, and statistically, they are responsible for many more successful deadly attacks.[328]

[325] The White House, "National Security Strategy," The White House, October 12, 2022, 31, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/.

[326] House, 31.

[327] House, 31.

[328] Seth G. Jones et al., "The War Comes Home: The Evolution of Domestic Terrorism in the United States," Center for Strategic and International Studies (CSIS), 2020, 3, http://www.jstor.org/stable/resrep26423.

Also, far-right groups have been able to spread their ideologies through social media more successfully. This thesis explores how intelligence fusion centers can counter this threat and counter far-right disinformation campaigns to contain the spread of far-right narratives and prevent the division of U.S. society.

A. THE ROLE OF THE IFC IN HOMELAND SECURITY

The National Network of Fusion Centers is an important element of the U.S. information sharing environment. Globalization and emerging technologies have increased the importance of IFCs as U.S. decision makers realized that the new threats are directly targeting states and local municipalities, and consequently, state and local government agencies cannot be insulated from federal intelligence information anymore.[329] The IFCs present one of the main channels that feed information to their respective local municipalities and individual states. The IFCs' initiative is a result of the 9/11 terrorist attacks on the United States, and their primary goal initially was to fight against terrorism by foreign actors. However, this idea has evolved, and it is driven by state and local needs. The IFCs have broadened their mission scope in order to be more responsive to local needs. Broadening the fusion centers' model from strictly countering terrorism to an "all-hazard" or "all-crime" scope was a natural evolution that will provide better situational awareness for the federal services as it also provides better support to local law enforcement and other local partners to address broader threats.

From the historical background, we can conclude that the IFCs are adaptive organizations. As described in Chapter II, the historical roots of the military intelligence fusion centers and the High-Intensity Drug Trafficking Area center model provided good examples for building contemporary fusion centers. From this starting point to the present time, the IFCs have been trying to adapt, and because of the decentralized model that they use, they are able to evolve faster than some conservative federal services like the FBI. This characteristic is extremely important for keeping pace with and responding to the globalized threat environment and the development of internet technologies.

[329] Lewandowski and Guidetti, "The Role of Fusion Centers in Homeland Security," 17.

As a new organization, the fusion centers must teach the local security services and partners how each can take advantage of their capabilities. The success of the fusion centers in supporting local law enforcement depends on the local security services' knowing how to interact with the fusion centers. To that end, the fusion center liaison officer program is an important mechanism for teaching local security services how to use the intelligence centers in their respective districts. The conclusion of this research suggests that personal connections are the most useful in terms of interactions between fusion centers and local police, health services, fire stations, and other public and private partners.[330] Therefore, the liaison program plays an essential role in creating robust intelligence sharing with local services, and it creates greater flexibility. Another area that fusion centers must focus on is increasing the budget for training with local partners. This approach will ensure the creation of robust connections with the community and help train local partners on how to use fusion centers' capabilities.

The IFCs also need to increase investment in education and training for their own employees. The survival of the network of intelligence fusion centers depends heavily on state and local funding. The citizens' acceptance and approval of IFCs depends on how much the local population trusts them and sees their value. If local citizens are not satisfied with their work or even, in some instances, are frightened of the center, then the local population will pressure the local government to cut down funding. Therefore, the IFCs need to maintain a high level of trust with citizens. Privacy violations are a big obstacle to building this trust. Therefore, it is essential to increase employees' knowledge about protecting civil rights and civil liberties.

Additionally, fusion centers play a key role in the creation of a robust network incorporating federal security services and local security organizations and partners, which are essential to U.S. homeland security. The IFCs also are important for implementing and sustaining the intelligence-led policing model for local law enforcement. Broadening the mission scope in response to local needs is a step toward transforming intelligence fusion centers from information hubs to real analytical centers necessary for developing a stronger

[330] Lewandowski, Carter, and Campbell, "The Role of People in Information-Sharing," 188.

local security environment. At the same time, each fusion center operates in a different state and in a different environment; hence, they need to be highly adaptive to local needs in order to continue their operations.

B. HOW IFCs CAN ADDRESS FAR-RIGHT DOMESTIC VIOLENT EXTREMISM

Far-right extremism is considered a major threat to U.S. homeland security. Far-right groups use a very decentralized model of organization in order to stymie the security services. Where there is no clear leader, but many low-level and local leaders responsible for their respective groups, the task of rooting out the mastermind of an organization becomes challenging. This leaderless organizational structure creates difficulties for intelligence agencies to infiltrate and obtain information about the groups' plans. On the other hand, this leaderless organization model creates weak control over the different groups and dilutes funding, which creates reduced operational capabilities and decreases of the groups' abilities to successfully organize and execute a major terrorist attack. That is why right-wing extremists are concentrating their efforts on low-level impact attacks with greater frequency. They also rely on inspiring lone-wolf actors to conduct violence.

Creating violence is the most effective tactic used by far-right extremist groups to spread their ideology and attract people. Creating intentional clashes between far-right and far-left protesters has led to the popularization of the far-right ideology, and this has led to accelerating the level of violence. The culmination in violence of far-right extremism happened when politicians started to recognize the appeal of far-right ideas. Then the far-right ideology transferred from local news to mainstream media. The mainstream political recognition united far-right movements from across the spectrum of far-right ideology, and this led to the violent protest on January 6, when the U.S. democracy was challenged.

The IFCs' involvement in countering far-right violence is limited, but there are still opportunities for them to contribute. One of the problems limiting their contribution is the lack of domestic violent extremism law that defines what constitutes violent extremists. That narrows explicitly the possibilities of what information IFCs can collect on domestic violent extremists and their ability to issue early warnings because collecting information

on U.S. citizens is restricted by the U.S. Constitution. However, from the example presented in Chapter III, it is evident that IFCs can collect information about U.S. citizens in specific situations, like when individuals are involved in a conspiracy to overthrow or attack the government. The case study in Chapter III provided evidence about the successful generation of intelligence warnings based on information collected from social media platforms. It turns out that most of the warnings and intelligence during the Capitol insurrection on January 6 were produced based on intelligence gleaned from social media communications. The DC Fusion Center provided sufficient warnings about the preparations for that attack. Thus, the IFCs possess the legal and technical capabilities to collect information from social media in similar situations, which can be invaluable.

C. THE ISSUE OF DISINFORMATION AND WHAT IFCs CAN DO ABOUT IT

Digital communication is essential for far-right movements. Before the development of social media, far-right extremism was not so widespread, but the digital environment provided a new opportunity to spread propaganda more broadly and more rapidly. Spreading disinformation and creating conspiracy theories is an essential part of the digital activities of far-right groups. These disinformation campaigns serve as a recruitment tool for new sympathizers. They also create grievances that can push people to violence, leading to increased domestic violent extremism. The example of Pizza Gate, as discussed in Chapter IV, is evidence of the effect disinformation can have on some people who are open to believing in conspiracy theories. Therefore, disinformation and conspiracy theories serve as a tool for increasing the violence motivated by far-right ideology.

Another problem is that disinformation in the far-right movement creates opportunities for foreign state actors to influence the U.S. domestic audience and drive deep divisions in society. People who believe in far-right ideas tend to respond more readily to disinformation and spread it unwittingly. This creates an opportunity for foreign actors to take advantage of this audience and, through them, to amplify their propaganda campaigns. This creates division in U.S. society and undermines democracy.

Disinformation is a complex problem that needs to be addressed. If this problem is not addressed properly, it will continue to mislead a growing segment of U.S. society. It will continue fueling violence and provide foreign manipulators with cheap access to American society. Disinformation is not a problem only in the United States; it is a global problem. If we can provide a solution for this problem and decrease the influence of disinformation campaigns, we will also undermine far-right violence worldwide.

The main problem for the U.S. government is how to take control over the supply of and demand for disinformation. The supply of disinformation can be addressed on a federal level, as we saw during the 2020 elections, when efforts by the FBI and other agencies were more successful in reducing the harmful effects of disinformation than they had been in 2016. However, the tools used in 2020 were designed primarily to be used against foreign actors, which has a limited effect in deterring domestic violent extremism. The demand part of the equation has more temporary effects, and it takes a lot of resources and time to address. This problem will not be solved only on the federal level; it requires support at the local level as well. The problem is that local security services are not prepared to address these cyber issues. They are more focused on local problems and do not encounter enough cyber threats. Moreover, disinformation in social media is a new phenomenon, and its consequences have become obvious only recently.

Nonetheless, IFCs can take part in addressing the demand side of the disinformation problem. IFCs are analytical centers and hubs for sharing information from federal institutions with local services, partners, and institutions. Through a top-down approach, the existing networks with local communities can be used to create resilience in those communities when combating disinformation campaigns. Educating the public and enhancing their digital literacy is the most effective measure for decreasing the influence of disinformation.[331] Through a bottom-up approach, IFCs can analyze their area of responsibility and whether their respective communities face a higher risk of exposure to disinformation. By doing that, they can help federal services determine on which social

[331] The Public-Private Analytic Exchange Program, "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue Part Two," 38.

groups they should focus resources and efforts. In general, IFCs are not prepared to address problems like disinformation. However, with federal support IFCs can be effectively included in efforts to address cyber issues like disinformation. Conversely, federal institutions need local support, and IFCs can provide it, but currently, their capabilities are limited.

D. RECOMMENDATIONS

The U.S. society must revisit the limits of the Intelligence Community in combating the exploitation of social media communication that promotes domestic violent extremism. Far-right extremism is a problem recognized by the U.S. Intelligence Community.[332] The next step should be creating an appropriate model for countering this threat. The collection of information is an essential part of this model, and IFCs can facilitate that step. According to Silber, platforms like "Telegram, Parler, … Facebook, Twitter, and YouTube are rich, open-source mediums where DVEs [domestic violent extremists] meet, talk, and even plot."[333] After an examination of the intelligence warning during the Capitol insurrection on January 6, Erik Dahl suggests that there is a need for discussion about how to collect information on social media and to determine a clearer line between what intelligence services can collect and what should be considered free speech.[334] IFCs can collect information about social media communication but only in a limited way and under specific circumstances that do not allow for reliable predictions of domestic violent extremist attacks. As shown in this thesis, social media is crucial to violent extremists for their organization, recruitment, and preparation of plots; therefore, understanding where to set an appropriate limit on the collection of social media information for the prevention of attacks or plots will make the work of IFCs more effective.

Creating central offices that will deal with the problems of disinformation and domestic violent extremism is necessary for better integration of IFCs. Silber suggests the

---

[332] The Office of the Director of National Intelligence, "Unclassified Summary of Assessment on Domestic Violent Extremism," 3.

[333] Silber, "Domestic Violent Extremism and The Intelligence Challenge," 19.

[334] Erik Dahl, "Lessons Learned from the January 6th Intelligence Failures," *Just Security*, September 26, 2022, https://www.justsecurity.org/83245/lessons-learned-from-the-january-6th-intelligence-failures/.

Online Social Media Analysis Unit must be created in the Office of Intelligence and Analysis within DHS.[335] In order for that unit to work and operate properly, "the standards for collection should be public, transparent, and focused on the bright line between constitutionally protected speech and threats of violence."[336] Simultaneously with that unit, there is a need for the creation of the Domestic Violent Extremism Analysis Unit, which would reside in the National Counterterrorism Center.[337] Similar to the National Counterterrorism Center's responsibilities in combating foreign terrorism, this new unit would be responsible for collecting, analyzing, and disseminating information on domestic violent extremist activities. These centralized offices responsible for collecting social media information and performing analysis on domestic violent extremism would centralize the work of IFCs and provide standards that fusion centers would be required to comply with. In this case, the possibility of privacy and civil liberty violations would be decreased due to the centralized model.

Finally, IFCs must communicate their activities more openly with citizens and civil society. The perception of the public regarding IFCs is not as positive as it needs to be. Transparency is essential if the IFCs' ability to collect information on social media activity is widened. IFCs should create a public information bureau or designate personnel responsible for publicizing accurate information on topics regarding civil liberties and privacy violations.

E. OPPORTUNITIES FOR FURTHER RESEARCH

This research was focused on the challenges presented by far-right extremists for state intelligence fusion centers. However, in the United States, there is also a significant threat from far-left violent extremists with ideologies and tactics different from those of far-right groups. Far-left extremism has largely escaped attention from security institutions and the mainstream media because of the other more significant and dangerous threats. But because far-left extremists are still a threat, studying them would be useful. Possible future

335 Silber, "Domestic Violent Extremism and The Intelligence Challenge," 19.

336 Silber, 19.

337 Silber, 20.

research in that area could compare far-right and far-left extremism and analyze the challenges they pose for fusion centers addressing this threat.

Another possible research direction is exploring international experience fighting far-right extremism and what foreign states do to combat their disinformation campaigns. France, for example, is a good starting point. Emilio Ferrara analyzed the 2017 presidential elections in France. He concluded that the alt-right affiliated Twitter account involved in a disinformation campaign during the 2016 presidential elections in the United States that supported Trump became active again during the 2017 presidential elections in France.[338] France and the United States are both liberal democracies. Therefore, comparing France's approach to fighting domestic violent extremism could provide solutions applicable to the U.S. security and government system, even though there are differences in both societies.

F. CONCLUSION

The IFCs have an important role in homeland security, and there is significant potential for this role to grow. The specific place where they are located, between the state and federal authorities, makes these centers unique and provides them with the flexibility necessary for adjusting to contemporary threats. On the other hand, that flexibility brings the risk for abusing U.S. citizens' rights. Finding the perfect balance is crucial for the future of IFCs.

Domestic violent extremism is a federal problem that directly affects local communities, and IFCs must be involved more seriously in this problem. The example of the fusion centers' successful involvement during the Capitol insurrection on January 6 occurred under specific circumstances, despite constraints on the fusion centers' capabilities that prevented them from addressing this threat on a larger scale. The increasing wave of violent far-right extremists and the inspiration of lone-wolf attacks affecting local communities requires IFCs be more deeply involved in helping local security services and communities manage those trends. For that reason, more federal

338 Emilio Ferrara, "Disinformation and Social Bot Operations in The Run Up to the 2017 French Presidential Election," *First Monday* 22, no. 8 (August 7, 2017): 3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2995809.

support is needed in funding, developing, and including fusion centers in countering domestic violent extremism.

LIST OF REFERENCES

The Anti-Defamation League. "HEAT Map ™" Accessed August 31, 2022. https://www.adl.org/resources/tools-to-track-hate/heat-map.

Allen, Charles. "State of Terrorism Intelligence: Confronting Foreign and Emergent Domestic Threats." *Homeland Security Today*, September 15, 2021. https://www.hstoday.us/911/state-of-terrorism-intelligence-confronting-foreign-and-emergent-domestic-threats/.

Anti-Defamation League. "Funding Hate: How White Supremacists Raise Their Money." Anti-Defamation League, 2017. https://www.adl.org/resources/report/funding-hate-how-white-supremacists-raise-their-money.

Bartlett, Jamie, and Carl Miller. "The Power of Unreason: Conspiracy Theories, Extremism and Counter-Terrorism." *London: Demos*, 2010. https://www.demos.co.uk/files/Conspiracy_theories_paper.pdf?1282913891.

Bauer, A., J. P. Sullivan, A. DeMarce, B. M. Jenkins, and Los Angeles County Sheriff's Office. *Terrorism Early Warning: 10 Years of Achievement in Fighting Terrorism and Crime*. California: Los Angeles County Sheriff's Department, 2008. https://books.google.com/books?id=pWU6mwEACAAJ.

BBC News. "Confederate Flag Taken down from South Carolina Capitol," July 10, 2015, sec. U.S. & Canada. https://www.bbc.com/news/world-us-canada-33483415.

Beckett, Lois. "Virginia: Thousands of Armed Protesters Rally against Gun Control Bills." *The Guardian*, January 20, 2020, sec. U.S. news. https://www.theguardian.com/us-news/2020/jan/20/virginia-gun-rally-activists-richmond.

Behrmann, Savannah. "Acting DHS Secretary: White Supremacy Is 'Most Persistent and Lethal Threat' Internally to US." USA Today, September 23, 2020. https://www.usatoday.com/story/news/politics/2020/09/23/dhs-secretary-white-supremacy-poses-persistent-and-lethal-threat/3511913001/.

Bimfort, Martin T. "A Definition of Intelligence." *CIA Historical Review Program*, 1994. https://www.cia.gov/static/554d7d05a62d7d6de84b5b84ae6702ae/A-Definition-Of-Intelligence.pdf.

Bjørgo, Tore, and Jacob Aasland Ravndal. "Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses." *International Center for Counter-Terrorism*, September 2019. https://doi.org/10.19165/2019.1.08.

Burris, Val, Emery Smith, and Ann Strahm. "White Supremacist Networks on the Internet." *Sociological Focus* 33, no. 2 (2000): 215–35. https://www.jstor.org.libproxy.nps.edu:2048/stable/20832076.

Butler, Alan, Jeramie Scott, and John Davisson. "Comments of the EPIC to the Privacy and Civil Liberties Oversight Board on Notice of Public Forum on Domestic Terrorism." *EPIC - Electronic Privacy Information Center* (blog), April 2022. https://epic.org/documents/epic-comments-agenda-for-pclob-may-2022-meeting-on-domestic-terrorism/.

Byman, Daniel. *Spreading Hate: The Global Rise of White Supremacist Terrorism*. New York: Oxford University Press, 2022.

Canady, Timothy M. "Rise of Domestic Violent Extremism and Law Enforcement's Ability to Effectively Investigate Seminar Research Paper." *University of Wisconsin-Platteville*, 21, 53.

Carter, David L., and Jeremy G. Carter. "The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement." *Criminal Justice and Behavior* 36, no. 12 (December 1, 2009): 1323–39. https://doi.org/10.1177/0093854809345674.

Carter, Jeremy G., David L. Carter, Steve Chermak, and Edmund McGarrell. "Law Enforcement Fusion Centers: Cultivating an Information Sharing Environment While Safeguarding Privacy." *Journal of Police and Criminal Psychology* 32, no. 1 (March 2017): 11–27. https://doi.org/10.1007/s11896-016-9199-4.

Carter, Jeremy G., Carla Lewandowski, and Gabrielle A. May. "Disparity Between Fusion Center Web Content and Self-Reported Activity." *Criminal Justice Review* 41, no. 3 (September 2016): 335–51. https://doi.org/10.1177/0734016816651925.

Cederberg, Gabriel, Jordan D'Amato, Corinna Fehst, Simon Jones, Kunal Kothari, Aleksandra Milcheva, and Irene Solaiman. "National Counter-Information Operations Strategy." Belfer Center for Science and International Affairs: Harvard Kennedy School, 2019. https://www.belfercenter.org/publication/national-counter-information-operations-strategy.

Center for Information Security. "Elections Infrastructure Information Sharing & Analysis Center." Accessed October 30, 2022. https://www.cisecurity.org/ei-isac/.

Chan, Elvis M. "Fighting Bears and Trolls: An Analysis of Social Media Companies and U.S. Government Efforts to Combat Russian Influence Campaigns During the 2020 U.S. Elections." Master's thesis, Naval Postgraduate School, 2021. https://calhoun.nps.edu/handle/10945/68309.

Coburn, Tom. "Federal Support for an Involvement in State and Local Fusion Centers." *PERMANENT SUBCOMMITTEE ON INVESTIGATIONS*, October 3, 2012, 141.

Collins, Susan M. "Summary of Intelligence Reform and Terrorism Prevention Act." Summary. United States Senate Committee of Government Affairs, 2004.

Connelly, Phoebe, Natalia Jiménez-Stuard, Tyler Remmel, and Madison Walls. "Warnings of Jan. 6 Violence Preceded the Capitol Riot." *Washington Post.* Accessed October 4, 2022. https://www.washingtonpost.com/politics/interactive/2021/warnings-jan-6-insurrection/.

Cooney, Mikaela, Dr Jeff Rojek, and Dr Robert J Kaminski. "An Assessment of the Utility of a State Fusion Center by Law Enforcement Executives and Personnel." *Journal of Intelligence Analysis* 20, no. 1 (September 2011): 19. https://www.researchgate.net/publication/249009791.

Counter Extremism Project. "James Mason's Siege: Ties to Extremists." Accessed October 18, 2022. https://www.counterextremism.com/james-masons-siege-ties-to-extremists.

The Cybersecurity and Infrastructure Security Agency. "About CISA." Accessed November 2, 2022. https://www.cisa.gov/about-cisa.

Dahl, Erik. "January 6th Intelligence Failure Timeline." *Just Security*, June 7, 2022. https://www.justsecurity.org/81806/january-6-intelligence-and-warning-timeline/.

———. "Lessons Learned from the January 6th Intelligence Failures." *Just Security*, September 26, 2022. https://www.justsecurity.org/83245/lessons-learned-from-the-january-6th-intelligence-failures/.

Dahl, Erik J. *Intelligence and Surprise Attack : Failure and Success from Pearl Harbor to 9/11 and Beyond.* Washington, DC: Georgetown University Press, 2013.

———. "The Localization of Intelligence: A New Direction for American Federalism." *International Journal of Intelligence and CounterIntelligence* 34, no. 1 (January 2, 2021): 151–78. https://doi.org/10.1080/08850607.2020.1716563.

DEA Museum. "An Overview of the El Paso Intelligence Center | DEA Museum." DEA Museum, 2011. https://museum.dea.gov/video-archive/el-paso-intelligence-center.

The Department of Homeland Security. "National Network of Fusion Centers Final Report," 2017, 35. https://www.dhs.gov/sites/default/files/publications/2017_National_Network_of_Fusion_Centers_Final%20Report.pdf.

The Department of Homeland Security. "Homeland Threat Assessment October 2020," n.d., 26. https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.

The Department of Homeland Security. "National Network of Fusion Centers Final Report," 2018, 15. https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf.

The Department of Public Safety. "The Intelligence Production Cycle | Iowa Department of Public Safety." Accessed July 17, 2022. https://dps.iowa.gov/divisions/intelligence/intel-cycle.

Domestic Terrorism Database. "Domestic Terrorism Database." Accessed September 17, 2022. https://apps.revealnews.org/domestic-terror-int/index.html.

Drury, Colin. "'Commander' of Feuerkrieg Far-Right Terror Group Unmasked by Police as 13-Year-Old Boy." *The Independent*, April 30, 2020. https://www.independent.co.uk/news/world/europe/far-right-terror-group-commander-teenage-boy-fire-war-division-estonia-a9460526.html.

Edelson, Laura, Minh-Kha Nguyen, Ian Goldstein, Oana Goga, Tobias Lauinger, and Damon McCoy. "Far-Right News Sources on Facebook More Engaging." Medium. *Cybersecurity for Democracy* (blog), March 4, 2021. https://medium.com/cybersecurity-for-democracy/far-right-news-sources-on-facebook-more-engaging-e04a01efae90.

Ellis, Clare, Raffaello Pantucci, Jeanine de Roy van Zuijdewijn, Edwin Bakker, Melanie Smith, Benoît Gomis, and Simon Palombi. "Analysing the Processes of Lone-Actor Terrorism: Research Findings." *Perspectives on Terrorism* 10, no. 2 (2016): 33–41. https://www.jstor.org/stable/26297551.

The Federal Bureau of Investigation and The Department of Homeland Security. "Strategic Intelligence Assessment and Data on Domestic Terrorism," 2021, 40.

Ferrara, Emilio. "Disinformation and Social Bot Operations in The Run Up to the 2017 French Presidential Election," no. University of Southern California-Information Sciences Institute (2017): 33. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2995809.

Feuer, Alan, Luke Broadwater, Maggie Haberman, Katie Benner, and Michael S. Schmidt. "Jan. 6 Timeline: Key Moments From Before the Attack on the Capitol to Now." *New York Times*, June 9, 2022. https://www.nytimes.com/interactive/2022/us/politics/jan-6-timeline.html.

Freilich, Joshua D., Steven M. Chermak, Jeff Gruenewald, William S. Parkin, and Brent R. Klein. "Patterns of Fatal Extreme-Right Crime in the United States" 12, no. 6 (2018): 14.

Fusion Center Liaison Officer (FLO) Programs. Video. Accessed July 27, 2022. https://nfcausa.org/video/.

Gais, Hannah, and Megan Squire. "How an Encrypted Messaging Platform Is Changing Extremist Movements." Southern Poverty Law Center. Accessed October 19, 2022. https://www.splcenter.org/news/2021/02/16/how-encrypted-messaging-platform-changing-extremist-movements.

Ganesh, Bharath. "The Ungovernability of Digital Hate Culture." *Journal of International Affairs* 71, no. 2 (Spring/Summer 2018): 30–49.

Glawe, David J. "The Office of Intelligence and Analysis FY 2020–2024 Strategic Plan." Department of Homeland Security, 2020. https://www.dhs.gov/publication/office-intelligence-and-analysis-fy-2020-2024-strategic-plan.

The Global Advisory Committee. "Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers." Global Justice Information Sharing Initiative, 2015. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/cyber_integration_for_fusion_centers.pdf.

Global Justice Information Sharing Initiative. "Baseline Capabilities for State and Major Urban Area Fusion Centers." Washington, DC: The U.S. Department of Justice, 2008. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/baseline%20capabilities%20for%20state%20and%20major%20urban%20area%20fusion%20centers.pdf.

Global Justice Information Sharing Initiative and DHS's Homeland Security Advisory Council. "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era." The U.S. Department of Justice, 2006. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines0.pdf.

———. "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era." The U.S. Department of Justice, 2006. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines_law_enforcement.pdf.

Goodin, Dan. "NSA and FBI Warn That New Linux Malware Threatens National Security." Ars Technica, August 13, 2020. https://arstechnica.com/information-technology/2020/08/nsa-and-fbi-warn-that-new-linux-malware-threatens-national-security/.

Gorelick, Jamie, and Michael Chertoff. "Subcommittee for Disinformation Best Practices and Safeguards." Homeland Security Advisory Council: Department of Homeland Security, n.d. https://www.dhs.gov/homeland-security-advisory-council.

Graphika Team. "Step Into My Parler; Suspected Russian Operation Targeted Far-Right American Users on Platforms Including Gab and Parler, Resembled Recent IRA-Linked Operation That Targeted Progressives." *New York: Graphica*, 2020. https://graphika.com/reports/step-into-my-parler/.

Gray, Kathleen. "In Michigan, a Dress Rehearsal for the Chaos at the Capitol on Wednesday." *New York Times*, January 9, 2021, sec. U.S. https://www.nytimes.com/2021/01/09/us/politics/michigan-state-capitol.html.

Hoekstra, Peter, David Dreier, Henry Hyde, Duncan Hunter, Jane Harman, Robert Menendez, and Ike Sleleton. "Intelligence Reform and Terrorism Prevention Act of 2004." Conference Report. Washington, DC: House of Representative, 2004. https://books.google.bg/books?id=NC1heYaq9NMC&printsec=frontcover&dq=intelligence+reform+and+terrorism+prevention+act&hl=bg&sa=X&redir_esc=y#v=onepage&q=intelligence%20reform%20and%20terrorism%20prevention%20act&f=false.

Homeland Security Today. "'This Is Our House!' A Preliminary Assessment of the Capitol Hill Siege Participants." Program on Extremism. George Washington University, March 2021. https://www.hstoday.us/subject-matter-areas/counterterrorism/this-is-our-house-a-preliminary-assessment-of-the-capitol-hill-siege-participants/.

Homeland Security Today. "Protecting Every Voice: FBI Expands Resources on Election Security.", October 23, 2019. https://www.hstoday.us/subject-matter-areas/cybersecurity/protecting-every-voice-fbi-expands-suite-of-resources-on-election-security/.

House, The White. "National Security Strategy." The White House, October 12, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/.

Howard, Philip N, Bharath Ganesh, Dimitra Liotsiou, John Kelly, and Camille François. "The IRA, Social Media and Political Polarization in the United States, 2012–2018." Oxford University: Propaganda Computational Research Project, 2018. https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf.

Isikoff, Michael. "Exclusive: The True Origins of the Seth Rich Conspiracy Theory. A Yahoo News Investigation." *Yahoo News,* July 2019. https://news.yahoo.com/exclusive-the-true-origins-of-the-seth-rich-conspiracy-a-yahoo-news-investigation-100000831.html.

Jones, Seth G. "The Rise of Far-Right Extremism in the United States." *CENTER FOR STRATEGIC & INTERNATIONAL STUDIES*, 2018, 9. https://www.csis.org/analysis/rise-far-right-extremism-united-states.

Jones, Seth G., Catrina Doxsee, Nicholas Harrington, Grace Hwang, and James Suber. "The War Comes Home: The Evolution of Domestic Terrorism in the United States." Center for Strategic and International Studies (CSIS), 2020. http://www.jstor.org/stable/resrep26423.

Justin Hendrix. "Capito Attack: Federal Agencies' Use of Open Source Data and Related Threat Products Prior to January 6, 2021." Report to Congressional Requesters. Washington, DC: The Government Accountability Office, May 5, 2022. https://www.justsecurity.org/81384/facebook-provided-warning-to-fbi-before-january-6-gao-report-reveals/.

Kang, Cecilia, and Adam Goldman. "In Washington Pizzeria Attack, Fake News Brought Real Guns." *New York Times*, December 5, 2016, sec. Business. https://www.nytimes.com/2016/12/05/business/media/comet-ping-pong-pizza-shooting-fake-news-consequences.html.

Kayyali, Dia. "The History of Surveillance and the Black Community." Electronic Frontier Foundation, February 13, 2014. https://www.eff.org/deeplinks/2014/02/history-surveillance-and-black-community.

Kettl, Donald F. "Modern Federalism's Big 3 Moments - Potomac Chronicle: There's Been a Sea Change in the Way Levels of Government Deal with Each Other." *Governing Magazine (USA)*, October 1, 2017. *Access World News*. http://infoweb.newsbank.com/apps/news/openurl?ctx_ver=z39.88-2004&rft_id=info%3Asid/infoweb.newsbank.com&svc_dat=AWNB&req_dat=0D0CB5FC0F5C3AD5&rft_val_format=info%3Aofi/fmt%3Akev%3Amtx%3Actx&rft_dat=document_id%3Anews%252F169D4DAB7005B380.

Kristof, Nicholas. "Opinion | When Antifa Hysteria Sweeps America." *New York Times*, June 17, 2020, sec. Opinion. https://www.nytimes.com/2020/06/17/opinion/antifa-protests.html.

Kroll, Andy. "Will Julian Assange and WikiLeaks Finally Tell the Truth About Seth Rich?" *Rolling Stone* (blog), November 26, 2019. https://www.rollingstone.com/politics/politics-news/will-julian-assange-and-wikileaks-finally-tell-the-truth-about-seth-rich-918946/.

Lee, Micah. "How NCRIC Keeps Tabs on Black Lives Matter Protesters." The Intercept, August 17, 2020. https://theintercept.com/2020/08/17/blueleaks-california-ncric-black-lives-matter-protesters/.

Levinson, Charles. "With Super PAC, QAnon's Con Chases Mainstream — and Money." Protocol, March 3, 2020. https://www.protocol.com/qanon-conspiracy-new-super-pac.

Lewandowski, Carla. "Observations from within a State Fusion Center: Operations and Daily Routines." *IALEIA Journal*, 2012, 72–91.

Lewandowski, Carla, Jeremy G. Carter, and Walter L. Campbell. "The Role of People in Information-Sharing: Perceptions from an Analytic Unit of a Regional Fusion Center." *Police Practice and Research* 18, no. 2 (March 4, 2017): 174–93. https://doi.org/10.1080/15614263.2016.1250631.

Lewandowski, Carla, and Ray Guidetti. "The Role of Fusion Centers in Homeland Security." In *Homeland Security and Intelligence 2d Ed. by Keith Gregory Logan*, 173–90. ABC-CLIO Santa Barbara, CA, 2018.

Lewandowski, Carla, and Thomas J. Nestel. "Police Communication at the Local Level: An Exploratory Study." *Journal of Policing, Intelligence and Counter Terrorism* 11, no. 1 (January 2, 2016): 49–62. https://doi.org/10.1080/18335330.2016.1161224.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. CQ Press, 2022.

Luxner, Larry. "Ahead of the 2020 U.S. Elections, the Disinformation Threat Is More Domestic than Foreign." *Atlantic Council* (blog), September 23, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/ahead-of-the-2020-us-elections-the-disinformation-threat-is-more-domestic-than-foreign/.

Marchio, James D. "The Evolution and Relevance of Joint Intelligence Centers." *Studies in Intelligence* 49, no. 1 (March 2005): 18.

Masse, Todd, and John Rollins. "A Summary of Fusion Centers: Core Issues and Options for Congress." CRS Report. Washington, D.C.: Congressional Research Service, September 19, 2007. https://www.everycrsreport.com/reports/RL34177.html#:~:text=A%20Summary%20of%20Fusion%20Centers%3A%20Core%20Issues%20and,well%20as%20the%20obstacles%20and%20risks%20they%20face.

McHugh, Liam, and Tobias Armour. "Trends in Domestic Violent Extremism – Lobo Institute," 2021. https://www.loboinstitute.org/trends-in-domestic-violent-extremism/.

Merchant, Nomaan. "US Delays Intelligence Center Targeting Foreign Influence." U.S. *News & World Report*. Accessed October 14, 2022. //www.usnews.com/news/politics/articles/2021-12-23/us-delays-intelligence-center-targeting-foreign-influence.

Miller, Cassie, and Graves Howard. "When the 'Alt-Right' Hit the Streets: Far-Right Political Rallies in the Trump Era." Southern Poverty Law Center. Accessed September 15, 2022. https://www.splcenter.org/20200810/when-alt-right-hit-streets-far-right-political-rallies-trump-era.

Miller, Rena S. "A Persistent and Evolving Threat: An Examination of the Financing of Domestic Terrorism and Extremism." *Congressional Research Service*, 2020, 7.

Miller-Idriss, Cynthia. *Hate in the Homeland: The New Global Far Right.* Princeton: Princeton University Press, 2020. https://muse.jhu.edu/book/77540.

Miller-Idriss, Cynthia and Brian Hughes. "Blurry Ideologies and Strange Coalitions: The Evolving Landscape of Domestic Extremism." Lawfare, December 19, 2021. https://www.lawfareblog.com/blurry-ideologies-and-strange-coalitions-evolving-landscape-domestic-extremism.

Mole, Charlie. "Seth Rich: How a Young Man's Murder Attracted Conspiracy Theories." *BBC News*, April 21, 2018, sec. BBC Trending. https://www.bbc.com/news/blogs-trending-43727858.

Monahan, Torin, and Neal A. Palmer. "The Emerging Politics of DHS Fusion Centers." *Security Dialogue* 40, no. 6 (December 2009): 617–36. https://doi.org/10.1177/0967010609350314.

Montgomery, Molly. "Disinformation as a Wicked Problem: Why We Need Co-Regulatory Frameworks." Brookings, 2020. https://www.brookings.edu/research/disinformation-as-a-wicked-problem-why-we-need-co-regulatory-frameworks/.

Muhlhausen, David. "Terror Trends: 40 Years' Data on International and Domestic Terrorism." The Heritage Foundation. Accessed May 26, 2022. https://www.heritage.org/terrorism/report/terror-trends-40-years-data-international-and-domestic-terrorism.

National Fusion Center Association. "National Strategy for the National Network of Fusion Centers 2014–2017 | Public Intelligence," 2015. https://publicintelligence.net/national-fusion-center-strategy-2014-2017/.

Neiwert, David. "Domestic Terror in the Age of Trump." Reveal, July 9, 2020. http://revealnews.org/article/domestic-terror-in-the-age-of-trump/.

NBC News. "DHS Is Gathering Intelligence on Security Threats from Social Media." Accessed September 27, 2022. https://www.nbcnews.com/politics/national-security/dhs-launches-warning-system-find-domestic-terrorism-threats-public-social-n1266707.

NBC News. "New York's 8,000 Cameras Helped Snare Bomb Suspect Ahmad Rahami." Accessed August 9, 2022. https://www.nbcnews.com/storyline/ny-nj-bombings/more-8-000-cameras-helped-snare-bomb-suspect-ahmad-rahami-n650891.

The Office of the Director of National Intelligence. "About the Information Sharing Environment." Accessed May 7, 2022. https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise.

The Office of the Director of National Intelligence. "Unclassified Summary of Assessment on Domestic Violent Extremism." Office of the Director of National Intelligence, March 2021. https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2194-unclassified-summary-of-assessment-on-domestic-violent-extremism.

The Office of the Director of National Intelligence. "What Is Intelligence?" Accessed July 15, 2022. https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

O'Harrow Jr, Robert, Andrew Ba Tran, and Derek Hawkins. "The Rise of Domestic Extremism in America." *Washington Post*. Accessed May 26, 2022. https://www.washingtonpost.com/investigations/interactive/2021/domestic-terrorism-data/.

PBS. American Insurrection. Frontline Film, 2022. https://www.pbs.org/wnet/exploring-hate/films/american-insurrection-a-frontline-film-2022/.

The Public-Private Analytic Exchange Program. "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue." Department of Homeland Security Public, 2019. https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

———. "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue Part Two." Department of Homeland Security, 2021. https://publicintelligence.net/dhs-combatting-disinformation-2021/.

Ravndal, Jacob Aasland, and Tore Bjørgo. "Investigating Terrorism from the Extreme Right: A Review of Past and Present Research" 12, no. 6 (2018): 18.

Reuters. "Dylann Roof Wrote White Supremacist Manifestos: Prosecutors," August 22, 2016, sec. *U.S. News*. https://www.reuters.com/article/us-south-carolina-shooting-idUSKCN10X29A.

Riley, Kevin Jack, and Rand Corporation, eds. *State and Local Intelligence in the War on Terrorism*. Santa Monica, CA: RAND Corporation, 2005.

Rollins, John. "Fusion Centers: Issues and Options for Congress." CRS Report. Washington, D.C.: Congressional Research Service, January 18, 2008. https://bja.ojp.gov/program/it/privacy-civil-liberties/reports-research/service/2337#:~:text=Fusion%20Centers%3A%20Issues%20and%20Options%20for%20Congress%20%28RL34070%2C,enhance%20the%20federal%20government%E2%80%99s%20relationship%20with%20fusion%20centers.%22.

Rousis, Gregory J., F. Dan Richard, and Dong-Yuan Debbie Wang. "The Truth Is Out There: The Prevalence of Conspiracy Theory Use by Radical Violent Extremist Organizations." *Terrorism and Political Violence*, November 19, 2020, 1–19. https://doi.org/10.1080/09546553.2020.1835654.

Sacco, Lisa N. “Sifting Domestic Terrorism from Domestic Violent Extremism and Hate Crime.” CRS Report. Washington, DC: Congressional Research Service, June 1, 2022.

Schuurman, Bart, Edwin Bakker, Paul Gill, and Noémie Bouhana. “Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis,.” *Journal of Forensic Sciences* 63, no. 4 (2018): 1191–1200. https://doi.org/10.1111/1556-4029.13676.

Scott, Jeramie, and Jake Wiener. “Comments of the EPIC to the Department of Homeland Security Data Privacy and Integrity Advisory Committee.” *EPIC - Electronic Privacy Information Center* (blog), October 2020. https://epic.org/epic-again-urges-dhs-advisory-committee-to-investigate-fusion-centers/.

Silber, Mitchell D. “Domestic Violent Extremism and The Intelligence Challenge.” *Atlantic Council*, May 2021, 29.

Smith, Allison G. “How Radicalization to Terrorism Occurs in the United States: What Research Sponsored by the National Institute of Justice Tells Us.” *Washington, DC: U.S. Department Of Justice, Office of Justice Programs, National Institute of Justice*, 2018, 27.

Southern Poverty Law Center. “Louis Beam.” Accessed October 16, 2022. https://www.splcenter.org/fighting-hate/extremist-files/individual/louis-beam.

Southern Poverty Law Center. “Hate Crimes, Explained.” Accessed September 14, 2022. https://www.splcenter.org/hate-crimes-explained.

Squire, Megan. “Alt-Tech & the Radical Right, Part 3: Why Do Hate Groups and Terrorists Love Telegram? – Centre for Analysis of the Radical Right.” Radical Right Analysis, 2020. https://www.radicalrightanalysis.com/2020/02/23/alt-tech-the-radical-right-part-3-why-do-hate-groups-and-terrorists-love-telegram/.

Starbird, Kate. “Disinformation’s Spread: Bots, Trolls and All of Us.” *Nature* 571, no. 7766 (July 2019): 449–449. https://doi.org/10.1038/d41586-019-02235-x.

Stengel, Richard. “We Should Be as Worried About Domestic Disinformation as We Are About International Campaigns.” *Time*. Accessed October 21, 2022. https://time.com/5860215/domestic-disinformation-growing-menace-america/.

Stokes, Roger L. “Employing the Intelligence Cycle Process Model Within The Homeland Security Enterprise.” Master’s thesis, Naval Postgraduate School, 2013. https://calhoun.nps.edu/handle/10945/39018.

Stone, Kelley Edmonds. “Creating an Information Sharing and Analysis Center: A Case Study of The North Central Texas Fusion Center.” PhD diss, University of Texas, 2014.

Subcommittee on Intelligence and Counterterrorism Committee on Homeland Security. "Assessing the Threat from Accelerationists and Militia Extremists." Washington, D.C., July 16, 2020. https://www.congress.gov/event/116th-congress/house-event/110911.

Sullivan, John, and Genevieve Lester. "Revisiting Domestic Intelligence." *Journal of Strategic Security* 15, no. 1 (April 2022): 75–105. https://doi.org/10.5038/1944-0472.15.1.1976.

"Surveillance Cameras and the Times Square Bombing." Accessed August 9, 2022. https://slate.com/technology/2010/05/surveillance-cameras-and-the-times-square-bombing.html.

The Surprising Origins of the Modern Conspiracy Theory. Documentary. BBC Real, 2022. https://www.bbc.com/reel/video/p0chchj8/the-surprising-origins-of-the-modern-conspiracy-theory.

Taylor, Robert W. and Jennifer Elaine Davis. "Intelligence-Led Policing and Fusion Centers." In *Critical Issues in Policing: Contemporary Readings*, 6th ed., 224–43. Long Grove, Ill: Waveland Press, 2010.

Thompson, Carolyn. "Grand Jury Indicts Man In Buffalo Supermarket Shooting." HuffPost, May 19, 2022. https://www.huffpost.com/entry/buffalo-supermarket-shooting-payton-gendron-indicted_n_62864ecce4b00685b66a4d44.

Thompson, Terry L. "No Silver Bullet: Fighting Russian Disinformation Requires Multiple Actions." *Georgetown Journal of International Affairs* 21, no. 1 (2020): 182–94. https://doi.org/10.1353/gia.2020.0033.

Thomson, James. *Conflict and Cooperation in Intelligence and Security Organisations: An Institutional Costs Approach*. 1st ed. London: Routledge, 2021. https://doi.org/10.4324/9781003107231.

Van Puyvelde, Damien. "Fusing Drug Enforcement: A Study of the El Paso Intelligence Center." *Intelligence and National Security* 31, no. 6 (September 18, 2016): 888–902. https://doi.org/10.1080/02684527.2015.1100373.

Vitali, Joshua D. "Fueling The Fire: An Examination of Right-Wing Extremism in The United States Over The Last Decade." Master's thesis, Naval Postgraduate School, 2020. https://calhoun.nps.edu/handle/10945/65460.

The White House. "National Strategy for Information Sharing," 2007. https://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html.

Williams, Heather J., Luke J. Matthews, Pauline Moore, Matthew A. DeNardo, James V. Marrone, Brian A. Jackson, William Marcellino, and Todd C. Helmus. *Mapping White Identity Terrorism and Racially or Ethnically Motivated Violent Extremism: A Social Network Analysis of Online Activity*. Santa Monica, CA: RAND Corporation, 2022. https://doi.org/10.7249/RRA1841-1.

Zegart, Amy. "In the Deepfake Era, Counterterrorism Is Harder." *The Atlantic*, September 11, 2019. https://www.theatlantic.com/ideas/archive/2019/09/us-intelligence-needs-another-reinvention/597787/.

Zegart, Amy B. *Spying Blind*. Princeton, NJ: Princeton University Press, 2009.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California