EXECUTIVE SUMMARY

The October 2020 Department of Homeland Security 'Homeland Threat Assessment' report clearly identifies foreign influence activity in the United States as a significant threat to national security. As one of the largest police departments in the United States, and a key partner with the U.S. government's interagency counterterrorism community, the LAPD is well-positioned to pilot the ABTShield disinformation-monitoring program specifically designed to counter this national cybersecurity threat. As Los Angeles readies to host the 2028 Olympic Games, ABTShield can provide additional levels of security for local, state, and federal entities preparing a secure environment for the Olympics.

THE THREAT

- Modern law enforcement operations require instant, up-to-date, and comprehensive data on digital/ social media activity. Reaction time is critical for managing crises, both from public safety and strategic communications perspectives.

- Online manipulation is flourishing. Malign actors are amplifying socially divisive and false narratives to sow division in American society, encourage conflict between political factions, and undermine trust in public institutions - including law enforcement and the government writ large. Manipulated internet traffic (positioning and promoting certain types of narratives), and activity by fake social media accounts on a variety of platforms promoting discord are a major threat to public safety.

- Aside from the public safety aspect of protest activity incited by social media activity, whether Antifa or nationalist right wing activity, The LAPD itself is being targeted by organized attacks of automated bots and trolls (e.g. police brutality misinformation and "defund the police" narratives). On current timeframes, even when malicious activity is detected after it has gone viral, it is often too late to avoid the consequences.

THE SOLUTION

ABTShield provides a comprehensive, client-tailored warning system (Information Operations radar) providing ongoing, real-time analysis of relevant internet traffic using AI, machine learning, and human analysis. ABTShield will identify emerging threats, tracking online activity that could signify new threats, delivering information on new "high volume" narratives and origin analysis (organic vs artificial). Our product will:

- Detect and analyze relevant narratives emerging in internet articles, tweets and comments - tracking client-identified areas of interests as well as newly-appearing topics (e.g. "LA riots", "police violence", "BLM protests", etc.) and entities (e.g. "LAPD", "Armenians", "Proud Boys", etc.)

- Analyze social reactions to news and articles (is a topic sticking and spreading in the information sphere?)

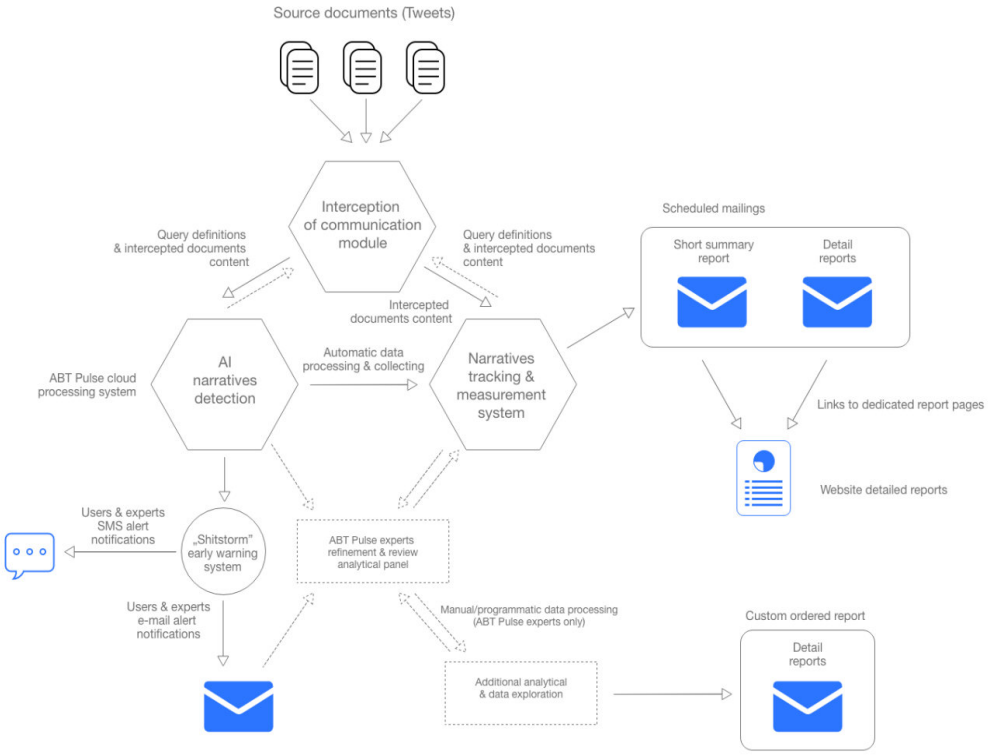
- Detect bot and troll attacks on publisher sites, webpages, commentary, forums, or social accounts based on ABTShield's proprietary, award-winning behavioral analysis.

ABTShield is fully scalable

- Not limited to a specific language or territory; it is topic/narrative driven
- Can be provided across the U.S.government interagency for similar threat analysis
- Has limitless possibilities in terms of analytics development (proposed R&D)
- Offers 24/7 flexibility for data access anywhere.

The ABTShield LAPD Strategy

The diagram below describes the support ABTShield can provide the LAPD. It is designed to give LAPD maximum information with minimal involvement (all dotted lines represent internal ABTShield processes, which do not require any LAPD action). ABTShield's customizable solution means LAPD may order in-depth reports on topics of specific interest to Command Staff or the



THE METHODOLOGY

ABTShield concentrates on three aspects of the disinformation process:

1. Disinformation

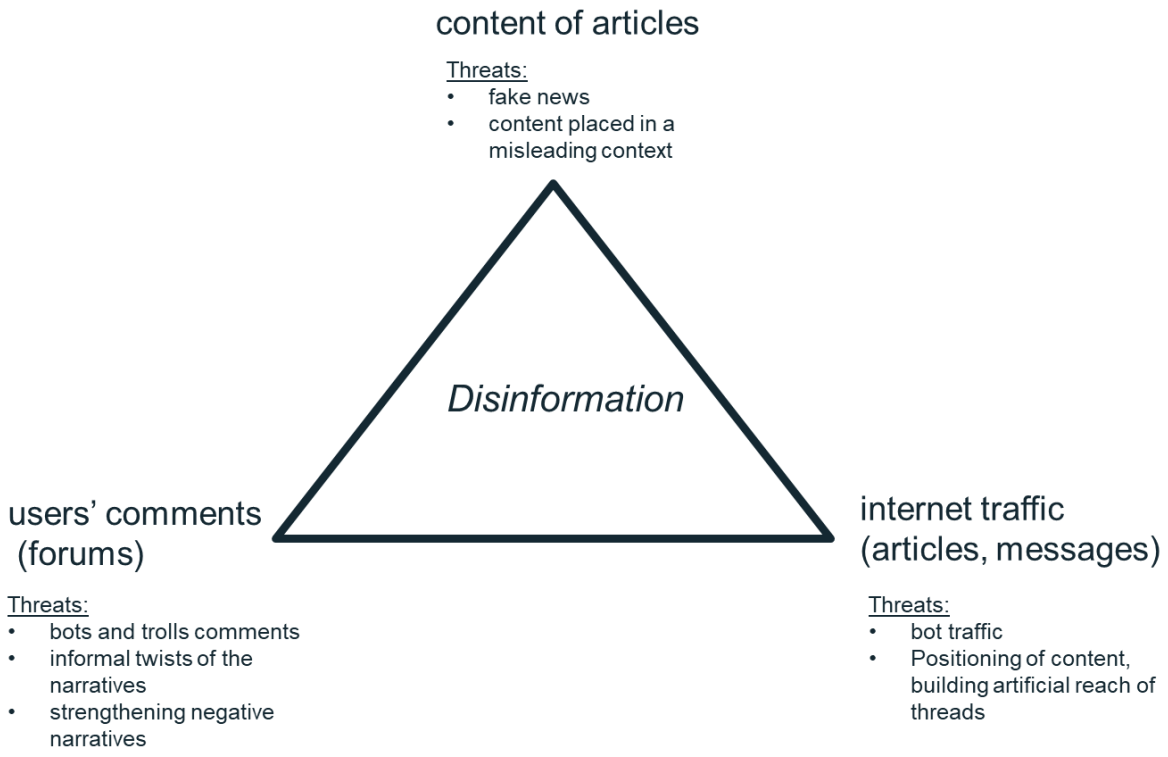
- Once a new trending theme is located online, we determine its authenticity. Once verified as false we identify it as a disinformation narrative.

2. Artificial traffic manipulating and amplifying disinformation

- It is estimated that approximately half of the Internet traffic is not generated organically i.e. not by active live users. The artificial traffic very often serves to position disinformation. We leverage publisher agreements to identify these situations.

3. Artificial accounts, social media comments generated by bot and trolls

- We analyze traffic on social media (twitter, facebook, youtube) and define if within a given topic/theme there exists disinformation generated in large numbers by bot accounts and trolls (specialized technologies or groups of paid operators of multiple accounts, created solely to conduct info operations)



<u>Behavioral analysis of traffic</u>

Sample questions:

- *What % of users commenting on the event are real and what % are robo-trolls?*

An internet bot is an automated computer program intended to perform certain tasks online instead of a human being. A great majority of bot-generated internet traffic comes from those meant to mimic human behaviour. This enables them to assume a fake identity and influence real human beings' opinions and decisions.

ABTShield identifies bot attacks through traffic analysis and end user account activity. ABTShield provides real-time results and identifies specific connection sources that are potentially dangerous.

We can detect them based on their behavioral patterns such as:

- Long or even uninterrupted operation
- Extraordinary performance or effectiveness
- Incredible rapidity of action
- Surprising randomness
- Abnormal variability

Comment analysis is part of the behavioral analysis that makes up an attack diagnosis. We can take into account:

- duplicating, multiplying the same or similar comments/messages
- shared links leading to a misinformative source of information (web pages)

Semiotic analysis

Sample questions:

- *In how many cases has a fake article been propagated through links?*
- *What is the scale of bot attacks focused on a specific public figure?*
- *What articles / topics are most attacked by bots/trolls?*

In the case of attacks we analyze:.

- The specific content of comments (e.g. filtering due to the occurrence of keywords), which allows us to determine, for example, the degree of inclusion of names, institutions, political parties, known people, etc. in disinformation activities
- Associations of article content (keywords) with the level of bot and troll attacks

Identification and segmentation of disinformation strategies

Sample questions:

- *What are the main threads/narratives appearing in the framework of the disinformation campaign?*
- *What techniques and tactics does the opponent use?*

Our quantitative analysis (text mining) experts and semiotic (market/communication researchers) deal with text analysis and describe segments of narrative misinformation in qualitative and quantitative terms.

Using various API connections, we currently gather monthly terabytes of date from sources as:

- Social media (Twitter, YouTube, public Facebook pages, etc.)
- Online publishers (CNN, Fox News, Wall Street Journal, etc.)

- Blogs
- Forums

According to specific characteristic of a source, we use:

- “firehose” technique to acquire all generated documents by a provider
- search by query if allowed by publisher
- scheduled scanning of selected website
- search engines querying for predefined subjects and authors.

THE TEAM:

EDGE NPD, creator of ABTShield, specializes in identifying and combating online manipulation/disinformation by combining competencies in behavioral psychology, social communication, network and security technologies, and AI modeling. EDGE NPD was created within Kantar, one of the world’s leading market research institutions. As part of the media group WPP, Edge NPD worked as a special unit in developing new research methodologies focusing on diagnosis of public opinion and social behavior analysis. As an independent company Edge NPD has had seven years of success providing services and technologies for private and public clients. Edge NPD works in collaboration with digital media and advertisers, allowing for comprehensive analysis of internet user behavior and anomaly detection. Edge NPD is one of 40 Google-certified research verification (internet traffic analysis) organizations, and has initiated multiple projects related to advertising and technology - our hallmark 'clean advertising' initiative includes key advertising organizations (SAR, IAB, IAA). Edge NPD, in association with the Google DNI Fund, developed ABTShield (Anti-Bot and Troll Shield), an innovative service that identifies malign traffic and disinformation affecting clients' sites and social media.

- EDGE NPD is a NATO/US Department of State supplier; we have also carried out projects for the European Parliament.
- EDGE NPD is a laureate of Innovation 2020 awarded by the advertising industry (SAR)
- EDGE NPD was recognized as a top 100 innovator in Central Eastern Europe (NE100) by Google, Financial Times, Visegrad Fund, Respublica
- EDGE NPD is a laureate of Most Creative in Business Award (by Brief Magazine and marketing committee)

The ABTShield team for the LAPD will be lead by EDGE NPD Owner and CEO, Dobromir Cias. Mr. Cias studied mathematical sociology at Warsaw University and quantitative methods at Warsaw School of Economics. As an entrepreneur with over 20 years of experience, Mr. Cias combines business, technical, and sociological knowledge to lead one of the most innovative start-ups in the information and business intelligence industry. He is recognized as one of the top 100 innovators in CEE (NE100 award) by Google and Financial Funds, and was awarded "most creative in business" by the marketing committee in PL. Mr. Cias previously served as New Product Development Director and Research Unit Director at Kantar, WPP. He participated in more than 1,400 research projects. He was repeatedly awarded by European research associations (PTBRiO, ESOMAR) and honored by Sir Martin Sorell (WPP) for the EU 2008-2010 crisis analysis. He is the author of dozens publications on market analysis, analytical methods, and research methodologies. He has worked with partners such as the U.S. Embassy in Warsaw, NATO, and the European Union on highly customized efforts to combat disinformation.

LAPD PROPOSED BUDGET

ABTSHIELD SCOPE OF WORK:

- ABTShield, in consultation with the LAPD-designated representatives, will determine up to 10 priority topics and identify currently known accounts/sources of interest to the LAPD to monitor.
- ABTShield will prepare source data (basic reporting level includes 200k messages/month): Twitter (public tweets), Instagram (Instagram posts), Forums (Reddit, Disqus, ect.), Blogs (Tumblr, WordPress, ect.), Videos (Youtube, Vimeo, ect.), News (WSJ, NYT, ect.), Web (all other sites)
- ABTShield will prepare filters and tags and all other technology for precise processing of information related to LAPD's priority areas
- ABTShield, in consultation with the designated LAPD representative, will establish the customer service process and communication procedures.
- ABTShield will provide a dedicated team for the LAPD account including an Account Manager and 2 analysts along with additional analytic support from the entire ABTShield staff as needed.
- ABTShield's team will provide consolidated daily reporting to the LAPD (i.e., defining topics, defining new narratives). The applicability of the dynamic threads and narratives monitoring will be refined with the LAPD representative through direct contact (mail, videoconference) upon request.
- The daily report will include a summary of statistics on threads and narratives related to LAPD priorities; The report will encompass all sources, such as social media, articles, forums, blogs. ABTShield will report for each narrative
    - Where is the thread or narrative appearing? (source/ type of media)
    - How many messages are there? (is it becoming 'sticky'?)
    - What is the reach of the narratives? (is it growing and creating a potential public safety or messaging issue for LAPD?)
    - Is the narrative organic or supported by bot/trolls?
    - What are the suspicious sources of the narrative?

TERM OF SERVICE

- Pricing included for the above Scope of Work for a period of 12 months
- The price includes all cost components related to infrastructure maintenance and technology. ABTShield is maintained on a cloud service provided by Google (Google Cloud) Website

ANNUAL COST: $150,000 USD

ADDITIONAL SERVICE OPTIONS

Extended access to data Twitter

- Includes access to the full Twitter API (upgrade 2.0.), which allows ABTShield to acquire more detailed data about users and their locations (data: URLs, Polls, Geo Profile);
- Increases the analyzed data to approx. 1 million tweets/month

ANNUAL COST: $15,600 USD

Extended Weekly Reporting Option

- ABTShield will create a detailed weekly report using a team of specialists expert in information theory and terrorism.
- ABTShield's network analysis would identify relationships between bad actors and reach the sources of disinformation (list of sources generating disinformation, list of accounts supporting the dissemination of disinformation)
- ABT Shield would provide network analysis and written commentary describing the disinformation scenarios using the AMITT Framework and the Digital Forensic Research Lab / Atlantic Council Dychotomies of Disinformation (https://github.com/DFRLab/Dichotomies-of-Disinformation, https://github.com/misinfosecproject/amitt_framework)

ANNUAL COST: $62,000 USD

Custom Setup of Front-end Service for LAPD.

- EDGE NPD can prepare custom service access for LAPD
- LAPD representatives could define queries regarding monitored topics and threads directly in the system (online / web front-end).
- LAPD representatives could view the results of analyzes not only in e-mails but 24/7 in their customized panel
- LAPD would have access to all resources on the Google account (databases)
- ABTShield would provide an unlimited number of monitored queries/threads (limited only by the volume of source data API) to an unlimited number of LAPD users
- ABTShield would require three months for front-end service set up.

ONE TIME COST: $50,000 USD

Practical Disinformation Training for LAPD

- ABTShield will provide training prepared in conjunction with Collegium Civitas University, a Center for Counteracting Terrorism.
- Training will utilize real-life examples of disinformation relative to LAPD priorities
- The training will provide participants with effective tools for defense against modern online manipulation. Participants will gain the ability to identify manipulative techniques used to create social anxiety and conflict. Other topics will include:
    - Awareness of new manipulation technologies
    - Increasing participants' resistance to mechanisms manipulating socially divisive issues
- ABTShield recommends this training be held after 4-6 months of direct collaboration with the LAPD.
- The training will be a 3-4 hour virtual course accommodating up to 15 LAPD personnel.

ONE TIME COST: $7,000 USD