Resolution
Technology
Analytics, LLC

# Resolution Technology Analytics, LLC (RTA)

Technology. Understanding. Now.

David deCamara
ddecamara@rtechanalytics.com

# RTA MISSION STATEMENT

The mission of RTA is to be the leading provider of curated open source information related to the illicit usage of technology worldwide and international developments in technology that could lead to its illicit usage.

# OUTLINE

- Resolution Technology Analytics (RTA) and Open Source Information
- *GETS* Database
- *GETS* Software Suite
- RTA Products

# RTA OPERATIONS

To perform its mission RTA Gathers, Evaluates, Tracks, and Stores (GETS) open source information in numerous languages and maintains an extensive database.

# WHY OPEN SOURCE INFORMATION?

- Extensive
  - Millions of journalists, NGOs, bloggers, governments, and "everyday people" are putting valuable information online
  - Any particular individual may have and often wants to show key pieces of information
- Quick
  - 2.5 billion smartphones in 2018 (Statista) can instantly upload data
- Cheap
  - Most access is free, much processing can be automated
- Valuable
  - High quality pictures and videos posted online provide a wealth of information
  - Complex understanding can be obtained from many pieces of simple data

**Terrorists agree…**

**Using this public source information, without resorting to illegal means, it is possible to gather at least 80% of information about the enemy.**
**– Al Qaeda Training Manual translation**

# WHY HAS OPEN SOURCE BECOME SO CRITICAL TO UNDERSTANDING THE TECHNOLOGY ENVIRONMENT?


- Information Age
  - Widespread digital platforms enable rapid creation, distribution, and accumulation of information
  - Mass market for information devices has driven development of low-cost consumer sensors, processors, and software
- Age of Innovation Opportunity
  - Large selection of readily available, capable electronics created for the information marketplace has given individuals and small groups the ability to create advanced products that can be used for illicit purposes
  - Private sector demand is compelling rapid technological development

# WHAT DOES OPEN SOURCE PROVIDE?

- Information not otherwise available
- Wide geographical coverage
- Rapid cueing for investigation
- Complement to other sources (e.g., exploitation, intelligence)
  - Completes the picture developed by other sources
  - Information for personnel training
  - Easy means for information exchange and discussion
- Commercially Off The Shelf (COTS) products details
- Knowledge of what others are seeing
- Lack of usage of items or techniques
- As last resort…primary source of information

# RTA EXPERIENCE & DEVELOPMENT

- 2004 - RTA's open source information effort grew out of the USMC Counter IED and ground electronic attack programs
  - The RTA president was the technical lead for USMC Counter RCIED Electronic Warfare (CREW) and Electronic Attack programs before and during Operation Iraqi Freedom
  - For the CREW and Ground/Airborne EA programs hundreds of communication systems were technically exploited to gain detailed understandings of their electronic and RF workings
  - Over 50,000 exploitation reports were analyzed
- 2009 - CREW efforts shifted from a Iraq/Afghanistan focus to a worldwide perspective
  - Over 40 detailed country communications infrastructure reports written
  - Over 20,000 exploitation reports analyzed
- 2012 - *GETS* Software Suite development began
  - 2013 *GETS* open source technology database data entry started
  - Over 4 million articles examined, 3.3 million articles automatically parsed

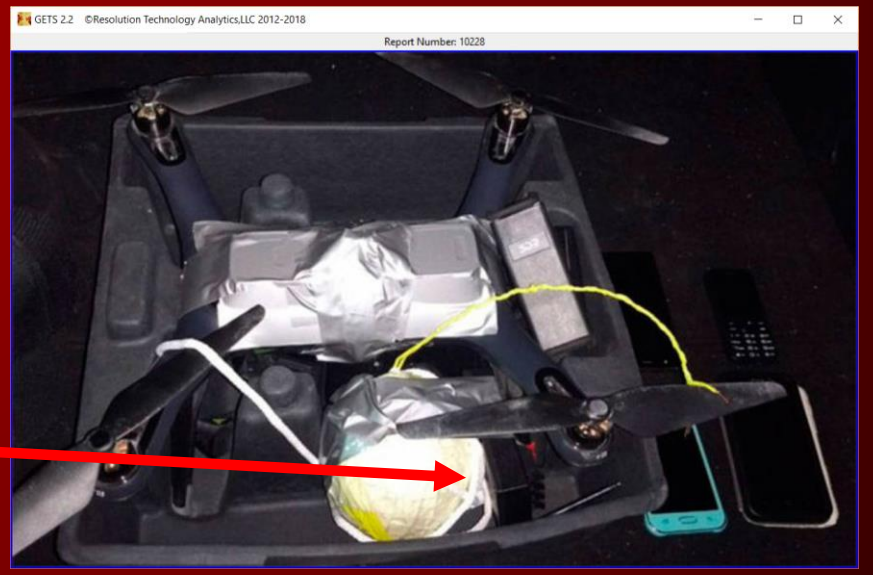
# RTA & OPEN SOURCE

**If you don't know what you are looking for you won't find it…**

- RTA specializes in analyzing illicit usage of technologies
  - Constantly scanning for new incidents
- Technical perspective
  - RTA views open source information from the perspective of what technology was used and how was it used
- Important aspects/characteristics
  - RTA has operational experience and technical background to understand details that could impact equipment and procedures
- Continuity
  - RTA, following hundreds of technical threads, immediately understands when a group makes changes to technology usage
  - RTA can look across time, location, and manner to find differences and similarities

# RTA - TECHNICAL PERSPECTIVE

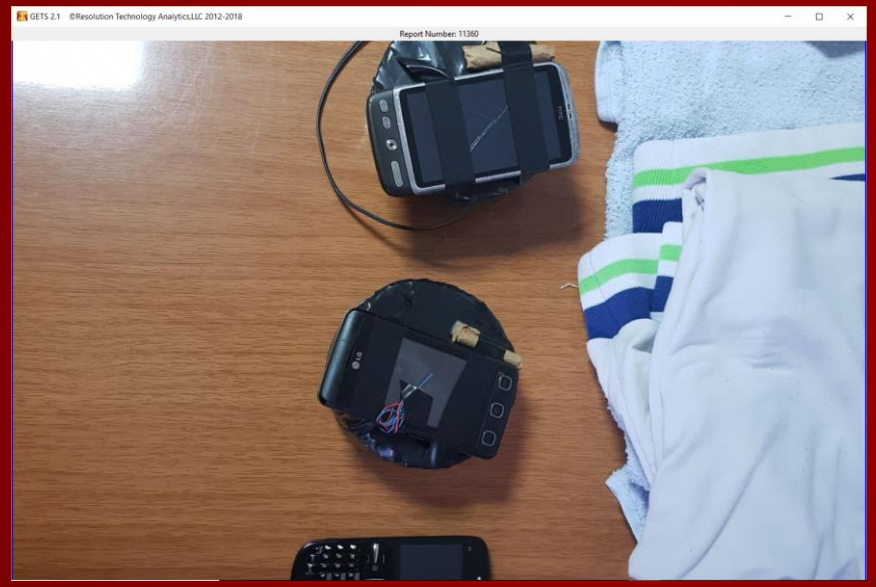
- RTA finds technical details not widely reported.
  - On October 20, 2017 a weaponized Mavic UAV was found in the trunk of a car in Guanajuato, Mexico while being shipped by drug cartel personnel. This was widely reported by both press and entities tracking open source information. However, what was missed by other sources, but reported by RTA, was that the trigger was a *DB04r* wireless fireworks initiator.
  - RTA was then able to connect this trigger type to the same trigger type used in a RCIED found 4 days later in the same Mexican state.

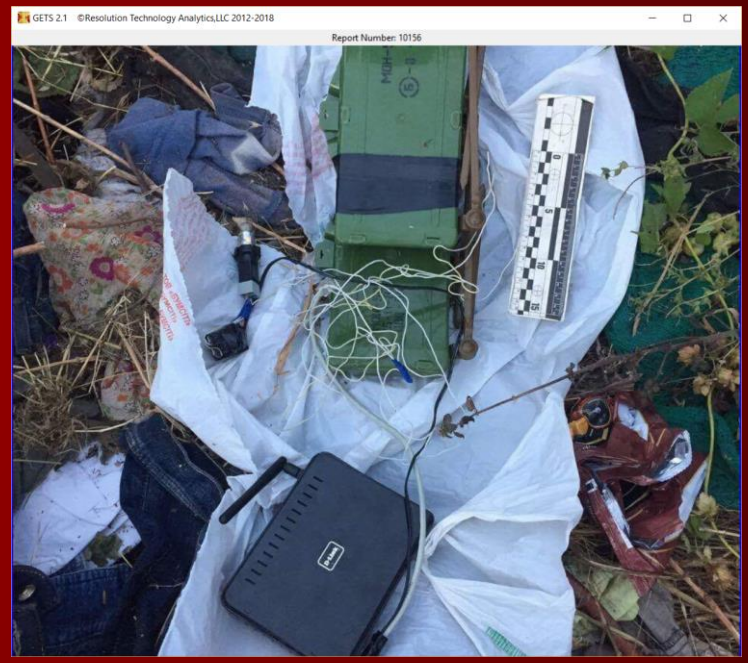
# RTA - TECHNICAL PERSPECTIVE

- New RCIED technologies…

Possible wall outlet RC device
Ukraine Oct17




Refurbished 2G/3G HTC Desire
& 2G LG Cookie Albania May18




D-Link WiFi Router
Ukraine Oct17

# RTA - IMPORTANT ASPECTS/CHARACTERISTICS

- Unique RCIED trigger ~~possibly~~ for use by ISIS in Mosul
  - RTA personnel reported ISIS use of cdma networks almost immediately so forces could make adjustments

start of Battle of Mosul — 16Oct2016

Local press reports ISIS is building comms network with towers on buildings and using devices similar to Senao LRCTs — 19Oct2016

Local press reports GSM jamming and ISIS switching to walkie-talkies and "Reber" [cdma] phones — 27Oct2016

Hundreds of empty ETS2258 cdma phone boxes found in major ISIS cache — 12Dec2016

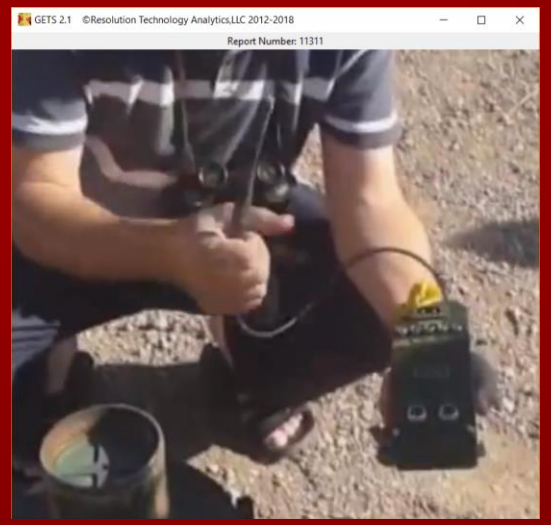
ETS2258 cdma phone found in ISIS car bomb in Mosul — 19May2017

# RTA - CONTINUITY

- Hezbollah operations in Syria – very similar RCIED trigger found over 5 year period


Jul2012 Hezbollah car bomb in Damascus Syria

Aug2014 Hezbollah RCIED
in Syria close to Lebanese border



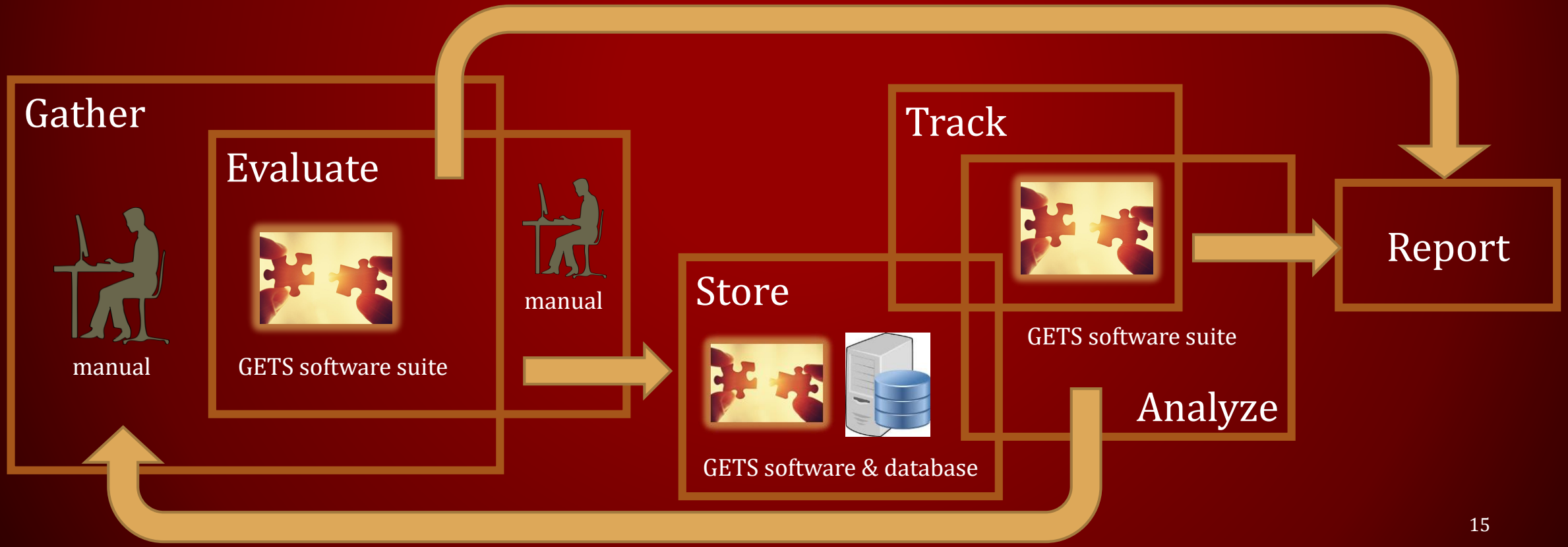

Mar2017 Hezbollah RCIED in Daraa Syria
(label appears to say 421.725)

# WHAT DOES RTA DO AND HOW?

- On a daily basis RTA conducts thousands of targeted, directed, and general searches of online media, social media, governmental, blog, and commercial websites.
- *GETS* software suite
  - Automates the "Gather, Evaluate, Track, and Store" components of these searches and processing
- *GETS* database
  - Relational database of all items found to have interest from a technical perspective
- Provides products with varying levels of evaluation, analysis, and correlation
- Feedback "learned" understanding and knowledge to improve *GETS* software and settings

# WHAT DOES RTA DO AND HOW?

**On a daily basis RTA conducts thousands of targeted, directed, and general searches of media, social media, governmental, blog, and commercial websites.**



# *GETS* DATABASE

**What is the *GETS* Database?**

Detailed collection of open source information related to the illicit usage of technology by terrorists, organized crime groups, and other non-state entities over the last 5 years.

# *GETS* DATABASES

- Technology Incidents Database
  - Database incorporating information, from the internet, related to technology incidents or usage (technology in the field)
- Technology Developments Database
  - Database of technologies that could be used illicitly or technology developments that could be adapted or provide impetus for development for illicit usage (technology not fielded yet)
- Commercial Equipment Database
  - Reference of platforms, systems, and devices that have been or could be used illicitly

# BENEFITS OF THE *GETS* DATABASE

- Understanding
  - Centralized repository
  - Technology usage and evolution through time
  - Usage techniques, trends
  - Correlation across geographic areas
- Reference
  - Usage history
  - Information exchange
  - Baseline & context for further study
- Instruction
  - Experienced personnel can broaden knowledge base and swiftly shift to new areas
  - New personnel can quickly gain broad baseline understanding of technology employments
  - Syllabi material
- Inexpensive

# *GETS* DATABASE - UNDERSTANDING

- RCIED Trigger types use by country (Countries A through M):
  - Categories are explained in backup slide.

| RCIED Trigger Categories | Afghanistan | Albania | Algeria | Bahrain | Colombia | Egypt | India | Iraq | Israel | Kenya | Lebanon | Libya | Mexico | Myanmar |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mobile phones & modems | X | X | X | X | X | X | X | X | X | X | X | X | | X |
| Low power, small command set devices | X | | | X | X | X | X | X | X | X | X | X | X | X |
| Two-way radios & DTMF receivers | | | | | X | X | ? | X | | | | X | | |
| High power consumer devices | | X | X | | X | ? | ? | X | | X | | X | | |
| Telemetry / Telecommand | | | | ? | | ? | | X | ? | | ? | ? | | |
| RC Toys | | | | | | | ? | | | | | | | |
| Wireless Local Loop (WLL) [cdma] | | | | | | | | X* | | | | | | |

# *GETS* DATABASE - UNDERSTANDING

- Since 2014 all *known* radio models used by Thai separatist militants have been TYT, nominally TH-F8 radios. In February 2017 they used an unknown model Baofeng. Could this be the start of a shift away from TYT radios?

TYT TH-F8 two-way radio 5/2014

TYT TH-F8 two-way radio 9/2014

TYT 2/2015


TYT 4/2016

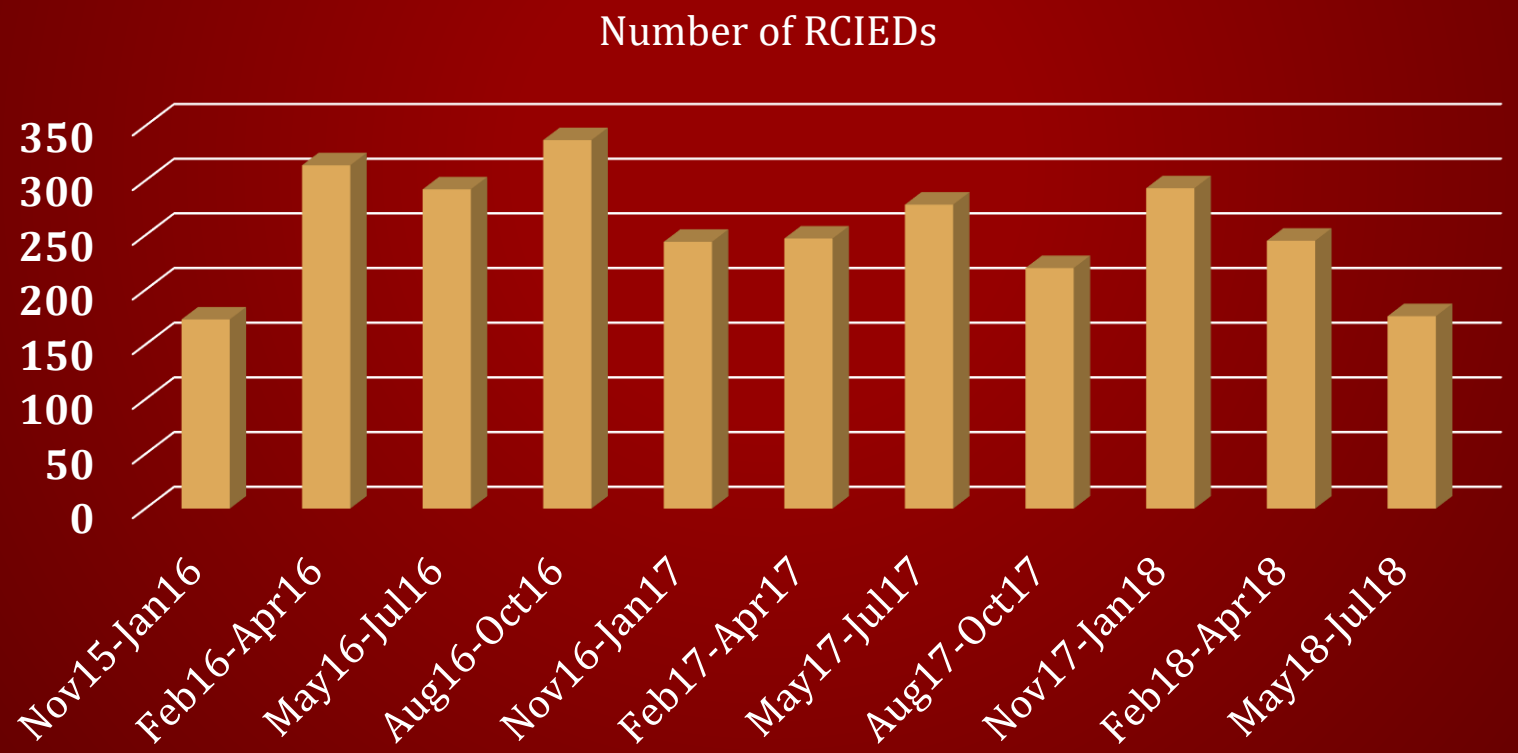
TYT TH-F8 two-way radio 7/2016

TYT TH-F8 two-way radio 11/2016

Unknown model Baofeng 2/2017

# *GETS* DATABASE - REFERENCE

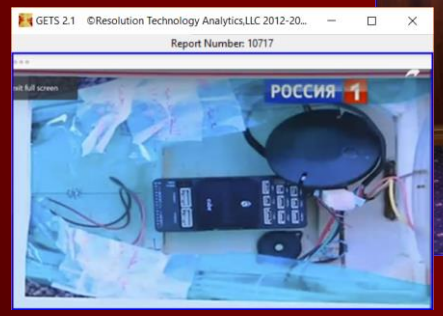
- Worldwide RCIED Incident totals by quarter
  - Note: These are the number reported explicitly as RCIEDs by the press, government, or social media sources.



# *GETS* DATABASE - INSTRUCTION

- UAV Developments:
  - Groups are starting to use autonomous navigation to direct UAVs to targets. This has been done by two groups since the beginning of the year. A group in Syria has on at least 15 occasions launched a total of about 40 UAVs using autonomous navigation to attack Russian bases in Syria. Also, an unknown Ukrainian separatist group launched a homemade UAV to attack a target based on pre-determined coordinates, but the UAV crashed before hitting the target.

Homemade UAV using PIXHAWK autopilot controller and GNSS data to autonomously attack targets.



Crashed homemade UAV in Ukraine that was carrying 1 kg of explosives and using autonomous navigation.

# *GETS* DATABASE STATISTICS (13JULY2018 CUTOFF)

- Total articles automatically parsed: 3.2+ million
- *GETS* database entries:
  - Technology incidents:  11,469 entries / 2173 images
  - Technology developments: 382 entries / 237 images
- IEDs incidents:  6846
- Caches (all types): 2064
- Unmanned Aerial Vehicle related: 816
- Communications: 470
- Incident entries by country:
  - Pakistan (1204), Colombia (1102), Syria (746), Iraq (782), Thailand (499), Ukraine (485), Yemen (563), Egypt (1109), US (473), ISIS (1001)
  - 122 countries with data
- Articles in 24 languages included

# *GETS* SEARCH / DATABASE FOCUS

- Improvised Explosive Device technologies
  - Triggers and sensors
  - Technology-related techniques
- Remotely/Autonomously-controlled vehicle technologies
  - Technological developments that could aid in their illicit or terrorist usage/effectiveness
  - Unintended, illicit and terrorist usage incidents
- RF Communications
  - Communications means and hardware used by illegal groups
  - Mobile device/computer-based communications applications
  - Internet of Things (IoT)
- Sensor/Surveillance technologies and technology-related techniques
- Artificial Intelligence (AI) non-standard uses
- RF Disruption technologies and incidents
- Maker/DIY designs and "Chinese" product adaptations with potential 'dual-use' applications

**Search / database focus is user defined…these are the current priorities**

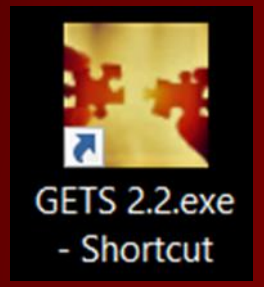
# *GETS* SOFTWARE SUITE

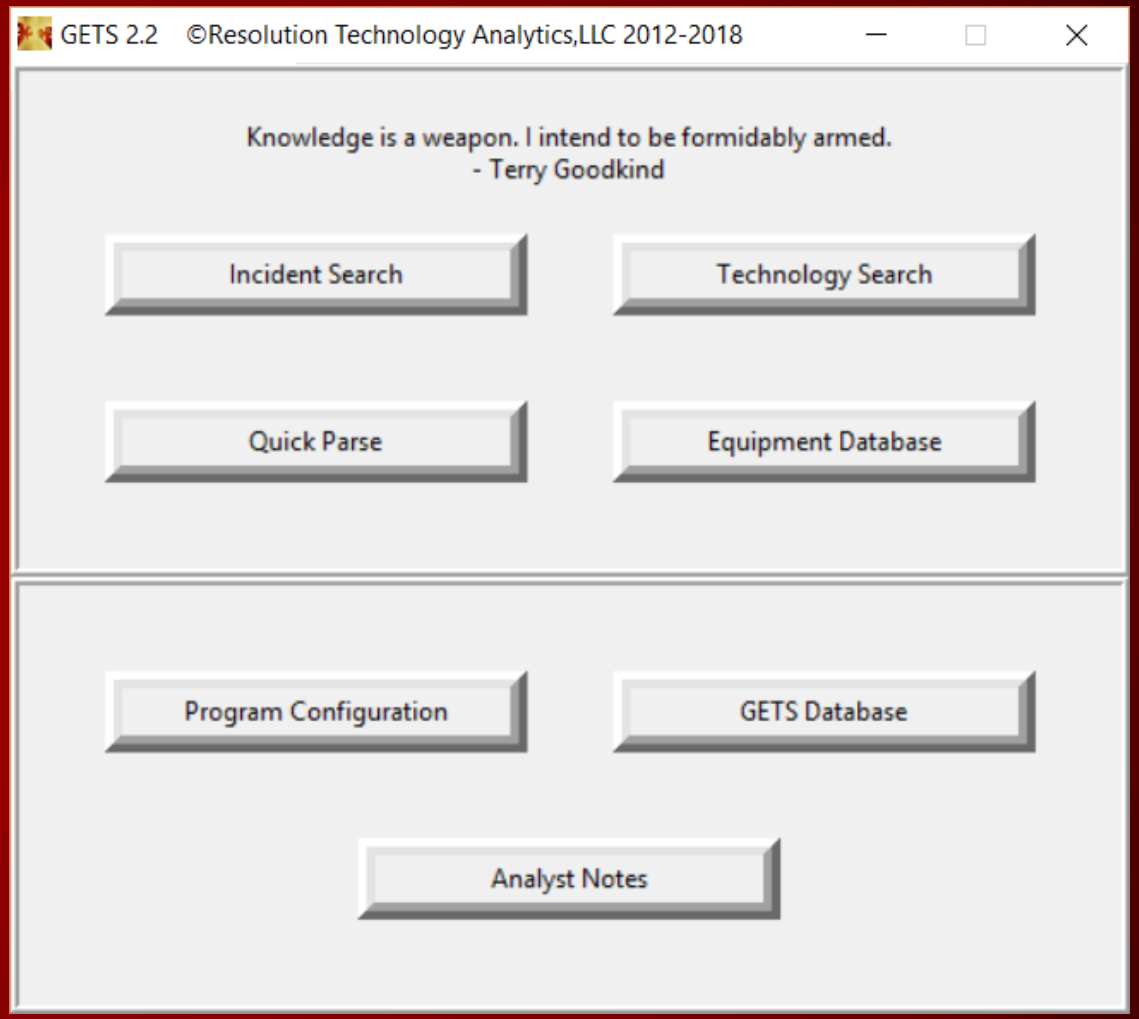
**What is *GETS*?**

An automated program to obtain, evaluate, store, analyze, and track information from the internet with a focus on illicit usage of technology.

# *GETS*

## *GETS* Main Window



# WHY NOT JUST USE A SEARCH ENGINE?

- Each search provides a limited number of search returns
  - Very often a key item is not in the search return
- Algorithms that determine which results to return are not known
  - You do not know what are the optimum search terms for what you are looking for
- Information is fleeting…
  - Search engine results vary with time; you can't just wait until you need the information to search for it
- No built-in parsing capability
- Difficult to search in non-native languages
- No storage or evaluations of returns of interest

# WHY USE *GETS*?

- Scheduled, highly tailored automated searches
  - Tailored searches and parsing provide specific information of interest
  - Search can be scheduled for convenient times (e.g., overnight)
  - Assistance with non-native language searches
- Getting the nuggets out of the mountain
  - Processing will differentiate articles with divergent content
- Language parsing capability
  - Often articles with key insights are published in native languages
  - Computer translators may omit key terms /phrases
- Repository of information
  - Enables feedback, provides "corporate memory," quick ability to analyze trends and rapid indications of new introductions or shifts in technology

# WHERE DOES *GETS* OBTAIN ITS INFORMATION?

- Searches of the internet, but other information can be entered
- User-entered URLs
  - Individual URLs
  - Groups of URLs based on common language / country / topic / other
  - Analysis tools help decide what URLs are optimal
- Aggregation websites
- BING (through API)
- All searches / URLs can be stored and run on user defined schedule

# WHERE CAN *GETS* BE USED?

- Any computer
  - Gather function requires an internet connection
  - Windows-based executable
  - MySQL database
  - Program is very stable and uses standard processing resources
  - Storage requirements depend on user requirements
- Networked computers
  - One computer acts as server for other computers
  - Currently only functions in intra-network
  - Database can be easily accessed remotely

# *GETS* SOFTWARE – ADDITIONAL FEATURES

- Keyword list creation tools
- Analysis tools for:
  - Selecting keywords and processing rules
  - Choosing URLs
  - Tracking incidents
- Scheduled run calendar
- Export data to .csv spreadsheets

# RTA PRODUCTS

# RTA ANALYTICAL STUDIES / BRIEFINGS

- RTA can rapidly develop thorough analytical products based on client-defined criteria and requirements:
  - Emerging, updated and/or directed research topics
  - Based on combination of timeframe, topic, country, group, region
  - Periodic versus one-time reports
  - Standalone versus open source input for all-source analysis
- Analytical products can include tracking (i.e., number of incident types over time intervals)
- Analytical product formats include slide presentation, text document or pdf.

# RTA INFORMATION SUBSCRIPTION SERVICE

- RTA can provide client-defined technical information to enable rapid client analyses, assessments, and actions
  - To ensure rapid dissemination this information is evaluated (for relevancy and plausibility), but is not analyzed (for comprehensiveness, related information, and accuracy).
  - Client-defined information coverage (e.g., all technology areas versus selected topics)
  - Information delivery periodicity can be daily, weekly or other
- Information format can be *GETS* Mini GUI with MySQL database or Excel files
  - Additional factors need to be considered for *GETS* Mini with db

# RTA ALERT SERVICE

- RTA can provide client-defined alerts with respect to technology-related incidents and developments.
  - Alerts based on combination of technology, topic, country, group, or region
  - Level of alerts can be defined (e.g., all items deemed high priority, all incidents that involve certain type of item, etc)
  - Data is unevaluated, but RTA analyst comments provided as necessary
  - Alerts can be at fixed time cycles or as information becomes available
  - Alerts are provided by email at information level specified by client
    - URL, pdf of document, summary of information, assessment or combination

# RTA *GETS* DATABASE

- The entire or portions of the *GETS* database can be purchased.
  - This provides a comprehensive record of technology related incidents.
- The database is provided with *GETS* Mini GUI that includes the Track function of the *GETS* software suite and applicable Evaluation modules.
- Database can be purchased with or without the Information Subscription Service.
  - With the subscription service weekly database updates are provided.

# RTA TECHNOLOGY CONSULTING

- RTA can provide:
  - experienced analyst assessments of technology usage and developments
  - insight and reports into expected future technology and technology usage developments based on extensive understanding of current and past operating environments, usage requirements, and emerging technology opportunities

Resolution
Technology
Analytics, LLC

David deCamara
803-847-2856
ddecamara@rtechanalytics.com

# BACK-UP SLIDES

# *GETS* DATABASE EXAMPLES

- RCIED trigger categories:
  - Mobile phones & modems – devices in this category include mobile phones of different standards generations and equipment used to send/receive cellular data communications
  - Low power, small command set devices – these devices use simple AM signaling formats to send/receive basic On/Off type commands and are less than 500 mW; examples include appliance controllers, wireless doorbells and vehicle entry systems; frequency is less than 500 MHz
  - Two-way radios & DTMF receivers – these devices are equipment used to send/receive narrowband voice and data signals using frequency modulation; frequency is less than 1 GHz
  - High power consumer devices – these are higher power (≥500 mW) communication devices that consumers may purchase legally in many countries, thus they are more readily available; examples include 'FRS-type' radios, long-range cordless phones, and (non-AM signaling format) car alarms
  - Telemetry / Telecommand – machine-to-machine devices that typically use FSK type formats and are for point-to-point data links; these devices are commonly put in project boxes and connected to whip, stub or makeshift coaxial antennas; frequency is less than 1 GHz
  - RC Toys – these devices use the (< 50 MHz) RF links for (non-hobby grade) RC Toys; these devices, although widely available, are infrequently used by terrorists due to their extremely short-range
  - Wireless Local Loop (WLL) – these devices are similar to mobile networks, except the consumer device is often not meant to be mobile; they are extremely rarely used for RCIEDs and these types of networks are being phased out in favor of LTE networks, which are mobile