Generative Representation of Synthetic Threat Actors for Simulation and Training

J. Wesley Regian
PeopleTec, Inc.
Huntsville, AL
wes.regian@peopletec.com

David A. Noever
PeopleTec, Inc.
Huntsville, AL
david.noever@peopletec.com

ABSTRACT

In this paper we describe a generalized and generative synthetic threat actor (SynthActor) modeling capability as currently implemented in the Web Ontology Language (OWL 2). SynthActor is general in the sense that it readily supports representation and reasoning about threat actors at any level of aggregation (individuals, groups and nation states) and for any domain of aggression (kinetic, cyber, insurgency, and asymmetric warfare). SynthActor is generative in the sense that it can automatically respond to simulated or hypothesized conflict situations with behaviors that are consistent with previously specified threat actor world views and technical/aggression capabilities. Threat actor world views are represented in SynthActor as cultural sub-models reflecting the belief systems of the actor (social, political and theological). Threat actor technical/aggression capabilities are represented in SynthActor as knowledge/skill properties of the actor (chemical, nuclear, explosives, cyber and melee). SynthActor enables modeling of threat individuals and groups as active and engaged entities which respond to changing situations, prosecute an agenda, define operational goals, and execute operations to achieve those goals. Violent threat actor properties, as modeled in SynthActor, are aligned with the Multilateral Interoperability Program (MIP) and its Information Model (MIM). MIM modeling enables automated machine sharing of information about violent threat actors and activities. Cyber threat actor properties, as modeled in SynthActor, are aligned with the Department of Homeland Security's Structured Threat Information Expression (STIX) modeling language. STIX modeling enables automated machine sharing of information about cyber threat actors and activities. SynthActor, with MIM and STIX language extensions, enables automated machine derivation and sharing of detailed information about realistically unfolding threat actor campaigns in adversarial simulation environments.

ABOUT THE AUTHORS

J. Wesley Regian has 32 years of experience in cognitive performance modeling and knowledge-based software technology development, primarily for military application with AFRL, AFOSR, and DARPA. His work has supported over 50 fielded systems. He has published over 100 papers on intelligence analysis, human terrain modeling, knowledge representation, knowledge management, human learning and memory, individual and developmental differences in human cognition, spatial ability and spatial information processing, cognitive modeling, skill acquisition, componential analysis of spatial tasks, cognitive automaticity, psychometrics, artificial intelligence, hypertext, hypermedia, training, computer-based training, intelligent computer-based training, virtual reality, and multi-source intelligence fusion. Dr. Regian was a National Research Council research adviser for ten years and Senior Scientist for Knowledge Based Systems at the US Air Force Armstrong Research Laboratory.

David Noever has 27 years of research experience with NASA and Department of Defense in machine learning and data mining. He received his Ph.D. from Oxford University, as a Rhodes Scholar, in theoretical physics and B.Sc. from Princeton University, summa cum laude, and Phi Beta Kappa. While at NASA, he was named 1998 Discover Magazine's "Inventor of the Year," for the novel development of computational biology software and internet search robots, culminating in co-founding the startup company cited by Nature Biotechnology as first in its technology class. He has authored more than 100 peer-reviewed scientific research articles and book chapters. He also received the Silver Medal of the Royal Society, London, and is a former Chevron Scholar, San Francisco. His primary research centers on machine learning, algorithms, and data mining for analytics, intelligence and novel metric generation.

Generative Representation of Synthetic Threat Actors for Simulation and Training

J. Wesley Regian
PeopleTec, Inc.
Huntsville, AL
wes.regian@peopletec.com

David A. Noever
PeopleTec, Inc.
Huntsville, AL
david.noever@peopletec.com

INTRODUCTION

Intelligence analysis includes the use of information about enemies to produce logically defensible assertions about enemies' past (forensic analysis), current (explanatory analysis), and future (anticipatory analysis) operations. Unlike other domains of expertise, intelligence analysts often must reason from purposefully deceptive data about enemy operations (Hayes, 2007). While threat actors may be successful - to varying degrees - in concealing some of their operations, they are often less effective in concealing their intentions and capabilities. In many cases, the motivations and intentions of threat actors are openly advertised by the actors themselves, and their capabilities are easily inferred from actor-related event data sources. Building on the intentions and capabilities of targeted threat actors is an important hallmark of accurate intelligence analysis, and is especially critical for anticipatory analysis. In this paper we describe our approach to semantic modeling of threat actor intentions and capabilities, and we discuss application of the resulting models to machine generation of alternative enemy courses of action in simulation environments.

THREAT ACTORS

We define threat actors as volitional entities at any level of aggregation (individuals, groups, organizations, and nation states) that present a threat to friendly, national or coalition interests. Volitional entities are able to decide on, commit to, plan for, and prosecute courses of action to achieve potentially explicit sub-goals and goals.

Deep Representation and Anticipatory Reasoning about Threat Actors

We stipulate that most threat actors, like most volitional entities, are rational actors. They make decisions and take actions that are prudent and logical given their goals, resource constraints, and the choices available. Terrorist threat actors are often singled out by laypersons as examples of irrational actors. For example, it has proven difficult for many to conceive of a suicide bombing as a prudent and logical choice on the part of the suicide bomber. However, if the world view of the bomber includes an imperative to drive societal change, eternal rewards in heaven, and monetary rewards for surviving family – then the martyr's death is rational (Hafez, 2006; Atran, 2003; Pronin, et al. 2006). In 2000, Sprinzak labeled these actor representations as "rational fanatics," pointing particularly to the 1983 Beirut bombing as the strategy's most dramatic modern inception point. Economics domain modelers of irrational behavior postulate the concept of "bounded rationality" (Simon, 1982), which argues the irrational actor does not have access to all the correct information needed to make rational decisions. Our approach is only slightly different. We handle apparent rationality exceptions by reference to threat actor "world views." Under our approach, terrorist threat actor decisions are prudent and logical according to their *world view*, goals, resource constraints, and the choices available. We do not take a position on the correctness, completeness, or consistency of the threat actor world view. Our goal is to accurately model the cultural world view as accepted by the threat actor.

Stevens, 2010 underscored that a severe lack of modeling tools constrains current real-world application. In the cybersecurity context specifically, he concluded that "security managers resist revisiting previously considered [threat modeling] techniques, until the community creates a demonstrably simpler, cheaper, or more scalable solution - often in product form. In the absence of such a threat modeling tool, at least commercially, you might be tempted to carry on deferring." For counterintelligence, Stanton, et al. (2015) tried to associate rule-based logic for Islamic threat actors and their response to air strikes. They noted the remarkable lack of publicly-available, data-driven studies.

According to Dugan, 2011, 96 percent of all terrorism related articles in peer-reviewed journals (from 1975-2002) were "characterized as thought-pieces, lacking any systematic case study or empirical analyses".

The deep-seated bewilderment about persons willing to die partially explains the challenge of modeling suicide bombers as rational actors. Yet suicide bombing is a favorite terrorist tactic and difficult to defeat, because human bombs are smart, accurate, asymmetric, cheap and psychologically potent. Previous work has quantitatively applied a rational choice paradigm to predict and model threats. To understand airline hijacking Dugan, et al (2005) noted the practical implications for reducing attacks by target hardening, punishment severity, perceived apprehension certainty and safe havens (e.g. Cuba diversions). To model responses to terrorism, Pronin, et al (2006) examined the stark implications for decisions on whether to bomb or negotiate. "If people perceive terrorists as rational beings whose views are responsive to objective facts, they will be inclined to resolve their differences with terrorists via diplomacy" or alternatively if threat actors are viewed as permanently biased and irrational, then more violent, unilateral solutions will be sought. These models differ from SynthActor mainly in their roots as part of a longer criminology theme, wherein terrorism as crime may be deterred by imposing increasingly harsher penalties on rational criminal threat actors. Extending such deterrence models to suicidal attackers, however, remains problematic, since their actions trigger with a nothing-left-to-lose mentality (and possible after-life, familial or social gains). While the martyr's narrative remains globally irrational, this threat actor type can locally make sense, albeit from the perspective that the individual choice of self-destruction remains intimately tied to understandable traditions, rituals, beliefs, and skillsets. Other researchers (Benmelech, 2007; Atran, 2003) have argued empirically against the public perception of the "crazed, cowardly" attacker, noting that most suicide bombers have higher than average education levels, socioeconomic status and diverse personality types (introvert vs. extrovert). While many suicide bombers express religious beliefs prior to recruitment, Merari (2002) reported no higher religiosity than for the overall Palestinian population. The public apprehension about suicide attacks however is fueled by the method's frequency and relative lethality (3-fold more casualties than other bombing methods, Global Terror Database, 2016), soft-target selection (malls, airports, etc.) and absence of a primary witness (the bomber) to link back forensically to their larger networks and groups. In short, the terror tactic continues and grows because it has proven effective as a means of terror.

In SynthActor, the component elements of volition that represent actor intentions, capabilities and methods are modeled as *memes*. Dawkins (1976) coined the term, defining a meme as "an idea, behavior, or style that spreads from person to person within a culture." From the perspective of threat actors, memes are facts and assemblages of facts that are both **known and true**. From the perspective of the SynthActor model, threat actor memes are facts, assertions and assemblages of facts/assertions that are either **known or *believed true*** by the threat actor. SynthActor supports two classes of memes to anticipate threat actor actions. First, Assertion/Belief memes define threat actor cultural and spiritual world views. Examples of common assertion/belief memes are that females should not be educated, apostate soldiers should not be in Islamic territories, or individuals who abandon the Islamic faith should be executed. SynthActor supports the representation of assertion/belief memes in detail, including for example the actor prescribed punishment for educating females or actor preferred methods for curtailing female education. Second, Knowledge/Skill memes represent threat actor organizational and technical capabilities. Examples of important knowledge/skill memes are how to construct an Improvised Explosive Device or suicide vest, how to construct a nuclear weapon, or where to obtain forged passports. SynthActor supports the representation of knowledge/skill memes in detail, including for example the explosive materials and actuator technologies currently used by a specific threat actor.

SynthActor is represented in RDF/OWL (Resource Description Framework / Web Ontology Language) and can store instance data in any modern, high-performance, persistent graph database. We are currently using Franz® AllegroGraph. Figure 1 shows a GRUFF representation of a partial SynthActor meme hierarchy. Examples of Cultural Worldview memetic classes are on the left, and Technical Capability memetic classes are on the right. For clarity of display, neither of these sets are exhaustive as shown here, and new memetic classes can be easily added as needed. Volitional Entities include Persons, Organizations, and Software Agents. Persons and Organizations are assumed to be motivated by Cultural Worldview memetic instances and their technical and organizational capabilities are assumed to be enabled by Technical Capability memetic instances. Software Agents, while modeled as Volitional Entities, are not directly motivated or enabled by memetic instances. Instead, Software Agent intentions and capabilities are a function of the memetic instances associated with the Persons or Organizations that develop the Software Agents.

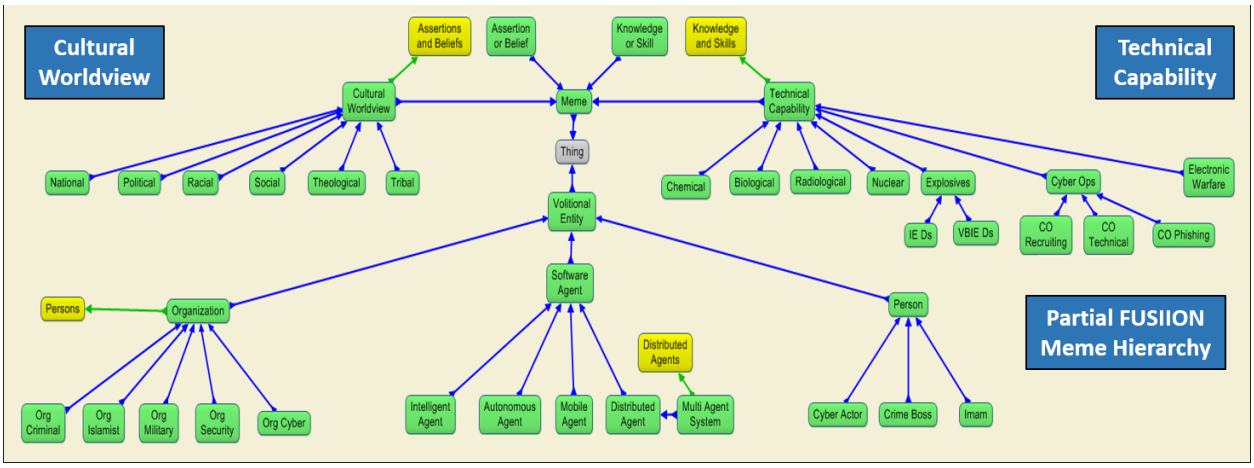

Figure 1. Threat Actor Meme Abstraction Hierarchy

Figure 2 provides contrasting examples of SynthActor Cultural Worldview descriptions for modeling two very different classes of threat actors. On the left we represent a recently arrested Sovereign Citizen group with nationalistic views, extreme right political leanings, and Evangelical theological perspectives. On the right we represent Boko Haram, which espouses Sunni/Wahhabi theological indoctrination with an extreme Salafist/Jihadist activism profile. These two very different cultural worldview profiles drive predictably different criminal activity profiles (summarized in yellow at bottom). We formally model these two groups of approximately similar size (30,101 members of Boko Haram vs. 40,377 members of Sovereign Citizen; START, 2016) but different goals and predicted behavior. While Boko Haram has accounted for 1688 attacks and 16,790 deaths since 2010, Sovereign Citizens have accounted for 4 attacks and 1 death. When violent, both groups use firearm tactics to target civilians including firefighters and police. Both present with a theologically identified perspective, but lack a well-defined social or tribal perspective.

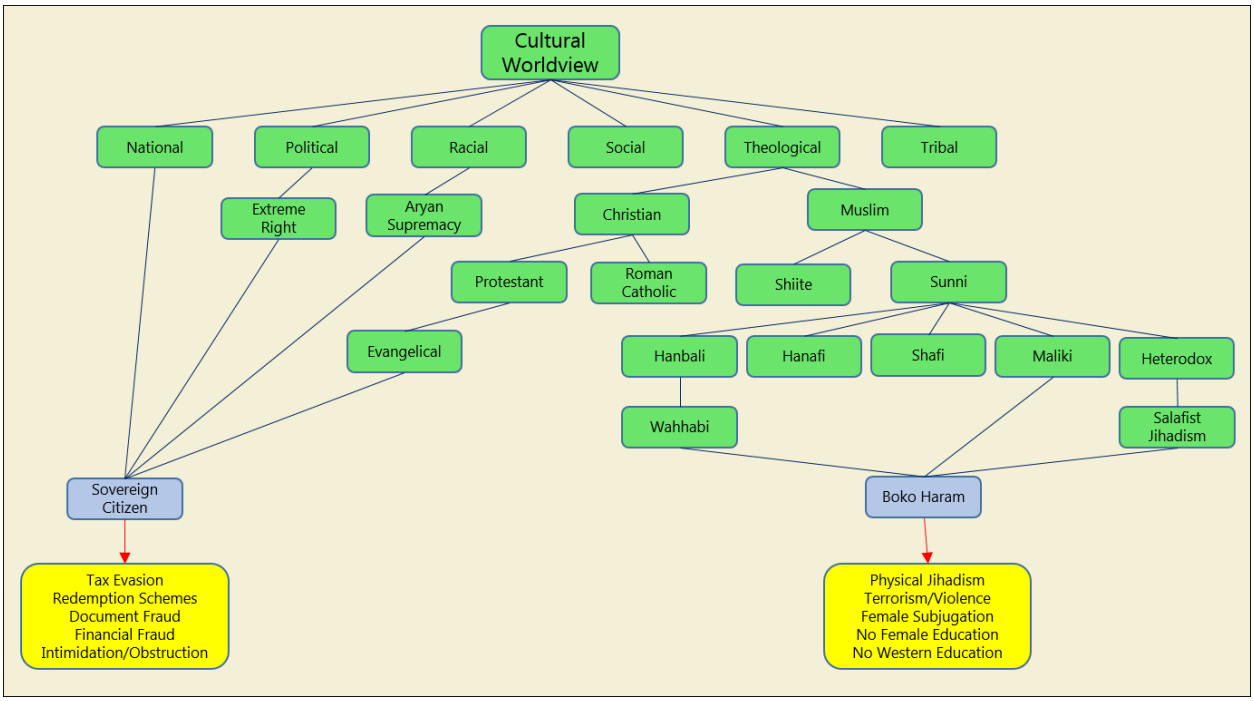

Figure 2. Instantiated Meme Abstraction Hierarchy

SYNTHETIC THREAT ACTORS

We are currently developing models of real world threat actors to support forensic and anticipatory analysis based on actor intentions, capabilities and methods in intelligence fusion settings. For a discussion of intelligence modeling applied to Islamic extremist, drug cartels, and multinational criminal organizations, see Regian (2012). In this paper, we propose that these synthetic threat actor models are directly applicable to simulation based training and what-if analysis for operational planners.

Graph Reasoning Example

To demonstrate the empirical derivation and application of these models for complex reasoning, we coded the Global Terrorism archives (START, 2016) into a graph database (Neo4j). Unlike a relational database organized around rows and columns, graph databases use semantic queries to find nodes (e.g. events, persons or organizations), edges (relationships between nodes) and structural properties (key/value pairs). We query for shared features between two notable 2014 attacks. Boko Haram kidnapped more than 200 girls on April 14 after storming a school with explosives. A member of Sovereign Citizen attacked Corinth, Texas police and firefighters with an AK-47 automatic rifle, jars of flammable liquids and propane tanks intended to explode when fired upon. The motive attributed to Boko Haram was consistent with their ideological imperative for slave brides (or to sell them for ransom). The motive attributed to Sovereign Citizen was publicity for a dubious 'get out the vote' stunt. An analyst looking for similarities would have to scour databases with considerable background and expertise on each group's ideology and tactics. A likely outcome would be no overlap. In Figure 3, we formally show the related elements between these two terrorist events.

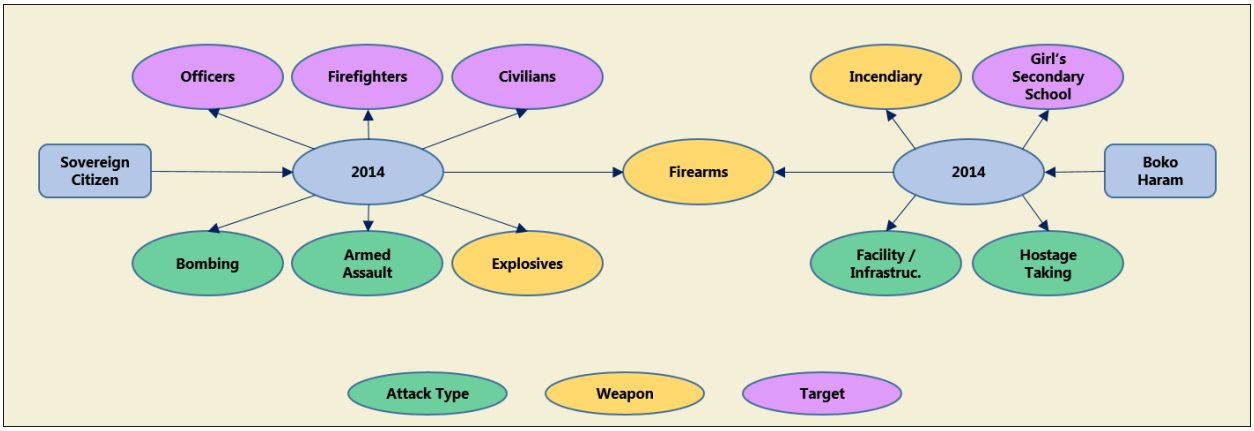

Figure 3. Graph Structure Showing Relationships between Boko Haram and Sovereign Citizen Attacks

The common relationship link between the two 2014 events was the use of firearms, incendiary or explosives as weapons. They also share a common target as civilians. No overlap is shown between their objectives as hostage taking (Boko Haram) or general violent publicity (Sovereign Citizen).

The method of querying the graph database is outlined in pseudo-code below. The query seeks the top 10 matches between two dated event identifiers with all shortest paths between those two events (e1 and e2).

```
match
        (e1:Event {id: 201404140009}),   # Boko Haram
         (e2:Event {id: 201408110060})   # Sovereign Citizen
        with e1,e2
        match
                p = allshortestpaths ( (e1)-[*]-(e2) )
        return p
limit 10
```

A more likely analyst's task would be to find all precursors to the Boko Haram kidnapping and provide a highlighted lessons-learned analysis for forensics. In Figure 4, we again query the graph to find shortest paths between hostage-taking events limited to Boko Haram and find that nine months earlier (July 2013), slave brides became a high priority for the group's attempts to further recruitment and retention of soldiers (Zenn, et al 2014). The graph results succinctly show the common and disparate elements of the 2013 precursor events and the much larger 2014 kidnapping. Other than the overlapping use of firearms and hostages, both the 2013 and 2014 kidnapping involved Christian women who would presumably be converted to Islam, brokered for release of soldiers or used as slave brides. The primary differences are also shown for 2014 attacks at a much bigger, organized scale (attacking a government facility/school infrastructure with explosives) than a small arms attack in 2013.

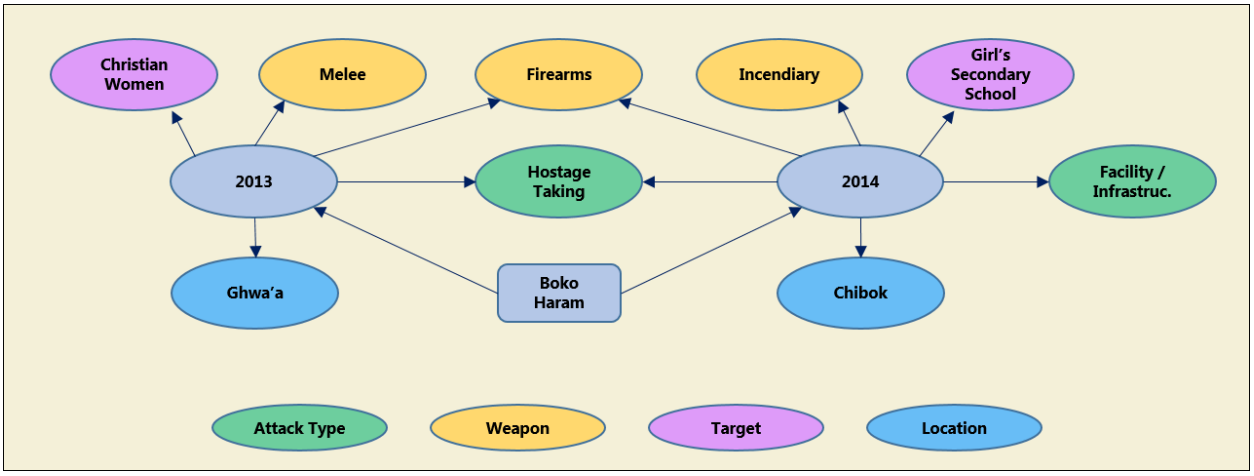

Figure 4. Graph Reasoning to Find Precursors to Boko Haram Kidnappings of Slave Brides

Simulation-Based Training

One obvious application of these data-derived threat actor models is in simulation-based and game-based training systems. SynthActor models would enable simulated threat actors to respond appropriately to trainee decisions and actions. In this case "appropriately" means the modeled actor will respond to user inputs in ways that are consistent with the data available about that actor from real world events and known actor world view profiles. Actor tactics and world view profiles can change over time. For example, tactics and world view changes are often associated with leadership changes in threat groups and nation states. Such changes can be empirically tracked and then implemented in SynthActor models. This will allow unscripted, game-like training with realistic outcomes not explicitly planned in detail by training developers. We present a simplified example of modeling the personality of a threat actor using real-world social media datamining. Sentiment models can provide insights into expected actor behavior for gaming. The application of statistical models to current events (2015+) thus offers a novel, testable and quantitative threat perspective. Twitter (and other news feeds) provides a concept map or word cloud that can support rapid and accessible insights into current topics and seed semantic models of ISIS behavior. A simplified example of this method's use is to track the use of the term 'infidel' across multiple countries and assess its relative importance to that country's view of the top 7000 (English) tweets segregated across six countries: Syria, Iraq, Afghanistan, Pakistan, Libya and Turkey. The data returns 61,453 stem words after filtering common English words, all numbers, punctuation or sentence case changes, and the original search terms which are known to occur frequently (e.g. ISIS+Turkey or ISIS+Syria are not part of the final data set). The resulting document corpus consists of a term matrix with country-labeled columns and word frequency rows. The term document matrix is visualized as a comparative word cloud, shown in Figure 5, where the country label reflects the ISIS-related search term (ISIS+Syria, ISIS+Turkey, etc.). Each country is assigned a country and word set. The word size shows its frequency in this data. A notable feature of this method is its automated ability to build and analyze large data sets quickly and extract evolving ISIS world views from open source intelligence.

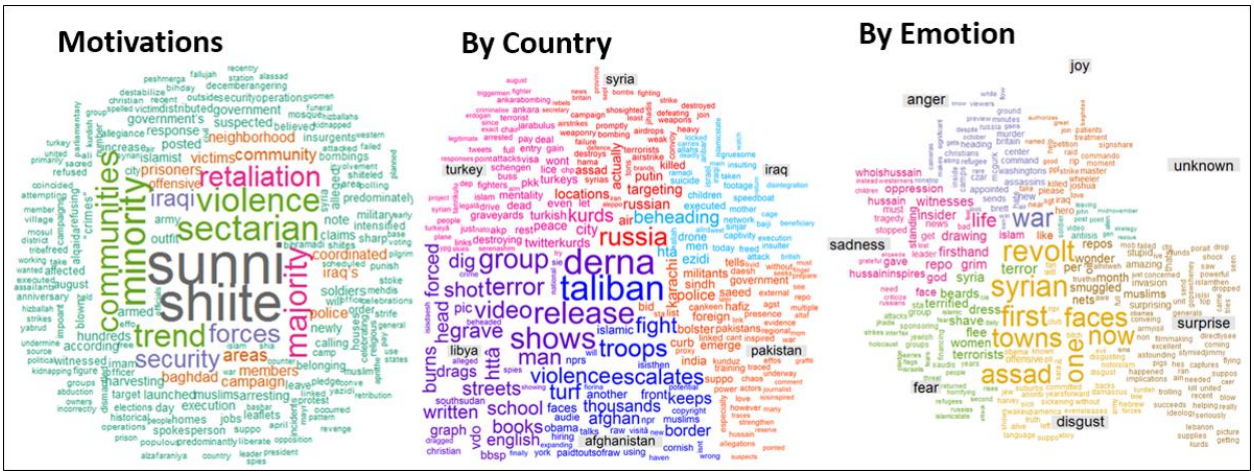

Figure 5. Sentiment Analysis of Social Media for Simulation and Agent Behavior. *Left shows the Global Terrorism Database assigned Attack motives. Center shows the sentiment by country based on Twitter opinion of the term infidel. Right shows the associated Twitter opinion on ISIS with emotional attributes.*

For training simulations, a terrorist's motivations is a key behavioral cue for driving narrative direction. For example, the formal motive may be described by sectarianism (Fig. 2 left). The research literature features Sunni-Shiite animosity as the dominant psychological element in the Global Terror Database. But if simulating a particular Pakistanian agents' probable reaction to encountering an 'infidel', the dominant themes emerge from social media data as distinct from sectarian models alone. On Twitter in Pakistan, infidels are described as 'external', 'foreign', and prompting a police or militant presence (Fig. 2, center, lower right). While simulation designers may want to understand and model a particular threat actor's response to encountering a foreign soldier, emotional behaviors can have a non-intuitive hiearchy based on Twitter opinion (Fig 2. right). For example the opinion about ISIS triggers a rank order transitioning from most frequent to least that initially may be hard to understand: Joy > Anger > Sadness > Fear > Disgust > Surprise. In our (October 2015) sample of 1500 ISIS tweets, more were positive (900) than negative (600).

In addition to modeling threat actor motives, entire scenarios can be mined from social media. For example, in the Turkish feeds a prominent theme is discussed that is headline driven: the death of American journalist, Serena Shim, in October 2014 in a suspicious car accident after reporting Turkish government support for the Syrian insurgency. An additionally interesting theme in Turkey is the escalating interest in visa travel through Europe, as highlighted by Twitter references to Schengen countries, visa and entry. Schengen countries are those "26 European states that have officially abolished passport and all other types of border control at their mutual borders" (Wikipedia). A creative scenario planner can dramatically move the game narrative from current events to possible outcomes with both realistic motivations and character categories.

Simulation-Based What-If Analysis

Data-derived threat actor models will also be useful in military contingency planning systems based on what-if-analysis. SynthActor-based systems could allow planners to play out various scenarios while planning responses to real world crises including counterinsurgency (COIN), counterterrorism, and domestic operations (DOMOPS) involving fringe subpopulations. Contingency planning is inherently anticipatory, reasoning about the future based on observed threat evolution. Consider, for example, anticipating likely future enemy attack types based on changing enemy profiles. One wants to catalog a library of threats and their deeper property sets with automated translation and injection of new threats into these formal models. For statistical inferences, the training (and testing) dataset was selected from an open-sourced June 2016 Global Terrorism Database or GTD. The National Consortium for the Study of Terrorism and Responses to Terrorism (START, 2016) maintains GTD. This record set contains 140,000 events catalogued from 1970-2016 and tracking 134 categories for classification. GTD encapsulates attacks by over 3000 distinct terrorist groups. Key categories provide a curated event timeline segregated by location (latitude/longitude,

province, etc.), the terrorist group, weapon (bombs, guns, etc.), nationality (Iraqi, US, UK, etc.), targeted groups (civilian, police, military, etc.) and targeted types (airports, maritime, etc.). Additional fields classify the binary categorical pattern of multiple incidents, suicide attacks, guns, hostages and claims of responsibility. In addition to summing the raw counts for each category, additional numeric fields enable tabulating the number of fatalities or wounded terrorist and US fatalities, property damage, and ransoms. To illustrate how we update models to reflect evolving attack types against various targets, we apply association rule learning (Hahsler, 2011) to historical terrorism-related events.

Figure 6. Association Rule Learning between Inputs and Outputs

As a data exploratory tool for simulation builders, association rule learning offers a way to discover interesting relations between many often-weakly correlated variables in very large databases. The basic idea is to select groupings of event descriptors (country, nationality of victims, weapons, etc.) and find those most likely to predict the outcome (suicide attack). For the approximately 60,000 attacks since 2010, we examine the correlates of suicidal attacks. As shown in Figure 6, the top axis is the input to the model (labeled LHS or left hand side of the association rule) and the right axis is the output of connected rule. In this rule visualization, size of the dot is the fraction of suicidal terrorist events that contain both elements. The color of the dot reflects confidence, where darker is more confident. This visualization is not unlike a correlation matrix for categorical (non-numerical) variables. From Figure 6, there are strong associations between the country of both the attacker and victims (e.g. Pakistani suicides killing other Pakistanis). The three countries that dominate this ruleset include: Iraq, Afghanistan, and Pakistan. As shown lower right, the dominant group is not known, but the suicide weapon of choice remains explosives, with lesser associations for firearms. For running simulations and designing what-if scenarios, the novel application of association learning offers automatic groupings for further exploration, even when linear correlation or non-numeric inputs dominate the model. While we have examined the irrational vs. rational conflict with a suicide attack, the presence of some associated precursors lends quantitative support for continuing the complex pattern analysis. In other words, strictly irrational behavior might appear random and therefore impossible to model, where rational fanaticism may offer some common (and predictive) tenets such as country, weapon, and targets.

NEXT STEPS

We are now focusing our efforts on automated, ongoing maintenance of SynthActor models based on very large data sources. In this unclassified paper, we can list some of the open sources we are accessing to build out and test SynthActor models. Here are some of the open sources for which we are developing automated extraction and tagging techniques.

- Open source terrorism data (current and past from Oct 2015) including foreign language translations and social media. Available archived intel reporting and Arabic translation for extended timeline correlations
- Global Terrorism Data (June 2016 update covering 1970-Dec 2015) including attack TTP geotagging and group attributions

- DARPA's Integrated Crisis Early Warning System (ICEWS) including 14 million events with source and target names, categories, and countries, as well as CAMEO (Conflict and Mediation Event Observations) codes, intensity scores, and geocoding down to the city level.
- Phoenix Data Project with specific codes for contemporary actors of interest, such as ISIL
- Kansas Event Data System (KEDS), and its successor, the Penn State Event Data System
- Global Data on Events, Location and Tone (GDELT) including a quarter-billion geo-referenced dyadic 'event records' covering all countries in the world 1979 to present, capturing who did what to whom, when, and where in the CAMEO taxonomy.
- Openstreetmap.org (Syria/Iraq): 45,000 Iraqi towns, 22,000 Syrian towns and geotagged data for roads, cafes, mosques, infrastructure, etc.
- Human terrain data from Syrian Martyr Revolution Database (SRMD), Assad opposition and humanitarian groups (149,000 events)
- Customized news crawlers (100,000 open source news tracking from 3000+ news sources in English). From research experience, de-duplication of multiple, but similar reports and sophisticated filtering are needed for raw news feeds to disambiguate important tracking events from competing news and outdated historical topics.
- Social media API tracking for Twitter daily since Oct 2015
- CIA World Database and various terror-specific, open leadership sources such as the Stanford Mapping Militants Project for assigning probabilistic regional players and demographic layers.

SUMMARY AND CONCLUSIONS

Anticipatory semantic models of threat actors are achievable, as evidenced by successful anticipatory intelligence analysis from expert analysts. Like others, we avoid using the term "predictive" to stay away from claims of precision. While it is not possible (without specific HUMINT) to predict that Boko Haram will attack a Borno State Girl's School in Maiduguri on Tuesday, it can be anticipated that Boko Haram will continue kidnapping girls based on continuity of group leadership, worldview, capabilities - and opportunities. This type of anticipatory reasoning is almost tautological, and is easily achieved by human analysts with accurate mental models of threat actor world views and capabilities. SynthActor is simply our attempt to represent machine understandable mental models of threat actors – with similar reasoning implications as models held by expert human analysts. A second unique contribution of this work is the empirical derivation and maintenance of SynthActor models by ongoing, automated monitoring of very large data sets to mine information about threat actor activities and sentiments.

ACKNOWLEDGEMENTS

The authors would like to thank the PeopleTec Technical Fellows program for encouragement and project assistance. This research benefited from support from U.S. Army Space and Missile Defense Command/Army Forces Strategic Command.

REFERENCES

Atran, S. (2003). Genesis of suicide terrorism. Science, 299(5612), 1534-1539.

Benmelech, E., & Berrebi, C. (2007). Human capital and the productivity of suicide bombers. The Journal of Economic Perspectives, 21(3), 223-238.

Dawkins, R. (1976). *The Selfish Gene*, Oxford, UK: Oxford University Press.

Dugan, L. (2011). The Making of the Global Terrorism Database and Its Applicability to Studying the Life Cycles of Terrorist. The sage handbook of criminological research methods, 175.

Dugan, L., LaFree, G., & Piquero, A. R. (2005). Testing a rational choice model of airline hijackings. Criminology, 43(4), 1031-1065.

Hafez, M. M. (2006). Rationality, culture, and structure in the making of suicide bombers: A preliminary theoretical synthesis and illustrative case study. Studies in Conflict & Terrorism, 29(2), 165-185.

Hahsler, M., Chelluboina, S., Hornik, K., & Buchta, C. (2011). The arules R-package ecosystem: analyzing interesting patterns from large transaction data sets. Journal of Machine Learning Research, 12(Jun), 2021-2025.

Hayes, Joseph (2007), "Analytic Culture in the U.S. Intelligence Community. Chapter One. Working Definitions", *History Staff, Center for the Study of Intelligence, Central Intelligence Agency*, retrieved 2016-05-24

Merari, A. (2002). Paper presented to Institute for Social Research seminar series, "The Psychology of Extremism," Univ. of Michigan. Ann Arbor, MI, 11.

Najgebauer, A., Antkiewicz, R., Chmielewski, M., & Kasprzak, R. (2008). The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution. Journal of Telecommunications and Information Technology, 14-20.

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Data file]. Retrieved from https://www.start.umd.edu/gtd

Pronin, E., Kennedy, K., & Butsch, S. (2006). Bombing versus negotiating: How preferences for combating terrorism are affected by perceived terrorist rationality. Basic and Applied Social Psychology, 28(4), 385-392.

Regian, J.W. (2012). Formal Modeling of Heterogeneous Social Networks for Human Terrain Analytics. *American Intelligence Journal, Volume 30, Number 2,* 114-119.

Simon, H.A. (1982). *Models of Bounded Rationality*, Cambridge, Mass.: MIT Press.

Sprinzak, E. (2000). Rational fanatics. Foreign Policy, (120), 66.

Stanton, A., Thart, A., Jain, A., Vyas, P., Chatterjee, A., & Shakarian, P. (2015, August). Mining for Causal Relationships: A Data-Driven Study of the Islamic State. In Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 2137-2146). ACM.

Steven, J. (2010). Threat modeling-perhaps it's time. IEEE Security & Privacy, 8(3), 83-86.

Trappl, R., & Petta (Eds.) (1997) Creating Personalities for Synthetic Actors: Towards Autonomous Personality Agents. Springer Series: Lecture Notes in Artificial Intelligence, Vol. 1195

Zenn, J., & Pearson, E. (2014). Women, Gender and the evolving tactics of Boko Haram. Journal of terrorism research, 5(1).