THREAT ANALYSIS

FOREIGN TERRORIST ORGANIZATIONS & ROGUE NATIONS: SOCIAL MEDIA DISINFORMATION CAMPAIGNS

Michael Prasad, CEM®
Intelligence Analyst

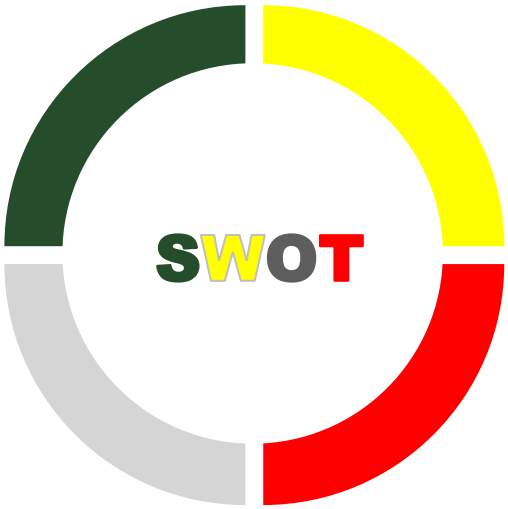
TLP: GREEN
UNCLASSIFIED

STRENGTHS

- Communication
- Collaboration
- Cooperation
- Coordination

OPPORTUNITIES

- Planning
- Organizational Constructs
- New Equipment & Technologies
- Training
- Exercising



WEAKNESSES

- Lack of Coordination
- Communications Gaps
- Supply Chain Dependence
- Limited Planning

THREATS

- Domestic Violent Extremists
- Foreign Terrorist Organizations
- Cyber Security
- Natural/Other Caused

EXTREMIST VS. TERRORIST: SHOULD IT MATTER TO EMERGENCY MANAGEMENT PRACTITIONERS?

There are obstacles to information sharing between the U.S. Intelligence community and state/local law enforcement agencies, most emanating from the USA Patriot Act. Designation as terrorism may or may not bring additional benefits to threat Protection and Prevention (two elements of Disaster Readiness, for which Emergency Management practitioners are responsible for – outweighing the impacts to U.S. civil liberties.

https://www.rand.org/blog/2021/03/implications-of-domestic-terrorist-group-designations.html

As part of a standard "SWOT" Analysis – the aspect of Foreign Terrorist Organizations (FTOs) is an important set of threats that create risks for any country's emergency management practitioners. Emergency managers, not just law enforcement, need to keep in mind their organization's disaster readiness (resiliency) along the standard path of Protect/Prevent/Prepare, Respond, Recover and Mitigate – including the adverse impacts that can be generated by these threats. Tools and techniques – along with collaboration, coordination, cooperation, and communication – to and from the military and civilian intelligence agencies can assist emergency management practitioners at all levels of government.[1]

It is crucial for emergency managers to understand the risks of any threat – and the possibility of adverse impacts to not only the communities they serve, but their own workforce (inclusive of all incident command and control structures) and those of allied partners. The training, indoctrination,

[1] Dycus, S. (2004). The role of military intelligence in homeland security. *Louisiana Law Review. 64*(4). https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=6053&context=lalrev

methodologies, and tradecraft of domestic violent extremists (DVEs) can come from many of these FTOs – whether they are directly influenced and/or sponsored (such as the HVEs); or they are indirectly studied and researched by the DVEs.[2] Using the experience and knowledge from historical warfare activities can also help prepare Emergency Managers to the DVE threat. This is applicable to the Incident Action Planning, through Unified Command and the use of the **Intelligence** branch.

The concept of disinformation (as well as propaganda, misinformation, malinformation, etc.[3]) is not new – what has happened is that its use by foreign state and non-state actors to undermine and influence the "policies, security, or stability of the United States, its allies, and partner nations"[4] has accelerated exponentially in the internet age. The United States has already seen disinformation impacts to its elections[5], COVID-19 response[6], and of course reputational impacts to individuals and organizations.[7] Social media disinformation can be very powerful, very quickly distributed (think "going viral"), and as Jonathan Swift noted way back in 1710, "Falsehood flies, and the truth comes limping after it."[8]

Social media disinformation utilizes a number of key logical fallacies[9] when it targets groups and individuals:

- **Mob Appeal**: By appealing to a crowd, the hope is that emotions will override the fallacy. Phrases such as "everybody knows" fit this method of opinion vs. fact.
- **Weak Analogy**: By comparing two or more disconnected items (for example COVID-19 and the Seasonal Flu), the reader is easily manipulated into making the connection on their own.
- **Suppressed Evidence**: Failing to share the differences in analogies made or omitting transparency information/data. Reposts of disinformation with additional unfounded claims only amplifies the disinformation.
- **Appeal to Authority**: By presenting disinformation (or reposting it) the authority only grows stronger, even when the original source may in fact be false and even utilize real officials' names and personas.

---

[2] Collins, A. (2020, September). The need for a specific law against domestic terrorism. George Washington University Program on Extremism. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/The%20Need%20for%20a%20Specific%20Law%20Against%20Domestic%20Terrorism.pdf

[3] Wardle, C. & Derakhshan, H. (2018). *Journalism, 'Fake News' & Disinformation.* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000265552

[4] National Defense Authorization Act, 2019, Section 1284 https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf

[5] Allcott, H. & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives 31*(2). https://web.stanford.edu/~gentzkow/research/fakenews.pdf

[6] Tagliabue, F., Galassi, L. & Mariani, P. The "Pandemic" of disinformation in COVID-19. SN Compr. Clin. Med. 2, 1287–1289 (2020). https://doi.org/10.1007/s42399-020-00439-1

[7] Parsons, D. (2020). The impact of fake news on company value: Evidence from Tesla and Galena Biopharma. TRACE: Tennessee Research and Creative Exchange. University of Tennessee, Knoxville. https://trace.tennessee.edu/cgi/viewcontent.cgi?article=3363&context=utk_chanhonoproj

[8] Swift, Jonathan. (1710, November 9). *The Examiner No. XIV*

[9] Chrisman, J. (2020, April 27). Illogic: Fallacies of logic. U.S. Army MWR – Ft. Gordon. https://gordon.armymwr.com/fyi/learn/illogic-fallacies-logic

The U.S. federal government divides its disaster readiness (and national defense) Intelligence activities (associated with Prevention and Protection) into two distinct jurisdictions: external threats and internal threats.

- **Foreign States and non-states (FTOs):** The monitoring, reporting, alerting and data collection activities on these groups are performed by the U.S. State Department's Global Engagement Center (GEC). The GEC has a focus now on Russia, China and Iran as the top state actors involved in disinformation campaigns. There are partnerships between government and academia for the research and monitoring of disinformation, especially what occurs via public social media accounts and on the web.
    - One of those partnerships is with the German Marshall Fund of the U.S. Alliance for Securing Democracy. Their Hamilton 2.0 Dashboard "provides a summary analysis of the narratives and topics promoted by Russian, Chinese, and Iranian government officials and state-funded media on Twitter, YouTube, state-sponsored news websites, and via official diplomatic statements at the United Nations" (alliance for securing democracy, 2021, p.1)[10]
    - The GEC has also partnered with Park Capital Investment Group LLC to create an open-source platform called Disinfo Cloud[11] which can help identify U.S. companies with tested tools and technology platforms which can help identify and thwart foreign-sponsored disinformation.
    - The U.S. federal government, through the Federal Bureau of Investigation (FBI) and the U.S. Department of Commerce's Bureau of Industry and Security, can seize websites linked to foreign nationals and nation-states (based on U.S. law) because of a disinformation threat.[12]
- **U.S. Nationals and U.S. Based groups:** The monitoring, reporting, alerting and data collection activities on these groups are performed by the U.S. Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA is fairly new, having been formed in 2018).[13]
    - CISA provides alerts to other U.S. Federal departments and agencies, and also in-depth education on both the various tradecraft threat elements used by DVEs (and potentially FTOs operating through U.S. groups) and the backgrounds/attack history of the groups themselves.
    - The FBI and DHS both investigate disinformation campaigns on the Homeland from both FTOs and DVEs. DHS also has as one of its strategic goals outlined in their *2019 Department of Homeland Security Strategic Framework for Countering Terrorism and*

[10] https://securingdemocracy.gmfus.org/hamilton-dashboard/
[11] https://disinfocloud.com/
[12] https://www.theguardian.com/world/2021/jun/23/us-takes-down-dozens-of-iran-linked-news-sites-accusing-them-of-disinformation
[13] https://www.cisa.gov/mdm-resource-library

Targeted Violence policy document to bolster information sharing about foreign disinformation campaigns, as well as bolstering communication and coordination with state, local, tribal and territorial government entities. This local emphasis is critical to represent the trusted voices within communities who can quickly counter disinformation campaigns at the grassroots level.[14]

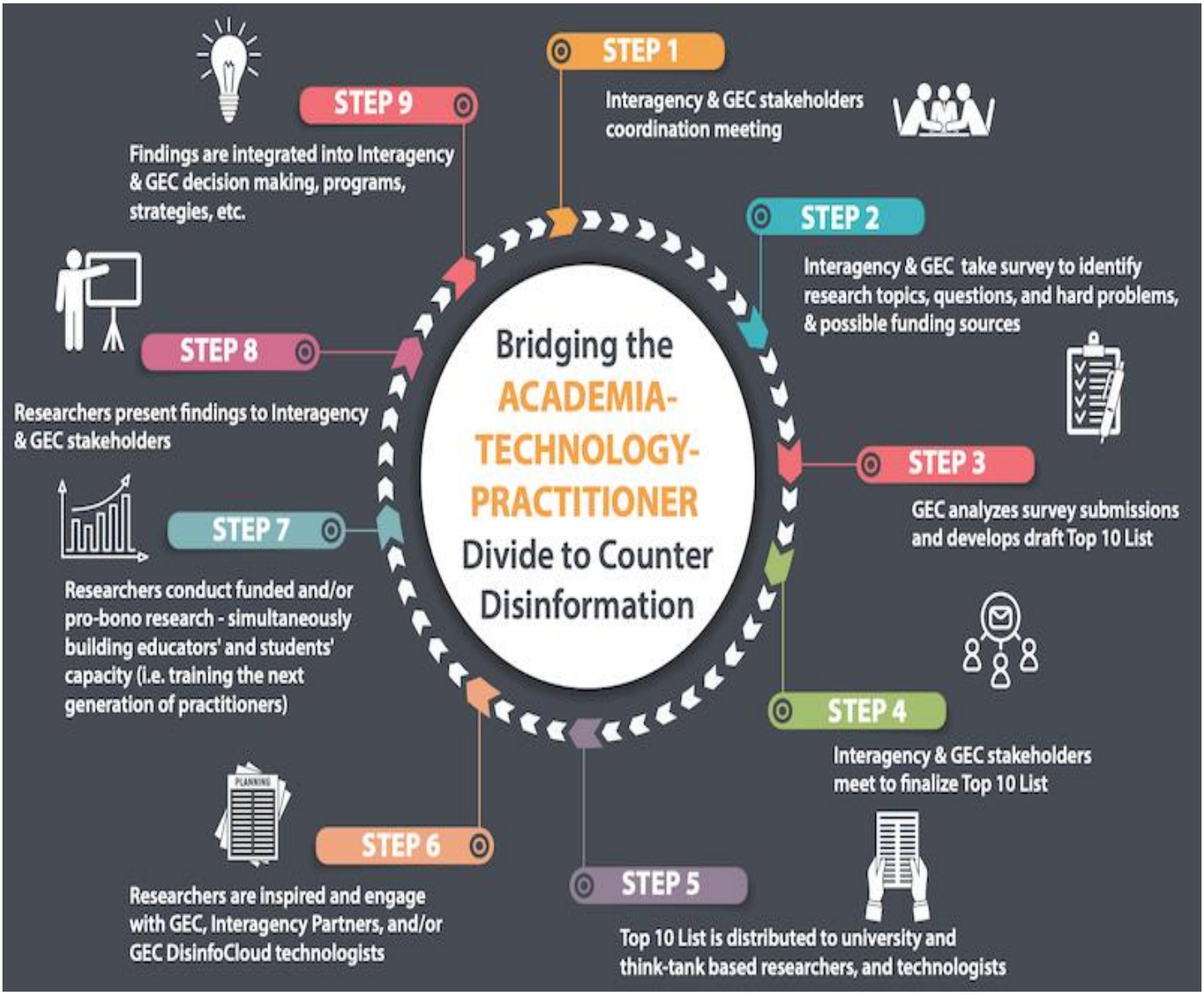


Figure 1 https://disinfocloud.com/blog/gec-top10researchtopics

[14] https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

DVEs USE THE SAME PLAYBOOK AS FTOs WHEN IT COMES TO SOCIAL MEDIA DISINFORMATION CAMPAIGNS

The FBI notes that terrorism threats impacting the United States (and therefore U.S. Emergency Management) has two key factors of recent impact:

- **Lone offenders**: Terrorist threats have evolved from large-group conspiracies toward lone-offender attacks. These individuals often radicalize online and mobilize to violence quickly.[15] Without a clear group affiliation or guidance, lone offenders are challenging to identify, investigate, and disrupt. The FBI relies on partnerships and tips from the public to identify and thwart these attacks.[16]
- **The Internet and social media**: International and domestic violent extremists have developed an extensive presence on the Internet through messaging platforms and online images, videos, and publications.[17] These facilitate the groups' ability to radicalize and recruit individuals who are receptive to extremist messaging. Social media has also allowed both international and domestic terrorists to gain unprecedented, virtual access to people living in the United States in an effort to enable homeland attacks. The Islamic State of Iraq and ash-Sham (ISIS), in particular, encourages sympathizers to carry out simple attacks wherever they are located—or to travel to ISIS-held territory in Iraq and Syria and join its ranks as foreign fighters. This message has resonated with supporters in the United States and abroad (FBI, 2021).[18]

Artificial Intelligence and Machine Learning are technological advances maliciously being used by FTOs and DVEs to increase their reach and distribution of social media disinformation.[19] These same tools can be utilized by "good actors" (government and the private sector, especially social media corporate giants) to prevent disinformation campaigns and protect the public, as noted previously.

THREATS CAN MOVE FROM THE WEB TO THE REAL WORLD VERY QUICKLY

The Q-Anon network, designated a domestic violent extremist threat in 2019, had a "PizzaGate" disinformation campaign that resulted in actual violent incidents.[20] West Point's Combating Terrorism Center has a detailed analysis of how their disinformation campaigns have generated lone offender participation in real world criminal activity.[21] The analysis and investigations into the January 6, 2021

[15] Lewis, J. & Ware, J. (2020, August 28). Spring provides timely reminder of Incel violence – and clarifies how to respond. International Center for Counter-Terrorism – The Hague. https://icct.nl/publication/spring-provides-timely-reminder-of-incel-violence/.
[16] https://www.fbi.gov/news/stories/fbi-releases-lone-offender-terrorism-report-111319
[17] Pew Research Center (2017, October 19). The future of truth and misinformation online. https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/
[18] https://www.fbi.gov/investigate/terrorism
[19] https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf
[20] https://www.tampabay.com/florida-politics/buzz/2020/08/26/politifact-qanon-hoax-has-been-linked-to-violence-fox-news-greg-gutfeld-falsely-claimed-it-hasnt/
[21] https://ctc.usma.edu/the-qanon-conspiracy-theory-a-security-threat-in-the-making/

attack on the U.S. Capitol – and its nexus to social media disinformation campaigns – is still in progress. At the very least, the FTOs have been amplifying and capitalizing on these events to further spread their own disinformation.[22]

An October 2020 U.S. Department of Homeland Security *Homeland Threat Assessment Report* noted that "Russian influence actors also posed [online] as U.S. persons and discouraged African Americans, Native Americans, and other minority voters from participating in the 2016 election" (DHS, 2020, pp. 12-13).[23]

That same report noted that foreign disinformation is not limited to national level impacts:

- China views a state or locality's economic challenges—including healthcare challenges due to COVID-19—as a key opportunity to create a dependency, thereby gaining influence. Beijing uses Chinese think tanks to research which U.S. states and counties might be most receptive to China's overtures.
- During the beginning of the COVID-19 outbreak, Beijing leveraged sister city relationships with U.S. localities to acquire public health resources. In February [2020], Pittsburgh shipped its sister city, Wuhan, 450,000 surgical masks and 1,350 coverall protective suits. Pittsburgh also established a GoFundMe account that raised over $58,000 to support Wuhan response efforts by providing medical supplies.
- In Chicago, Chinese officials leveraged local and state official relationships to push pro-Chinese narratives. Also, a Chinese official emailed a Midwestern state legislator to ask that the legislative body of which he was a member pass a resolution recognizing that China has taken heroic steps to fight the virus. (DHS, 2020, p. 13)[24]

TERRORIST OR PATRIOT: IT DEPENDS ON WHO'S KEEPING SCORE

Are "left-wing" groups such as Black Lives Matter and Antifa voicing political (and free speech) opinions and expressions or are they terrorist organizations? Can the same be said on the "right" for Three-Percenters and those groups that waive the Gadsden Flag (which also includes the National Rifle Association and the U.S. Navy)?

https://www.newsweek.com/antifa-activists-vow-keep-fighting-even-terrorists-1584622

https://komonews.com/news/local/washington-three-percenters-say-defense-department-is-wrong-to-label-them-extremists

https://www.newyorker.com/news/news-desk/the-shifting-symbolism-of-the-gadsden-flag

[22] https://www.njhomelandsecurity.gov/analysis/fto-propaganda-exaggerates-us-domestic-issues
[23] https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf
[24] https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

What can Emergency Managers do to increase their Readiness to Social Media Disinformation?

Actions may speak louder than words, but those words can incite violence and generate threats and risks. Emergency managers already know the power of social media as it relates to public information alerts and warnings. They themselves (and through their governmental leaders) must be the trusted source for accurate and timely information needed to maintain life safety, incident stabilization, and property/asset protection before, during and after a disaster. Many times, the communications (both to and from the public) are expedited and amplified by social media.[25] In some cases, social media may be the preferred (or only) way for members of the public to communicate with emergency management during a disaster. Disinformation campaigns can hinder or even threaten this method of communication – and can impact operations, finance/administration, planning, and logistics.

Emergency Managers should be connected to the Federal resources for Intelligence on FTO and DVE disinformation campaigns on a steady-state basis. This information should not be siloed within Law Enforcement only.

- If possible, **connect with the CISA** and other resources directly. Utilize governmental collaboration systems such as HSIN[26] and maintain a constant connection between law enforcement and emergency management. At the state level, utilize Fusion Centers[27] for this type of threat, in addition to the others.
- **Maintain your own cyber-monitoring capabilities.** Connect with academic researchers and other private sector partners who also monitor for cyber threats.
- **Do both of the above** – one example of this is the State of New Jersey. Their Fusion Center is populated by both their State Police (which runs the state's Office of Emergency Management as well – one of only two states in the Nation – Michigan being the other – to operate this way) and their Office of Homeland Security and Preparedness (OHS&P), which reports directly to the Governor's Office. In addition to generating its own threat analysis, the NJ OHS&P also has a robust Cybersecurity and Communications Integration Cell, which also provides public/private information alerts and sharing.[28] In many ways, there is too much data out there for social media monitoring (especially open-source data), including what is available on disinformation campaigns. Organizations may need to utilize aggregator and filtration software to help focus the view to the areas important to them specifically. One example of this is Swan Island Technologies TX360[29] product, which is used by Allied Universal Security amongst others, to help "Mitigate Risk and Improve Response and Recovery."[30]
- Countering disinformation campaigns requires the coordination of the organizations impacted with local, state, tribal and territorial governments. Emergency management can utilize their

[25] https://training.fema.gov/is/courseoverview.aspx?code=is-42
[26] https://www.dhs.gov/homeland-security-information-network-hsin
[27] https://www.dhs.gov/fusion-centers
[28] https://www.cyber.nj.gov/
[29] https://www.swanislandnetworks.com/about
[30] https://www.aus.com/security-systems/gsocaas/tx360

own public information capabilities, through their crisis communications team. This is true for private sector organizations as well as public ones.[31]

- Consider building communications templates in advance for disinformation campaigns, along the same lines as for fictitious disasters.
- Exercise these templates (and the team which will implement/activate them) on a regular, continual basis. Consider current examples in the media impacting other organizations (or even other countries) and exercise the "what if this had happened to us?" aspects. Evaluate those exercises and make needed improvements to the Planning, Organization, Equipment and Training of the Crisis Communications Team.
- Countering disinformation campaigns should not be limited to only "fighting back" via social media. The public may learn about the disinformation campaign from other sources and they themselves may not get their information via social media. And do not forget all the various languages that your constituents may use (including American Sign Language); as well as making sure your counter-messaging is accessible to people with disabilities and access/functional needs.[32]
- Finally, Emergency Managers are consequence management planners. The view that a Disinformation Campaign may be connected to another threat or hazard – or even that groups may be working in concert to promote complex coordinated attacks, is one which needs to be part of the Planning for both steady-state and disaster Operations. Reducing the "Pink Slice"[33] – what one does not know they do not know – about a threat or hazard to any operations is part of the continuous vigilance needed for Intelligence and Situational Awareness. The graphic on the following page illustrates how these clashes can occur – and sometimes even ad hoc collaborations and coordination between disconnected groups can make a bad situation worse:
    - 2017 Protest Events in Charlottesville, Virginia.[34] Multiple alt-right wing groups, white supremacy groups, anti-government groups had hand-to-hand combat events with Antifa, Black Lives Matter and other alt-left wings groups, even after propaganda campaigns indicated these would be "peaceful" free-speech protests.
    - January 6, 2021 political rally moves towards U.S. Capitol and becomes a massive civil unrest incident and a possible insurrection against the United States Government. Multiple alt-right wing groups, white supremacy groups, anti-government groups had hand-to-hand combat events with U.S. Capitol Police and other law enforcement agencies. Some have described the Protection and Prevention efforts as a failure of intelligence sharing amongst local, state and federal entities.[35]

[31] Sell, T.K., Hosangadi, D. & Trotochaud, M. (2020). Misinformation and the US Ebola communication crisis: Analyzing the veracity and content of social media messages related to a fear-inducing infectious disease outbreak. *BMC Public Health 20*, 550. https://doi.org/10.1186/s12889-020-08697-3

[32] https://www.govinfo.gov/content/pkg/CHRG-116hhrg39416/html/CHRG-116hhrg39416.htm

[33] https://blog.bartondunant.com/what-is-the-pink-slice/

[34] https://www.policefoundation.org/wp-content/uploads/2017/12/Charlottesville-Critical-Incident-Review-2017.pdf

[35] https://www.aei.org/foreign-and-defense-policy/intelligence/january-6-an-intelligence-failure/

When Multiple DVEs Collude and Clash

Do not assume that one set of DVEs only aligns with another (this graphic is just an example of one possible scenario). For example, Anti-Government Extremists could be aligned with White Racially Motivated Extremists, based on the specific incident - and some "groups" may even be on both sides of an issue - splintering themselves possibly by internal distinctions (i.e., race of the member).