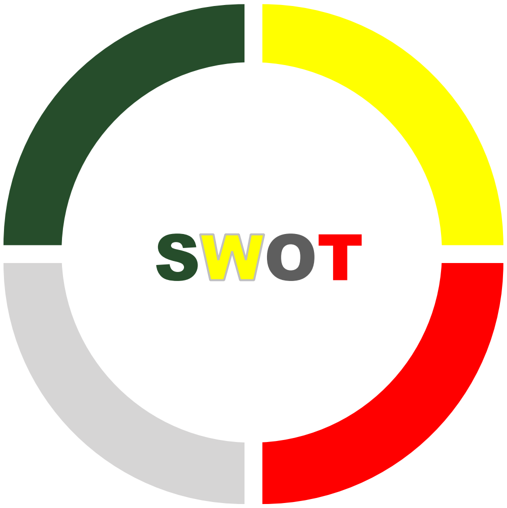


STRENGTHS

Communication
Collaboration
Cooperation
Coordination

WEAKNESSES

Lack of Coordination
Communications Gaps
Supply Chain
Dependence
Limited Planning

OPPORTUNITIES

Planning
Organizational Constructs
New Equipment &
Technologies
Training
Exercising

THREATS

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

NATIONAL
SECURITY POLICY
AND ANALYSIS
ORGANIZATION

STRENGTH ANALYSIS

MULTI-JURISDICTIONAL INTELLIGENCE SHARING: HOMELAND SECURITY INFORMATION NETWORK (HSIN)

Michael Prasad, CEM®
Emergency Management Intelligence
Analyst

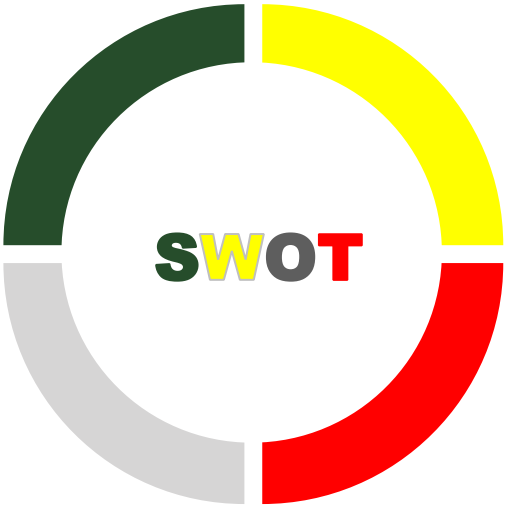
TLP: GREEN

UNCLASSIFIED

April 2022

STRENGTHS

- **Communication**
- **Collaboration**
- Cooperation
- Coordination



WEAKNESSES

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

OPPORTUNITIES

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

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 – one strength that law enforcement agencies within the United States is the Homeland Security Information Network (HSIN). **Emergency Managers**, not just law enforcement, need to keep in mind their organization's disaster readiness (resiliency) along the normal standard disaster phases 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]

This report will not include case examples from HSIN due to the Law Enforcement Sensitive (LES) Sensitive but Unclassified (SBU) designation of material.

[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

During an Incident is Not the Time to be Exchanging Business Cards

More information about HSIN can be found at https://www.dhs.gov/emergency-services. While designed as a law-enforcement collaboration and communication tool, the expansion to include emergency management should be included. There are a number of incident types which start out as law-enforcement only, yet quickly expand into fire, rescue, public health, transportation, critical infrastructure impacts, and more. There are also international intelligence concerns which transport themselves into U.S. Domestic threats and hazards, as well. The more that an Emergency Manager understands “left of boom”: in the Preparedness/Protection/Prevention phases, the better they are prepared – and ready – for the Response and Recovery work needed. These relationships and connections need to be working and in place, all the time – not just when something bad happens.

The concept of **Emergency Management Intelligence** is the curation and dissemination of these various intelligence aspects to Emergency Management officials before, during and after incidents happen. It takes what was designed by DHS through FEMA and applies it to an all-hazards approach, not just one that Prevents/Protects against Terrorism. The case for information-sharing beyond local law-enforcement into Emergency Management will be shown here through human-threat examples, but what is key to Emergency Management is the consistent use of tools and systems on an all-hazards approach. This is vital knowledge to have, for both complex coordinated attacks as well as attacks by adversaries during natural or other disasters, when our nation is perceived as being crippled or under duress already.

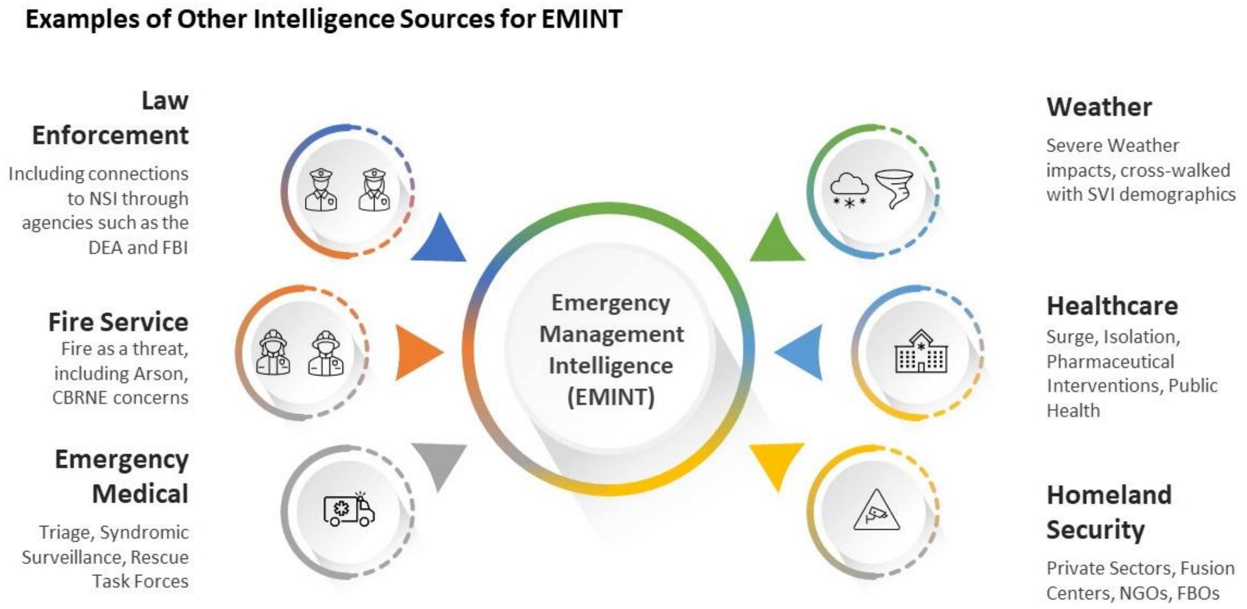

Examples of Other Intelligence Sources for EMINT
Law Enforcement
Including connections to NSI through agencies such as the DEA and FBI
Fire Service
Fire as a threat, including Arson, CBRNE concerns
Emergency Medical
Triage, Syndromic Surveillance, Rescue Task Forces
Emergency Management Intelligence (EMINT)
Weather
Severe Weather impacts, cross-walked with SVI demographics
Healthcare
Surge, Isolation, Pharmaceutical Interventions, Public Health
Homeland Security
Private Sectors, Fusion Centers, NGOs, FBOs

Figure 1 - From Barton Dunant. (c) 2021 - All Rights Reserved. Used with permission.

Under a Response/Recovery incident command structure by governmental and non-governmental partners, this is applicable to the Incident Action Planning, through Unified Command and the use of the **Intelligence** branch.

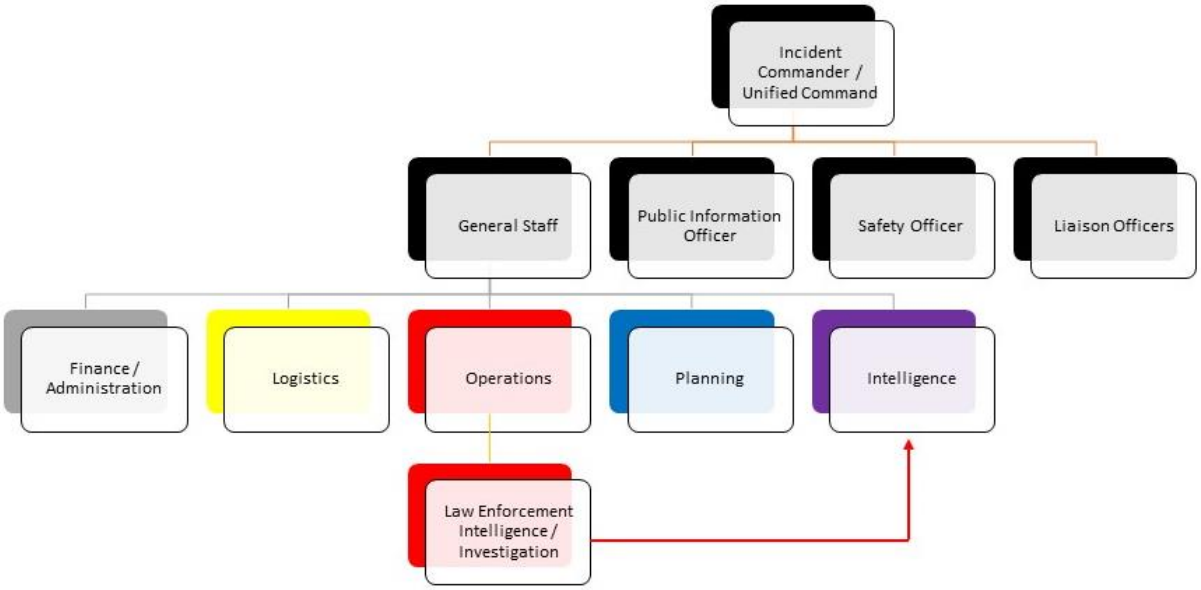

Incident Commander / Unified Command
General Staff
Public Information Officer
Safety Officer
Liaison Officers
Finance / Administration
Logistics
Operations
Planning
Intelligence
Law Enforcement Intelligence / Investigation

Figure 2 - From Barton Dunant. (c) 2021 - All Rights Reserved. Used with permission.

HSIN, as one of the tools in the toolbox for Emergency Responders, has a role in this curation and dissemination of Emergency Management Intelligence. Federal Intelligence Community members – both military and non-military – can make determinations on threats/hazards which should be shared with local law enforcement and other emergency management officials. The movement of classified status to sensitive but unclassified, can be performed – including with redaction and protection of civil rights of US persons. Emergency Management has a very specific – and important – use case need for this intelligence.

Examples of Emergency Management Intelligence Needs, Helped by HSIN

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.[2] 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.[3]
- **The Internet and social media**: International and domestic violent extremists have developed an extensive presence on the Internet through messaging platforms and online

[2] 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/.
[3] https://www.fbi.gov/news/stories/fbi-releases-lone-offender-terrorism-report-111319

> images, videos, and publications.[4] 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).[5]

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.[6] 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.

Connecting What Happens on the Internet to Real-World Threats

The Q-Anon network, designated as a domestic violent extremist threat in 2019, had a "PizzaGate" disinformation campaign that resulted in actual violent incidents.[7] 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.[8] The analysis and investigations into the January 6, 2021 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.[9]

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).[10]

[4] 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/

[5] https://www.fbi.gov/investigate/terrorism

[6] https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

[7] 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/

[8] https://ctc.usma.edu/the-qanon-conspiracy-theory-a-security-threat-in-the-making/

[9] https://www.njhomelandsecurity.gov/analysis/fto-propaganda-exaggerates-us-domestic-issues

[10] https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

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)[11]

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

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.[12] In some cases, social media may be the preferred (or only) way for members of the public to communicate with emergency

[11] https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf
[12] https://training.fema.gov/is/courseoverview.aspx?code=is-42

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[13] and maintain a constant connection between law enforcement and emergency management. At the state level, utilize Fusion Centers[14] 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 (who also operate that state's Office of Emergency Management – 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.[15] 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[16] product, which is used by Allied Universal Security amongst others, to help "Mitigate Risk and Improve Response and Recovery."[17]
- Countering disinformation campaigns requires the coordination of the organizations impacted with local, state, tribal and territorial governments. Emergency management can utilize their own public information capabilities, through their crisis communications team. This is true for private sector organizations as well as public ones.[18]
- 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

[13] https://www.dhs.gov/homeland-security-information-network-hsin
[14] https://www.dhs.gov/fusion-centers
[15] https://www.cyber.nj.gov/
[16] https://www.swanislandnetworks.com/about
[17] https://www.aus.com/security-systems/gsocaas/tx360
[18] 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

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.[19]
- 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.

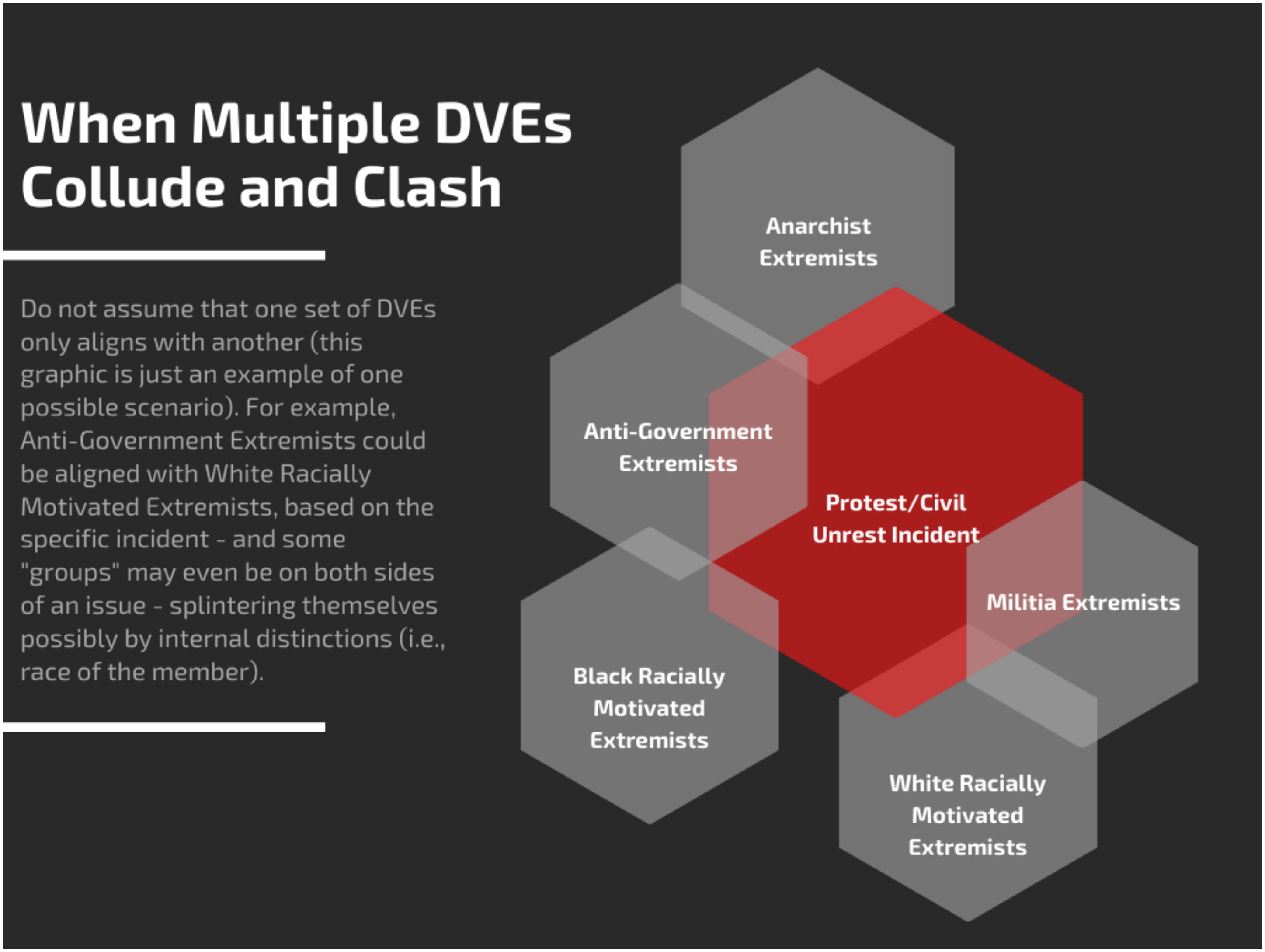
OUR ADVERSARIES COORDINATE, COLLABORATE, COOPERATE, AND COMMUNICATE AS WELL

Reducing the “Pink Slice”[20] – 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 at the end of this report 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.[21] 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.
- A 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 shortfalls that day in the Protection and Prevention efforts, as a failure of intelligence sharing amongst local, state and federal entities.[22]
- While Emergency Managers do not necessarily need to consider whether the COVID-19 pandemic was itself a terrorist act (the causality – or why – of incidents, disasters, etc. is not as critical as the adverse impacts generated), COVID-19 certainly had an impact on DVEs and FTOs. Pandemics – especially worldwide ones – may be considered a

[19] https://www.govinfo.gov/content/pkg/CHRG-116hhrg39416/html/CHRG-116hhrg39416.htm
[20] https://blog.bartondunant.com/what-is-the-pink-slice/
[21] https://www.policefoundation.org/wp-content/uploads/2017/12/Charlottesville-Critical-Incident-Review-2017.pdf
[22] https://www.aei.org/foreign-and-defense-policy/intelligence/january-6-an-intelligence-failure/

“global natural experiment that offers insight into causal processes”[23] by terrorists and extremists, for their own nefarious purposes.



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).

Anarchist Extremists
Anti-Government Extremists
Protest/Civil Unrest Incident
Militia Extremists
Black Racially Motivated Extremists
White Racially Motivated Extremists

[23] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7790481/

NATIONAL
SECURITY POLICY
AND ANALYSIS
ORGANIZATION

THREAT ANALYSIS

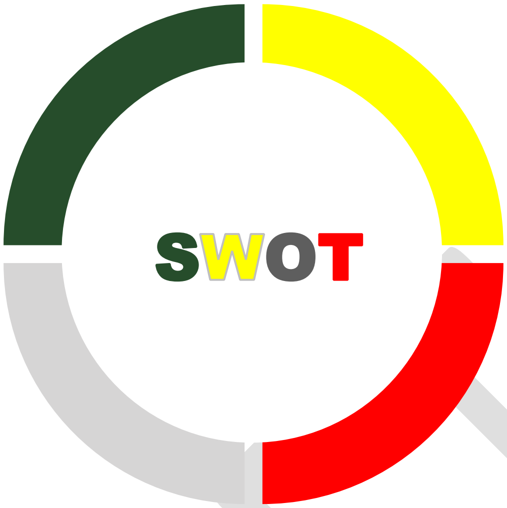
DOMESTIC VIOLENT EXTREMISTS: U.S. IMPACTS FROM EUROPEAN VEHICLE-BORNE ATTACKS

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

As part of a standard "SWOT" Analysis – the aspect of **Domestic Violent Extremists (DVEs)** 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 – includes the adverse impacts that can be generated by these specific threats and others. Tools and techniques – along with the organization's strengths of collaboration, coordination, cooperation and communication – to and from the military and civilian intelligence agencies can assist Emergency Management practitioners at all levels of government. It is crucial that Emergency Managers 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, methodologies and tradecraft of Foreign Terrorist Organizations (FTO) can be seen in many of these DVE's – whether they are directly influenced and/or sponsored (such as the Homegrown Violent Extremists or HVEs) or are indirectly studied and researched by the DVEs.

Using the experience and knowledge from historical DVE attacks in Europe by means of Vehicle-Borne Attacks (VBAs), can assist Emergency Management practitioners (not just Law Enforcement Officials) with Protection and Prevention missions. This Intelligence is also applicable to the Response Phase Incident Action Planning, to Unified Command for continuous Situational Awareness.

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 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

European DVE Attack Method: Vehicle Ramming Attacks on soft targets and crowded places

Europe has experienced an increasing number of Vehicle Ramming Attacks (VRAs) (also known as Vehicle-Borne Attacks or VBAs) in the last five years. In many countries where the access to deadly weapons of mass destruction (i.e., high-capacity guns, explosives, etc.) is significantly restricted, access to large vehicles requires minimal capability on the part of the attacker. These attacks can and do have significant impacts to crowded places, especially those “soft targets” with low levels of physical security protection and prevention barriers. VRAs are complicated, complex and chaotic incidents (Snowden & Boone, 2007):

- In April 2017, a stolen 30-ton commercial truck was used to target pedestrians in a busy shopping area in Stockholm, Sweden, killing four people and injuring 15. Undetonated explosives were found in the truck.
- In March 2017, a rental car was used to target pedestrians walking on Westminster Bridge in London, England, killing four people and injuring 40. The assailant abandoned his vehicle and proceeded to Parliament, where he killed a police officer with a knife.
- In July 2016, an ISIS-inspired individual used a 19-ton rental truck to attack pedestrians watching a fireworks display in Nice, France, killing 86 people and wounding more than 430. (U.S. Department of Homeland Security, n.d.)

In many cases, these successful attacks were inspired by and even encouraged by Foreign Terrorist Organizations (FTOs) – and which further inspired attacks in the United States such as:

- In October 2017, an ISIS inspired individual used a commercial-grade rental truck to attack pedestrians on a busy bicycle path near lower Manhattan, New York City, killing 8 and injuring more than 11 others. A pellet gun and a paintball gun were recovered from the scene. (U.S. Department of Homeland Security, n.d.)
- In November 2016, a student used his car strike pedestrians on a sidewalk at Ohio State University, injuring six people. He then left the vehicle and attacked five other people with a knife, before being shot and killed by a police officer. (Smith, Pérez-Peña, & Goldman, 2016)

Distinctly different from attacks originating *from* vehicles to others - or attacks *on* vehicles - the VRAs specifically use the size, shape, power and physics of the vehicle itself to cause death and destruction. According to the RAND Database of Worldwide Terrorism Incidents which has catalogued more than 40,000 worldwide terrorism incidents between 1968 and 2009, there were very few of these types of attacks. During that research timeframe vehicles were attacked carrying VIPs and military officers (high value targets); vehicles were used in attacks on embassies and other high visibility/high-value targets (car bombs, grenades and incendiary devices launched from vehicles, etc.) and also vehicle-on-vehicle attacks (including vehicles ramming each other) occurred (Rand, n.d.). Jenkins and Butterworth, in their 2019 report, noted that there have been 184 worldwide vehicle ramming attacks since 1964, but that 70% of these have occurred since 2014 – and VRAs which occurred in Europe or the United States accounted for more than half of all of the recent VRAs. (Jenkins & Butterworth, 2019).

Unlike the vast majority of vehicle-related attacks noted in the RAND database which occurred in conflict zones around the world, VRAs have become the weapon of choice for mentally unstable individuals and those who have been inspired by the rhetoric of jihadists. Both ISIS and al Qaeda encouraged VRAs as early as 2010, but the 2016 issue of *Rumiyah* appeared to have sparked a contagion of attacks, which appears to have peaked in

2019. That call from jihadists for VRAs on soft targets may have been written in response to the July 2016 truck VRA in Nice, France (Jenkins & Butterworth, 2019).

Still a worldwide concern: VBIEDs and now FAVBIEDs

While the focus of this article has been on VRAs, there continues to be a worldwide threat from Vehicle-Borne Improvised Explosive Devices (VBIEDS). Any emphasis on physical blocking devices or architectural design to reduce the impact of potential VRAs, should not replace continued vigilance and Protection/ Prevention aspects of Preparedness for VBIEDs.

And, with the ability for more autonomous vehicle capabilities – and the future state of fully autonomous vehicles (i.e., driverless vehicles), unfortunately this can become another tool for terrorists: The Fully Automated Vehicle-Borne Improvised Explosive Devices (FAVBIEDs). Mitigation efforts against FAVBIEDs must expand upon those in place now for VBIEDs and VRAs (Knopf, 2019).

While the FTO aspect of inspiring *anyone* (including those mentally unstable individuals, would-be jihadists, etc.) is certainly a concern, there are also DVEs who research and study these historic incidents, and can utilize vehicles for attacks on targeted groups/individuals as well as general soft targets such as public gatherings, pedestrian shopping areas, etc. Miller & Hayward also noted the imitative contagion factors itself (aligned along the social theory of Gabriel Tarde):

> These waves of imitative radiation are evident both internationally (where global ramming incidents have gone from insignificance to over 40 per year within two years) and at a more localized, micro-level. For example, on the 21 December 2014, 11 civilians were injured in Dijon, France, when a mentally unstable '40-year-old man of Arab origin' used a Transit-style van as a weapon in five parts of the city in the space of 30 minutes. Within 24 hours, a Frenchman, with a history of petty crime, alcoholism and mental health issues drove his van into shoppers at a Christmas market in Nantes, injuring ten. He then stabbed himself 13 times in the chest with a knife. Authorities believe he had no political or religious motive, but was directly inspired by the Dijon incident the previous evening (Miller & Hayward, 2019, p. 15)

Massive media coverage of these VREs, the easy access to vehicles (as compared to weapons) and the allure of instant fame can also trigger individuals to conduct VREs, especially as ripples of VRE waves, which have occurred. Some are targeted attacks (against groups, individuals, low-risk/high-impact areas, etc.) and others are random. As there is no single profile for a VRE attacker, the ability to conduct pre-incident Intelligence for Prevention and Protection is very limited.

Emergency Managers need to focus on the physical aspects of Mitigation, not the actors

While national defense and law enforcement may be focusing on the Intelligence aspects of Protection and Prevention (Preparedness) to reduce or eliminate the adverse impacts of VREs by stopping the actor; Emergency Managers must take a holistic approach that concentrates on mitigating those adverse impacts on the action itself – the VRA (along with VBIEDs/FAVBIEDs). If the vehicle can be stopped from getting to the crowd/target, its ability to be a weapon of mass destruction is significantly reduced. The reason for the VRA is immaterial to the Emergency Manager – only the fact that all soft targets must be protected against VRAs; and if a VRA does occur the swift medical response by members of the public and emergency responders will help save the lives of those who are injured.

Physical Mitigation activities fall under a concept called Crime Prevention Through Environmental Design (CPTED). Physical barriers – both permanent ones such as elevating areas accessible via stairs and ramps, trench-dug bollards, etc.; and temporary ones such as planters and barricades are both deterrents and tangible protection elements. In many cases the permanent modifications (or initial implementation as part of the initial facility/streetscape design) can be flexible to allow for vehicular traffic at some points and pedestrian-only traffic at other times:

> Portable barriers can be towed into place and setup in as little as 15 minutes to block off certain streets during a festival, for instance, and also allow for easy ingress and egress of approved vehicles. Bollards are a more permanent solution and can either be fixed or manually controlled by users who can raise or lower them depending on the circumstances (Griffin, 2017, p. 1).

The U.S. Department of Homeland Security (USDHS) also has recommendations on Mitigation strategies and Protective measures (U.S. Department of Homeland Security, n.d.); as does the Joint Counterterrorism Assessment Team (a collaboration by the National Counter Terrorism Center, USDHS, the U.S. Federal Bureau of Investigation and others) (Joint Counterterrorism Assessment Team, 2020). Europeans have also studied VRAs and possible Mitigation efforts along the same lines of CPTED (Jasiński, 2018). The same standards and ratings criteria used for CPTED devices such as sally ports (Thomas, 2017) and anti-ramming barriers (U.S. Army Corps of Engineers Protective Design Center, 2014) at critical infrastructure key resource (CIKR) sites, should be applied to soft-target areas.

And while coordinating with Law Enforcement on securing the scene for Investigation, Emergency Managers have a higher priority of coordinating and resourcing medical support to those injured during the VRA.

What is described as the “Golden Hour” and “Platinum Minutes” of trauma care (Daban, Falzone, Boutonnet, Peigne, & Lenoir, 2014), the quick response by medical professionals and others has been the focus of on-scene medical care of VRA and other Mass Casualty Incident (MCI) victims. While there is some dissent (Rogers & Rittenhouse, 2014) on these axioms (i.e., the rapid transport of victims from a scene has the potential for speeding accidents itself), those with profuse bleeding need to be stabilized immediately. The proper use of tourniquets – even by laypersons with minimal training – can save lives. In many of the same ways non-medical professionals have been trained to use Automatic External Defibrillation (AED) devices, taught CPR and even trained on administering NARCAN® (naloxone) for suspected drug overdoses; bleeding control techniques and equipment can be made available to non-medical professionals in advance of any incident. Equipment can also be strategically pre-positioned at high-risk areas, as AEDs are now in public spaces. The *Hartford Consensus* (Stop the Bleed)

Emergency Managers have broader responsibilities than just Law Enforcement

While there are elements of Law Enforcement primarily responsible for Protection, Prevention and Response missions associated with VRAs; the coordination of those missions aligning multiple organizations (Police, Fire, Emergency Medical Services, Public Works, Public Health, etc.) across the entire disaster cycles phases of Preparedness (Protection/Prevention), Response, Recovery and Mitigation. For many one-time public events involving crowds, the Preparedness activities to mitigate against the adverse impacts of a VRA would be led by the local law enforcement officials, but would need the cooperation, coordination, collaboration and communication with many other groups, departments, agencies, etc. That is the role of Emergency Management.

In addition to protecting the event itself from VRAs (or even against accidents simulating the impacts of a VRA), the overall community still needs access to emergency services in and around the area of the event. Bollards and barricades set up for the event cannot block emergency routes for ambulances and fire apparatus, without alternate routes and staging being established and coordinated in advance.

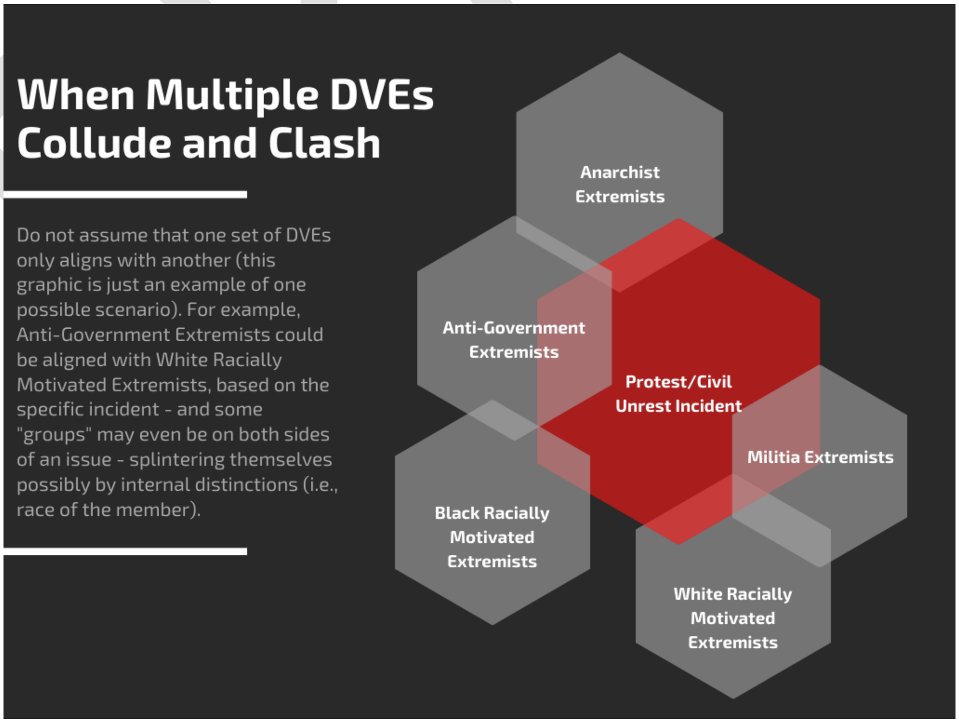
became the national policy for bleeding control in the United States, after the active assailant attack at the Sandy Hook Elementary School in Newton, CT in 2012 (American College of Surgeons, n.d.). There is even a protocol for Emergency Medical Services to bring a bag of tourniquets and other bleeding control supplies and “toss it to the crowd” so that pre-trained bystanders can assist, where there are not enough initial first responders on-scene.

Consequence Management aspects must be considered as well

While the VRA incident itself is a consequence of a threat becoming an attack; the additional consequence management planning (and anticipatory actions) must be considered that this attack could be part of a Complex Coordinated Attack. That means other sites could be at risk, first responders arriving on-scene could be attacked via secondary attacks and soft targets involved in the triage and treatment (hospitals, ambulance assembly points, staging areas, etc.) may be the subjects of attacks as well. Operational missions must be established for on-scene and off-scene security and responder accountability. Interoperable communications (including advance establishment of backups, if primary channels are compromised), Sally Port protocols for hot zones, strict credentialling standards and other criteria for Complex Coordinated Attacks must be utilized.

Well-planned events take into consideration the positives of people flow (for economic benefit, avoidance of traffic concerns, etc.) while protecting that population and the surrounding ones with CPTED and effective fire safety and emergency medical response access (Kennedy, 2020). On the other hand, failing to protect against the possibility of a VRA – especially when the Intelligence and prior actions indicate DVEs are poised to utilize any means possible for acts of violence – can lead to significant tragedies (After Charlottesville, 2018).

Also, it should be noted that since VRAs are sometimes crimes of opportunity, they may not be the *modus operandi* of the specific DVE, nor is this threat limited to DVEs. A VRA may be the result of someone fleeing the scene of another threat (The Guardian, 2020) – or the spontaneous product of the synergy when multiple groups of DVEs come together.



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).

Anarchist Extremists
Anti-Government Extremists
Protest/Civil Unrest Incident
Militia Extremists
Black Racially Motivated Extremists
White Racially Motivated Extremists

References

After Charlottesville. (2018). *Contexts, 17*(1), 16-27. doi:https://doi.org/10.1177/1536504218766539

American College of Surgeons. (n.d.). *The Hartford Consensus*. https://www.facs.org/about-acs/hartford-consensus

Daban, J.-l., Falzone, E., Boutonnet, M., Peigne, V., & Lenoir, B. (2014, September). Wounded in action: The platinum ten minutes and the golden hour. *Soins. Chirurgie, 59*, pp. 5-14. doi:10.1016/j.soin.2014.06.005

Griffin, J. (2017, May 5). *Stopping vehicle-borne terror attacks*. Security Infowatch.com. https://www.securityinfowatch.com/home/article/12332209/stopping-vehicleborne-terror-attacks

Jasiński, A. (2018, January 17). *Protecting public spaces against vehicular terrorist attacks.* doi:10.4467/2353737XCT.18.019.7992

Jenkins, B. M., & Butterworth, B. R. (2019). *"Smashing into crowds" - An analysis of vehicle ramming attacks.* Mineta Transportation Institute Publications. https://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1291&context=mti_publications

Joint Counterterrorism Assessment Team. (2020, December 18). *First Responder Tool Box.* https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/NCTC-FBI-DHS_Vehicle-Borne_Attacks-_Tactics_and_Mitigation-survey.pdf

Kennedy, M. (2020, January 1). *Event planning in a downtown district*. Fire Engineering.com. https://www.fireengineering.com/fire-prevention-protection/event-planning-in-a-downtown-district/#gref

Miller, V., & Hayward, K. (2019, January). 'I did my bit': Terrorism, Tarde and the vehicle ramming attack as an imitative event. *The British Journal of Criminology, 59*(1), 1-23. doi:https://doi.org/10.1093/bjc/azy017

New Jersey Office of Homeland Security & Preparedness. (2021). *New Jersey Predictive Threat Analysis.* State of New Jersey. https://www.njhomelandsecurity.gov/analysis/new-jersey-predictive-threat-analysis

Rand. (n.d.). *RAND database of worldwide terrorism incidents*. https://www.rand.org/nsrd/projects/terrorism-incidents.html

Rogers, F., & Rittenhouse, K. (2014, Spring). The golden hour in trauma: Dogma or medical folklore? *The Journal of Langaster General Hospital*, pp. 11-13. http://jlgh.org/JLGH/media/Journal-LGH-Media-Library/Past%20Issues/Volume%209%20-%20Issue%201/Rogers9_1.pdf

Smith, M., Pérez-Peña, R., & Goldman, A. (2016, November 28). *Suspect Is killed in attack at Ohio State University that injured 11*. https://www.nytimes.com/2016/11/28/us/active-shooter-ohio-state-university.html

Snowden, D., & Boone, M. (2007, November). A leader's framework for decision making. *Harvard Business Review*, 69-76. https://www.chds.us/ed/resources/uploads/2020/10/A-Leaders-Framework-for-Decision-Making-Snowden-and-Boone.pdf

The Guardian. (2020, December 12). *Multiple people injured after vehicle plows into crowd at New York protest*. TheGuardian.com. https://www.theguardian.com/us-news/2020/dec/11/new-york-vehicle-crowd-injuries-black-lives-matter-protest#:~:text=A%20vehicle%20plowed%20into%20a,York%20City%20police%20department%20said.

Thomas, L. (2017). Chapter 15 - Specialized Portal Control Devices and Applications. *Electronic Access Control (2nd Edition*, pp. 237-253. doi:10.1016/B978-0-12-805465-9.00015-4

U.S. Army Corps of Engineers Protective Design Center. (2014, January). *DoD anti-ram vehicle barrier list .* https://www.usace.army.mil/portals/2/docs/protection/dod_anti-ram_vehicle_barriers_january_20141.pdf

U.S. Department of Homeland Security. (n.d.). *Vehicle ramming: Security awareness for soft targets and crowded places.* https://www.cisa.gov/sites/default/files/publications/Vehicle%20Ramming%20-%20Security%20Awareness%20for%20ST-CP.PDF

NATIONAL SECURITY POLICY AND ANALYSIS ORGANIZATION

THREAT ANALYSIS

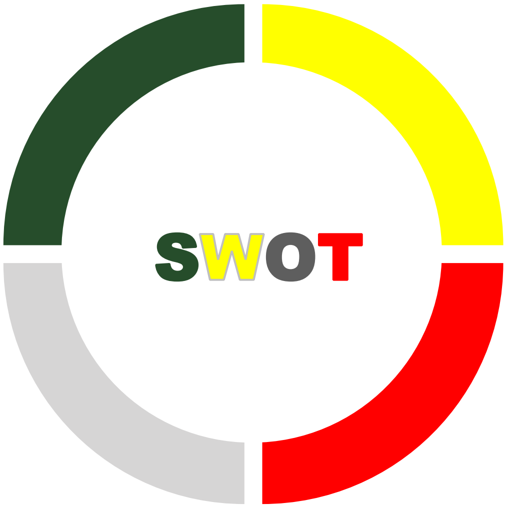
FOREIGN TERRORIST ORGANIZATIONS & ROGUE NATIONS: SOCIAL MEDIA DISINFORMATION CAMPAIGNS

Michael Prasad, CEM®
Intelligence Analyst

TLP: GREEN
UNCLASSIFIED

STRENGTHS

- Communication
- Collaboration
- Cooperation
- Coordination



WEAKNESSES

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

OPPORTUNITIES

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

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]

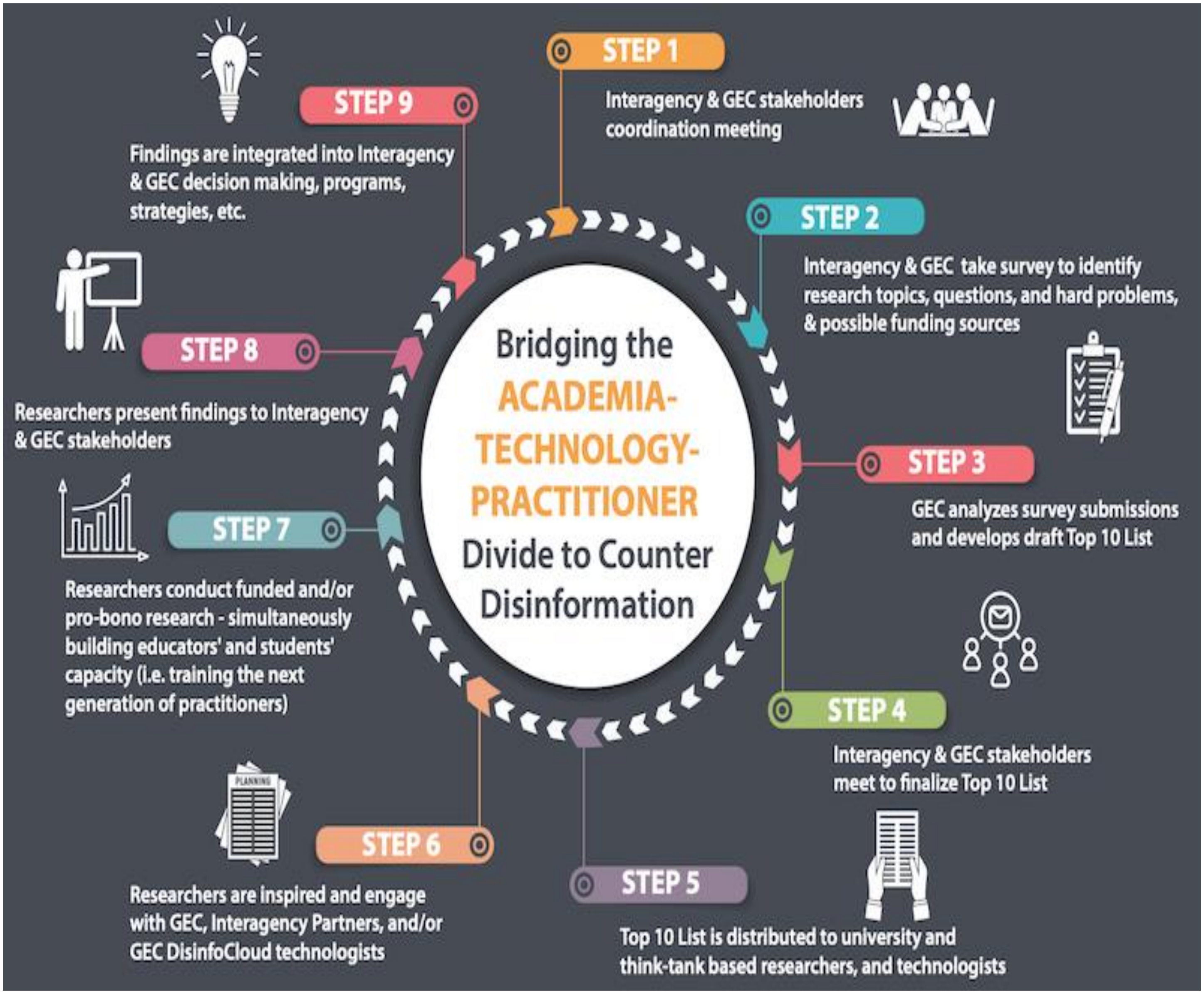

Bridging the ACADEMIA-TECHNOLOGY-PRACTITIONER Divide to Counter Disinformation
STEP 1
Interagency & GEC stakeholders coordination meeting
STEP 2
Interagency & GEC take survey to identify research topics, questions, and hard problems, & possible funding sources
STEP 3
GEC analyzes survey submissions and develops draft Top 10 List
STEP 4
Interagency & GEC stakeholders meet to finalize Top 10 List
STEP 5
Top 10 List is distributed to university and think-tank based researchers, and technologists
STEP 6
Researchers are inspired and engage with GEC, Interagency Partners, and/or GEC DisinfoCloud technologists
STEP 7
Researchers conduct funded and/or pro-bono research - simultaneously building educators' and students' capacity (i.e. training the next generation of practitioners)
STEP 8
Researchers present findings to Interagency & GEC stakeholders
STEP 9
Findings are integrated into Interagency & GEC decision making, programs, strategies, etc.
PLANNING

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

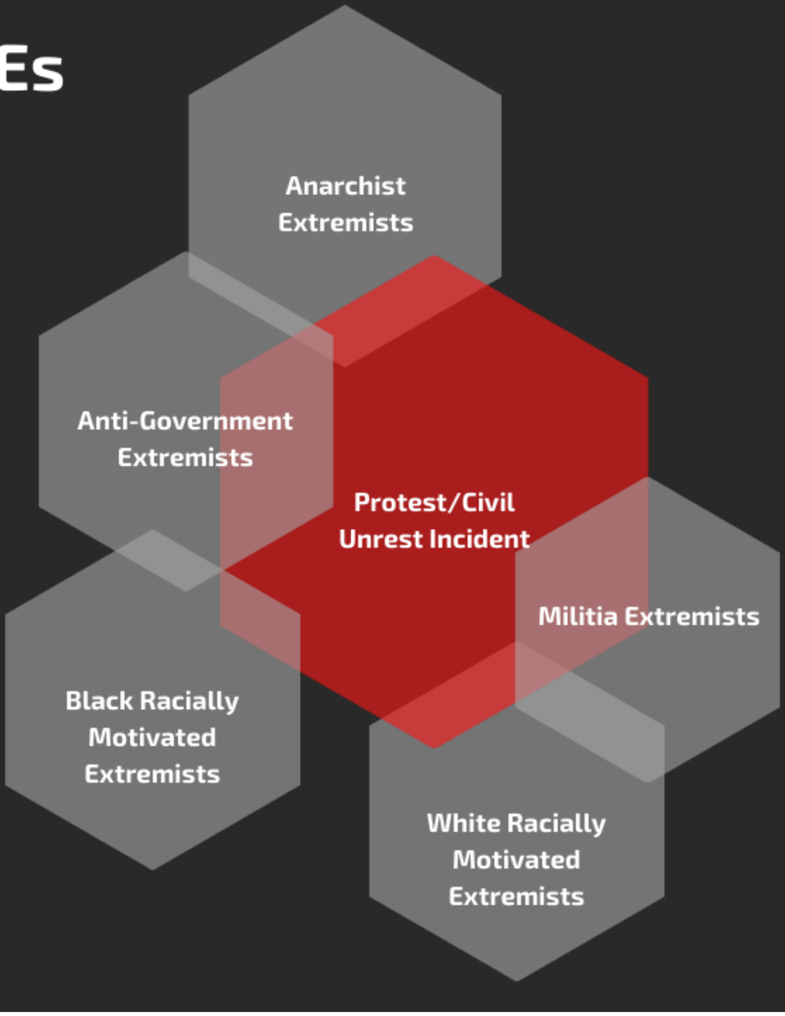
[33] https://blog.bartondunant.com/what-is-the-pink-slice/

[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).



Anarchist Extremists

Anti-Government Extremists

Protest/Civil Unrest Incident

Militia Extremists

Black Racially Motivated Extremists

White Racially Motivated Extremists