EXECUTIVE SUMMARY

DIGITAL FORUM
ON TERRORISM PREVENTION

- A Report on Trends and Insights -

DECEMBER 2017

- TABLE OF CONTENTS -

1. Executive Summary

Recent advances in technology have underpinned the growth of social media and messaging platforms online. However, that same technology has also enabled terrorist exploitation of the internet, where extremist organizations recruit, radicalize, and direct supporters. Since the July 2017 launch of the Global Internet Forum to Counter Terrorism--an organization led by Facebook, Microsoft, YouTube, and Twitter--there has been tangible progress made by both government and technology companies despite the complexity of the issues involved. At the same time, there is now a greater recognition that there will not be a silver bullet solution or a single solution to stopping terrorist activity online but that innovative public and private partnerships will be needed. At the Digital Forum on Terrorism Prevention in late September 2017, experts from government, the technology industry, startups, and community organizations gathered to discuss this topic, highlighting the following themes:[*]

Content Volume: In targeting terrorist content online, both the timing and volume of content have posed challenges. Participants observed that content must be taken down rapidly to prevent its viral spread; absent intervention, two-thirds of terrorist content is re-shared within the first two hours of its lifecycle. With users around the world uploading over 400 hours of content every minute online, governments and technologists are developing tools to automatically detect and flag terrorist content. Recent strides in this area indicate that technological solutions will be among the most effective ways to manage voluminous terrorist content, with more than 75% of content takedowns driven by automation activated in a timely manner. Additionally, progress has been made fielding tools to help startups and smaller companies, which otherwise lack the capacity to manage terrorist content. However, there remain challenges in managing this issue as extremist groups migrate to encrypted messaging platforms, where monitoring is more difficult. Finally, aggressive content takedowns can have unintended negative effects. For example, videos of terrorist violence often serve as critical evidence in criminal prosecution; deleting this type content has hampered recent law enforcement activities against groups such as ISIS.

Counter-Messaging: While content can be taken down in automated ways, takedowns are not a panacea. Violent terrorist content is tested against the community guidelines and terms of service set by content platforms, which are too static to cover all extremist messages. Participants noted that there remains work to be done in tackling terrorist content driven by non-violent ideology and narrative as they don't violate the terms of service of social media platforms. Progress has been made in counter-message campaigns, developed in partnership with community-based organizations, which serve as credible messengers to disrupt ideological narratives. These efforts have been recognized with the need to be followed by rigorous research, evaluation, and data analysis. Additionally, ensuring these messages reach

[*] The views presented in this report reflect those of individual participants in the Digital Forum on Terrorism Prevention and do not necessarily represent the position of the United States government or Department of Homeland Security.

the intended audiences effectively remains a challenge, exacerbated by gaps in measurement of results against behavioral outcomes.

Online to Offline Interventions: As companies develop tools that allow organizations to identify users susceptible to terrorist content, participants opined that local-level interventions will be required to prevent their radicalization. In offline interventions with former extremists, focusing on underlying social and personal issues was found to be more effective than attempting to directly engage with or change political or ideological ideas. Online to offline "off-ramps" need to be developed in partnership with local organizations, mirroring methods used in related fields such as domestic violence and suicide prevention.

This year, the technology sector and non-governmental entities invested more resources and focus in research and programming around these topic areas--meaningful increases compared to previous years. These increases can be expected to create more opportunities for community organizations to intervene against radicalization in offline environments, but only if they can transition from online to offline intervention. As the private sector develops new technological tools to manage content, success here will require efforts to support local-level efforts, particularly to train credible local actors in digital techniques to bridge these gaps and execute this "last mile" of interventions. Continued efforts in funding, personnel, and information sharing are critical to effectively tackle this important issue on a global basis.

Activities and Progress over last 6 months:

June 2017: Facebook announced plans to hire 3,000 individuals to monitor illicit content. Separately, the Department of Homeland Security Office for Terrorism Prevention Partnerships announced the recipients of $10 million in grants awarded to community based organizations, with over $1.3 million or about 10% of the funding directed specifically to countering violent extremist narratives.

July 2017: The Global Internet Forum to Counter Terrorism (GIFCT) was formed, the first time major companies have come together to work on research and technology techniques while also committing to help smaller companies and startups tackle this issue.

September 2017: At the 72nd UN General Assembly, UK PM May, Italian PM Gentiloni and French President Macron addressed world leaders on this topic. Google.org announced they were committing $5 million over the next two years to invest in nonprofits working on anti-radicalization efforts. The Digital Forum on Terrorism Prevention, led by the US government interagency Countering Violent Extremism Task Force and co-presented by the DHS Office for Terrorism Prevention Partnerships, Tech Against Terrorism, the George Washington Program on Extremism, and Fifth Tribe brought together 144 experts from industry, community organizations, research, and technology to discuss ongoing work and challenges.

October 2017: The seven Ministers of Interior met at the Italian-hosted G7 to discuss how to prevent the terrorist use of the Internet – with the participation of the private sector. The ministers considered how intelligence agencies can mitigate the threat from aspiring and returned foreign fighters, and how to disrupt channels being used to finance terrorist organizations.

2. Outreach and Development of This Report

Digital Forum on Terrorism Prevention

Following the September 2017 UN General Assembly Meeting on Terrorist Use of the Internet, 144 technologists and terrorism prevention leaders convened in Washington, D.C. for the Digital Forum on Terrorism Prevention. The forum was led by the US government interagency Countering Violent Extremism Task Force and co-presented by the DHS Office for Terrorism Prevention Partnerships, Tech Against Terrorism, the George Washington Program on Extremism, and Fifth Tribe. The purpose of this forum was to increase information sharing among terrorism prevention stakeholders and to showcase technologies and techniques developed to counter terrorist use of social media. The forum was attended by a wide array of government entities, startups, researchers, and representatives from private companies.

The event hosted a series of "lightning" talks by leaders from the technology, media, data science, and research sectors. These were followed by a panel discussion to discuss case studies, successes and challenges ahead. Additionally, 12 organizations hosted booths across the venue to showcase their work. An online video of the forum was also broadcasted to 200 terrorism prevention experts and leaders who were unable to attend the event in person.

This report, contributed by participants from the digital forum, summarizes the key outcomes and takeaways for policy consideration.

3. Trends from Government, Research & Industry

With the advent of social media, data has shown that extremists from around the world have the ability to recruit in increasing numbers. Groups such as ISIS have complemented their use of open social media platforms by increasingly using private, encrypted channels. Social media platforms have already made strides in content takedown and managing referrals of content through hash-sharing databases. Despite numerous existing initiatives, participants noted that silos still exist within government, research, and industry. They highlighted the value of sharing insights, as well as the productivity of practitioner-level forums to allow for information sharing.

Some key insights shared by the experts include:

1. **Targeting multiple forms of extremism:** Participants discussed the need for governments and industry to focus not only on deducing outcomes from online behavior of groups such as ISIS, but also on other emerging violent extremist threats. The exploitation of the internet by violent extremists will continue to evolve, and there is an imperative to look across the whole picture as extremist groups and movements glean insights from each other.
2. **Timing is Key:** Several private-sector experts agreed that the timing and speed of messaging responses to extremist content continues to be a critical factor in this online battle. Additionally, there remains a challenge in when and how to push appropriate counter-messaging aligned with real-time world events.
3. **Unintended Effects of Content Takedown:** While immediate content takedown is an important step to reduce the spread and volume of extremist content, researchers and academics warned of the difficulty in evaluating online behaviors as content moves into encrypted channels. Partnerships between industry and researchers are necessary to continue evaluating behavior patterns as takedown methods become more powerful.
4. **Growing Importance of Search Rankings:** Initiatives such as Jigsaw's Redirect Method--where searches for extremist content can be targeted and redirected to counter-narratives--have provided insight into how people respond to counter-messaging content. However, outside of the paid advertising landscape, it is still difficult for the technology sector to manage sensationalist terrorist content that is promoted in organic search rankings, especially with evolving keywords across multiple languages.

4. Trends from Data Science and Tools

Measurement & Data Analytics

While interventions, takedowns, and counter messaging efforts have ramped up to counter terrorist activity online, experts highlighted the fact that these efforts have not been consistently measured. This measurement gap deprives organizations of insight into which tactics work best against terrorist activities online.

Throughout the forum, experts identified key causal issues undermining measurements of online interventions:

- **Lack of Standard Measurements:** Even within government and private sector organizations, projects are utilizing different measurements for their reach and effects. This makes comparison virtually impossible. A few speakers demonstrated that with the use of standard social media metrics, it was possible to determine whether online campaigns were actually having their intended effects.
- **Need for Analytic Support:** Much as there is a lack of standard measurements in this space, there is a similar lack of unified analytic tooling to deal with the vast quantities of data collected around social media platforms. Participants noted that while many data tools are available, education was lacking to allow analysts to use these properly. Community organizations and governments also lack the ability to interpret many of these tools and translate these insights into policy, program, and action.
- **Data Trust and Privacy Rights:** Because much of the data about changes in perception and belief is derived from self-reported surveys, there is limited trust in the findings. Additionally, in collecting relevant data, participants expressed concerns for the preservation of privacy rights and public trust.

Ongoing efforts:

Engagements with smaller content providers: Tech Against Terrorism (ICT4Peace), the information sharing arm of the GIFCT, hosts global workshops to work with smaller companies which are designed to aid organizations with limited bandwidth to manage violent extremist content on their platforms. In late November, Tech Against Terrorism launched the Knowledge Sharing Platform, a set of tools to enable startups to help track and thwart terrorist content.

Training Local Community Organizations on Data Tools: Peace Tech Labs at the U.S. Institute for Peace provides "Peace Tech Exchanges" to deliver digital literacy training to organizations so that they can leverage low-cost technologies towards terrorism prevention. So far they have hosted 21 workshops in 9 countries. Beyond these workshops, Peace Tech Labs developed a startup accelerator, the Peace Tech Accelerator, to fund technology projects focused on peacebuilding and countering hate speech.

Improving Data Science and AI Driven Insights: A number of technology startups, including Omelas, Moonshot CVE, Graphika, and New Knowledge, are leveraging AI artificial intelligence and machine learning techniques to train computational models around macro-level patterns in violent extremist activity online. These tools support network analysis and the identification of proper indicators which can be measured by communities over time.

Technologist-led initiatives: Technologists that do not come from traditional terrorism prevention backgrounds have led independent projects due to personal interest. Among these are digital agencies like Fifth Tribe, which scraped extremist Twitter accounts and developed an open-source dataset. That data was used to engage over 45,000 data scientists on the data sharing platform Kaggle. Additionally, groups including Affinis Labs and American Abroad Media have hosted hackathons in communities around the world to recruit technologists in this online battle.

5. Trends from Online Counter-Messaging

Delivering Credible Messages

Counter-messaging has proved to be a critical tactic for tackling extremist content that remains undetected by terms of service enforcement on social media platforms. However, counter-messaging has many challenges. If done improperly, counter-messaging can have a "boomerang effect", potentially inflicting harm as well. Additionally, tactics used in traditional advertising are an overlooked element of successful targeting, especially understanding how users search and minimizing search engine optimization of extremist content.

Experts delivering counter-messaging campaigns noted the following trends:

- **Importance of credible voices involved:** The use of credible messengers has proven to be a critical component of successful counter messaging. Experts echoed the need for governments to stay away from trying to be these messengers, but rather should identify appropriate stakeholders and funding partners for this role. This type of credible voice-led influencer marketing allows campaigns to scale to intended audiences.
- **Broad reach is not always the right solution:** Speakers repeated throughout the day that most people are not violent extremists. To this point, large-scale messaging campaigns are often ineffective. In some cases, blanket mass campaigns can radicalize people by exposing them to an ideology they weren't previously aware of. In contrast, a campaign that reaches 100 people that reaches right individuals could be a more effective campaign to look at. A large opportunity for success in targeting extremists lies not in paid advertising but rather in mapping how extremists search for content. Conversely, large scale campaigns have an opportunity to impact and engage bystanders and communities.
- **Incorporating lessons from offline**: Speakers shared frustration that many online counter-messaging campaigns leave lessons learned from offline counter-messaging at the door, with a majority of messages focused on ideology which is often not an effective topic to discuss when trying to influence vulnerable individuals. Several experts have found that these tactics have more often than not been unsuccessful. This doesn't have to be the case, and elements learned from across creative advertising and offline efforts must be incorporated.

- **Investing in Experimentation and Sharing Failure:** Organizations have been eager to share successes, but they have been reluctant to share stories of campaign failure. For example, in programs that engage students in counter messaging, it is important to recognize that not all students will be successful; nonetheless, there will be many that develop effective creative campaigns.

- **Importance of information sharing:** Speakers noted the importance of sharing tactics to de-conflict campaign targeting. One speaker noted YouTube's well-intentioned experimentation with limiting the sharing of non-violent extremist videos to "view only" may have the unintentional consequence of depriving researchers from understanding communication patterns through video comments. The experts expressed a need to centralize effective campaigns to localize and cross-promote, while inserting local knowledge of drivers to these campaigns. One expert found a mix of embedding local knowledge with casual conversations around messaging had the best response rate.

Ongoing efforts:

Peacebuilding NGOs play a substantial role
A number of organizations involved in international development and peacebuilding, including the Institute for Strategic Dialogue, Search for Common Ground, and Creative Associates International, have been working for decades with industry, government, and researchers to develop counter-messaging campaigns and have valuable insight and experience to share

Involvement of different credible messengers and content creators
Programs such as Mythos Lab's work with comedians, YouTube Creators for Change involving YouTube Influencers, and Facebook's Online Civic Courage Initiative help organizations scale messaging tactics through different mediums. Additionally, through the "Peer to Peer: Challenging Extremism" competition, university students have developed campaigns to reach over 75 million people around the world to-date. In the United States, DHS has recently funded Masjid Muhammad to develop multimedia platform to engage one million Muslims with credible counter-messages. Programs such as the Against Violent Extremism Network engaged former extremists along for this fight, as well.

Partnering with advertising
Advertising firms and Search Engine Optimization companies such as MediaCom, Digitalis, and Breakthrough Media have been helpful partners in scaling campaigns that effectively leverage 21st century advertising techniques.

6. Next Steps: Guidance to Help Existing Efforts

Over the course of the Forum, participants contributed the following guidance for organizations working in the terrorism prevention online space:

Guidance 1 - Continued funding necessary to support community-level activities online

- While industry has helped with developing new tools, especially leveraging AI techniques, many experts noted there still remains a gap in mapping these solutions from online to offline environments. **Funding at the community level is necessary to solve this problem**. The DHS's 2017 $10 million offering to community-based groups is a model of how governments and philanthropists can help tackle this challenge with community partners.

Guidance 2 - Evaluation of successes in current activities in the space is critical; this requires new tools and long-term evaluation

- **Government insights on terrorist tactics and trends can help guide private sector and NGO action.** Participants applauded governments for their domain-specific expertise and the ability to see the big picture, linking crimes to their recruiting and radicalization precursors. Additionally, governments can help the technology sector better understand the online threat through delivering social media awareness briefings.

- With longer time horizons in mind, **governments can support long term thinking, research, and projects to counter terrorist activity online.** Breaking the cycle of quarterly objectives or funding that lasts for only 1-2 year periods may allow government-funded projects to better consider potential long term side-effects of approaches to counter terrorist activities online. This is critical where seemingly effective strategies negatively affect civil society in the long term. Additionally, governments can play a role in mandating for consistent sets of measurements across federally funded terrorism prevention programs.

Guidance 3 - Increase alignment between governments and the tech industry

- **Interactions between governments and the technology sector should explore the possibilities for alignment and compromise,** rather than operating in silos. Much as large technology companies engage in a form of diplomacy with governments, some participants from the private sector felt government was not doing the same. Both sides recognize that the internet is no longer an unregulated space, and they have shared interests in managing it.

- As private sector technology moves more rapidly than government-developed technology, **governments can work with technology companies to understand what tools are needed and possible for government efforts to succeed in the evolving online space.** Speakers noted governments cannot afford to determine technological solutions in a vacuum. Recent efforts have showed that private sector guidance can lead to outcomes sooner.

Guidance 4 - Convene working-level meetings between government entities and practitioners to boost community engagements

- **Increase multi-stakeholder meetings to allow for improved information sharing.** Participants noted the productiveness of multi-stakeholder, practitioner-level meetings such the Digital Forum on Terrorism Prevention to support dialogue and create connections among stakeholders who may not interact regularly.

- **Local Institutions can use Government and NGO resources to amplify and support tools and campaigns.** Where a startup or technology company develops an effective tool, a government partner or NGO can spread that tool widely to tackle terrorist activity.

- **By boosting digital literacy among local partners, governments can significantly increase their level of engagement with NGOs and the private sector.** These engagements allow governments to generate and measure effects in populations and issues which are seemingly outside of their control.

- **Governments can act as trusted partners to unify and de-conflict efforts against terrorism online, as their incentives are divorced from economic competition.** This is particularly important where information sharing is required, as companies would otherwise withhold information in order to preserve an economic advantage.