Terrorist Social Network Analysis: Past, Present, and Future

V.S. Subrahmanian
Lab for Computational Cultural Dynamics
Computer Science Dept. & UMIACS
University of Maryland
vs@cs.umd.edu
www.cs.umd.edu/~vs/
@vssubrah

Talk Outline

- STONE Shaping Terrorist Organization Network Efficacy [joint with A. Mannes, F. Spezzano]
  - Quantifying Terror Network Lethality
  - Predicting Successors of a Removed Terrorist
  - Identifying Who to Remove

- Social Media Analytics of ISIL Activity [ongoing]
  - Twitter [joint with S. Kumar]
  - YouTube [joint with M. Albanese]

- The Upcoming Threat Landscape
  - Next 2-4 Years: Bots, Ransomware, Banking Trojans, Bitcoin & Cryptocurrencies
  - 4-10 Years: ICS/SCADA, IoT Attacks

Goal of STONE

Maximally degrade the lethality of a terror network

BUT

- **No metrics to measure lethality of terror networks**
- **No models to predict number of attacks by a terror group**

How STONE Works – 4 Broad Problems to Solve

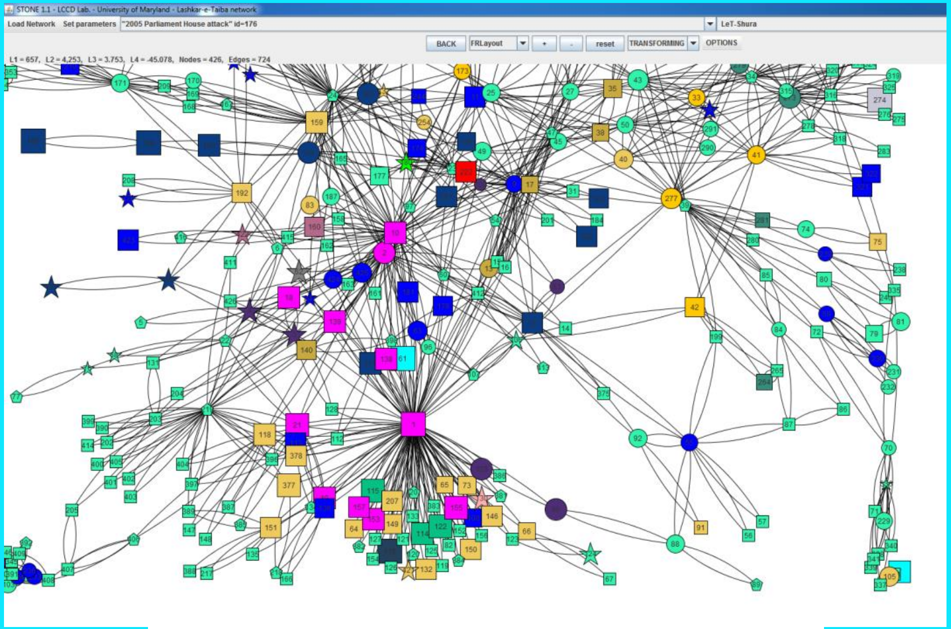
Predictive Model to Measure Lethality of a Terror Network (predict number of attacks)

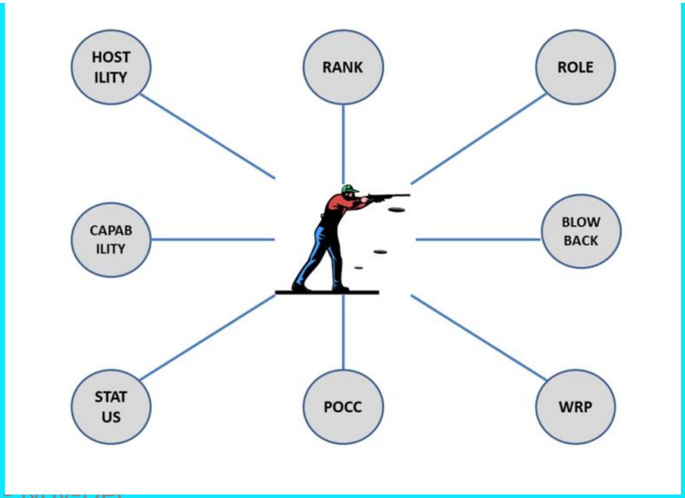
- Predict successors of a "removed" (captured, killed, etc.) terrorist
- Predict new possible networks when a terrorist is removed
- Identify who to remove from the network to minimize <u>expected</u> lethality of the resulting network

Terror Networks

Consists of

- Nodes – people, events
- Edges connect nodes. Edges labeled with relationships.
- *A <u>rank</u> labeling each node specifying how important the node is within* the hierarchy
- A *list of properties* for each node – with discrete and numeric values, e.g.
  - Role of the node in the organization
  - Clustering coefficient – how "tightly connected" is the node to its neighbors
  - Blowback level – level of blowback if the node is removed
  - Hostility Level including support for carrying out terror attacks
  - Competence in carrying out terrorist acts
  - Whether the individual is dead/otherwise removed from network/alive and active





Correlated Measure L4

Person P1 removed

Person P2 removed

Network N1 A1 Attacks

Network N2 A2 Attacks

Predictive regression model is highly accurate.

- **0.83 Pearson Correlation Coefficient for LeT network.**
- **0.8 for AQ network**

- We have different networks as people are removed from the network.
- Initially, we have network N1 and during this time, A1 attacks occur. Network N1 has properties L1(1), L2(1), and L3(1).
- When person P1 was removed, we have a new network N2 and during the time N2 existed, there were A2 attacks. Network N2 has properties L1(2), L2(2), L3(3).
- We build a regression model to predict number of attacks from historical data about the L1(i)'s, L2(i)'s and L3(i)'s.

What Happens when a terrorist is removed from the network?

Influence
- Who is most influential?
- Built on top of Google's PageRank algorithm

Connectedness
- Who belongs to a tightly knit network?
- Builds on top of clustering coefficients in social networks

Rank
- Replacement of a node will have comparable or lower rank
- Successor must have similar capabilities

Vertex Successor Prediction

First define a set of candidates to replace node r. Must have overlapping skills and must be at or below r's rank.

How does node v's influence change if node r is removed? Define WRP(v,r) – the weighted PageRank of *v*, assuming *r* is removed.

How do v's total ensemble of properties (incl. influence) qualify him as a successor to r? Define *rv(v)*, the relative value of *v* as a successor.

Probability of v as a replacement for r is the ratio of his relative value to the total relative value of all candidates.

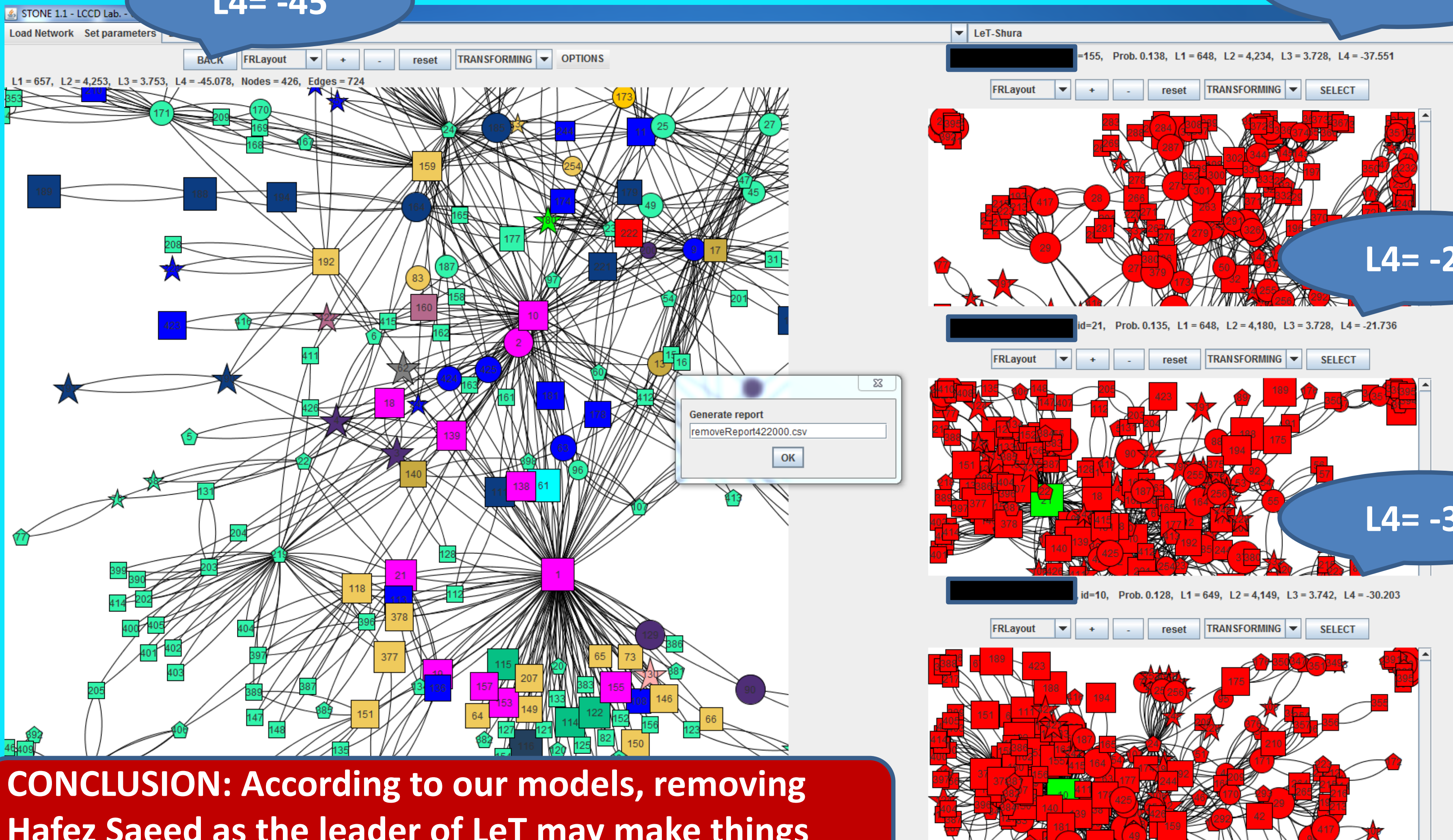
Replacement Probability

L4= -45

L4= -37

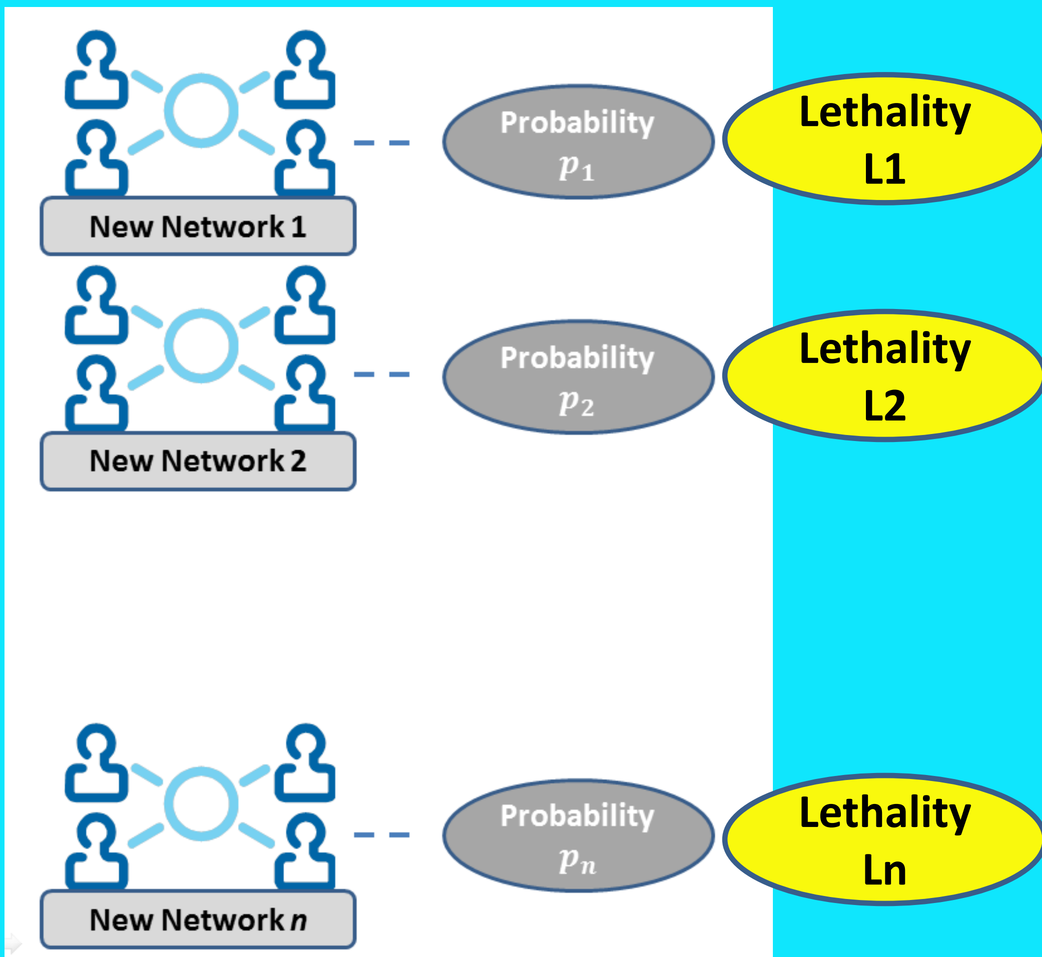
L4= -21

L4= -30



CONCLUSION: According to our models, removing Hafez Saeed as the leader of LeT may make things worse.

Pictorially.....



Algorithm 2 STONE-Reshape network reshaping algorithm

```
Input: Organizational network 𝒪𝒩 = (V, E, wt, ℘), maximum set size k.
Output: Set R of nodes to remove.
function RESHAPE(𝒪𝒩, k)
    R = ∅
    ℓ = L(𝒪𝒩)
    continue = true
    do
        r = arg min_{v∈V\R} L_EV(𝒪𝒩, R ∪ {v})
        ℓ_r = L_EV(𝒪𝒩, R ∪ {r})
        If(ℓ_r ≤ ℓ)
            R = R ∪ {r}
            ℓ = ℓ_r
        Else continue = false
        EndIf
    while(continue ∧ |R| ≤ k)
    return R
end function
```

Verification & Validation

- Tested and validated predictions on 4 terror networks: Al-Qaeda, Hamas, Hezbollah, Lashkar-e-Taiba.
- Predicting successor: In 80% of the cases, one of the top 3 predictions was the actual successor. This number not only includes terrorist leaders but lower level operatives as well.

Forecast: Hezbollah - Successor of Hassan Nasrallah

Pick #1
Hashem Saf al-Din

Pick #2
Hussein al-Khalil

Pick #3
Naim Qassem

Pick #4
Muhammed Yazbek

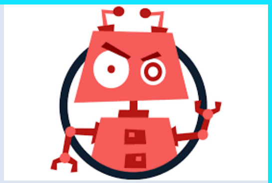
Talk Outline

- **STONE Shaping Terrorist Organization Network Efficacy [joint with A. Mannes, F. Spezzano]**
  - **Quantifying Terror Network Lethality**
  - **Predicting Successors of a Removed Terrorist**
  - **Identifying Who to Remove**
- **Social Media Analytics of ISIL Activity [ongoing]**

  - **Twitter [joint with S. Kumar]**
  - **YouTube [joint with M. Albanese]**
- **The Upcoming Threat Landscape**
  - **Next 2-4 Years: Bots, Ransomware, Banking Trojans, Bitcoin & Cryptocurrencies**
  - **4-10 Years: ICS/SCADA, IoT Attacks**

The Art of the Possible

Bots



Use bots to:
- influence opinion
- crush/overwhelm dissent
- expend adversary's resources

2015 DARPA Bot Challenge

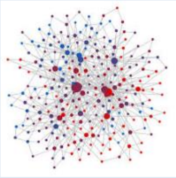
Identify Influencers

Key influencers not determined by followers or friends
Topic specific influencers
Diffusion Centrality

2014 India Election

Diffusion Model

Predict # of supporters on a topic
Predict # of opponents over time
Identify viral spread



2014 India Election

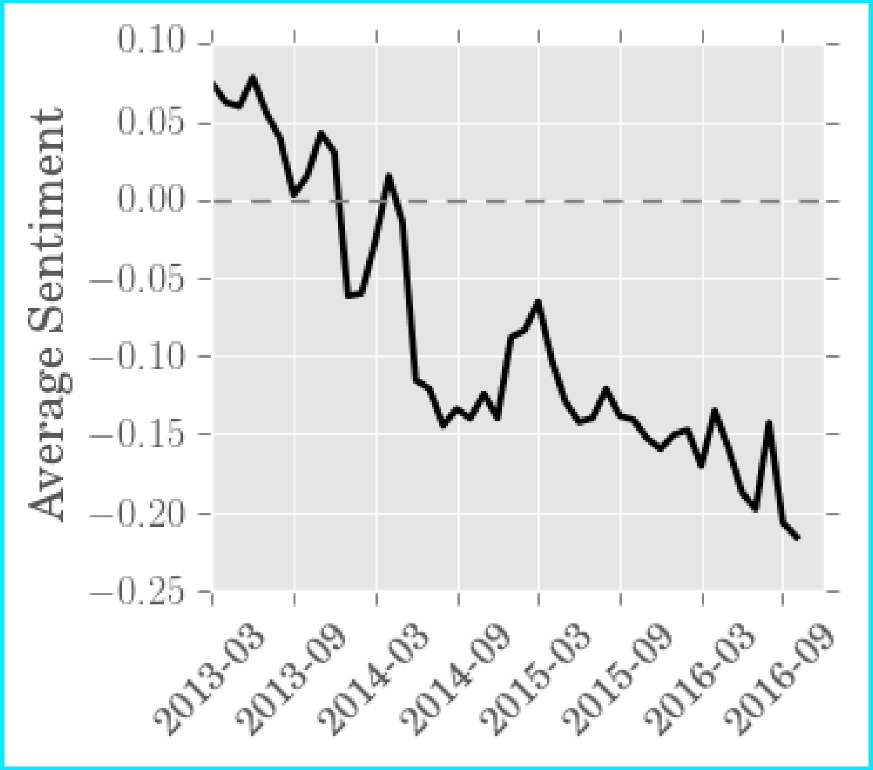
Identify Malicious Actors

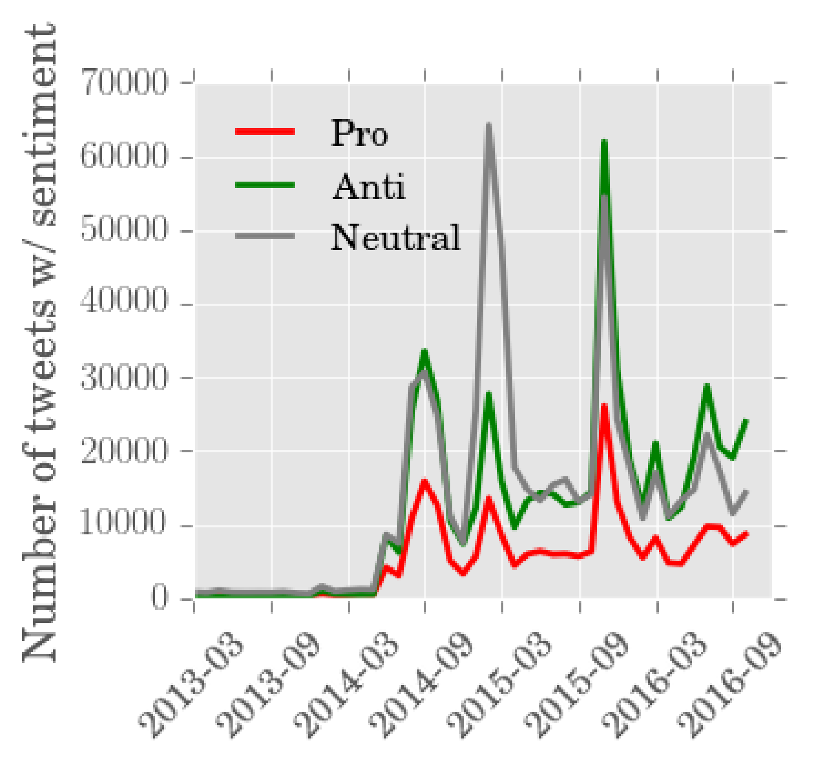
Online Marketplace fraud [Flipkart]
SMS fraud
Fake information [Wikipedia]
Fake accounts
Online trolls

ISIL Twitter Data

- Time frame (March 2013-Oct 2016)
- ~1.4M ISIL-related tweets
- ~737K Twitter users
- ~4K geo-tagged tweets
- Purpose
  – Dissemination of Ideology
  – Recruiting
  – Dissemination of Instructions
  – Command, Control, Communication
  – And more.....

Twitter Sentiment Toward ISIL

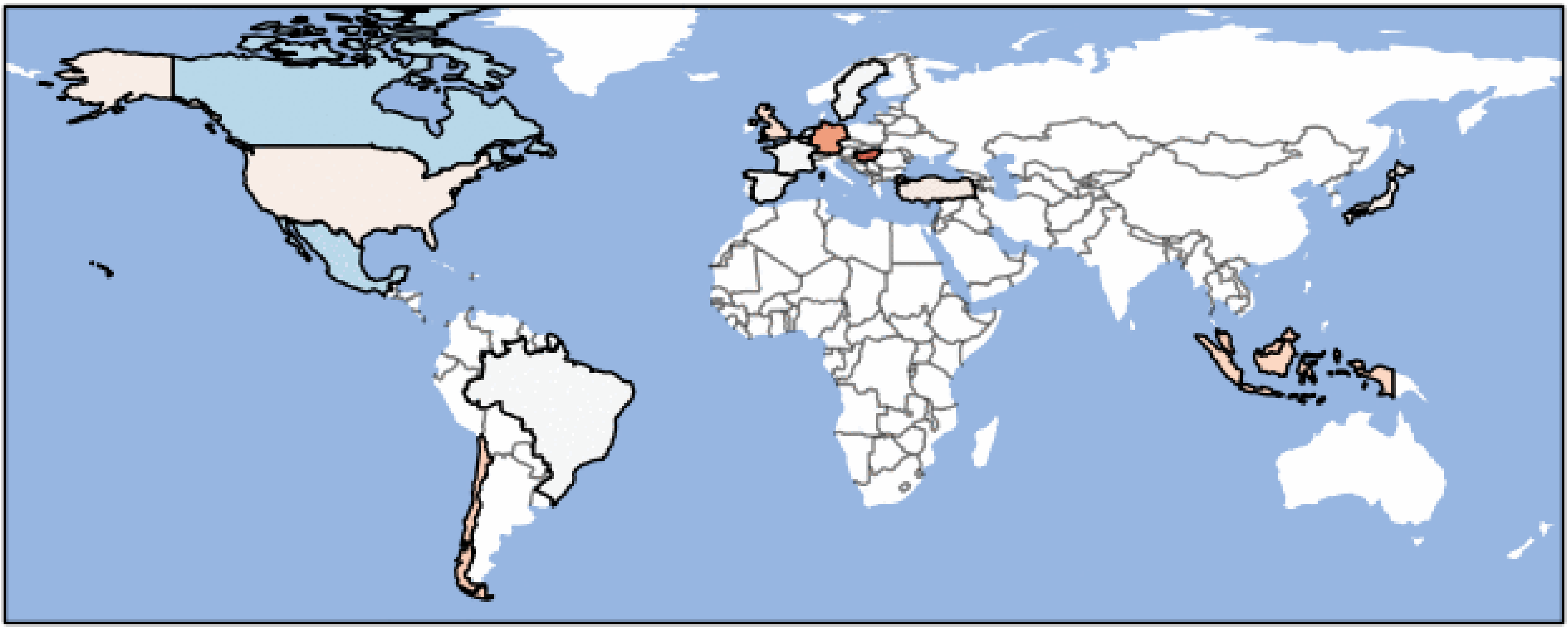




Twitter Sentiment Toward ISIL

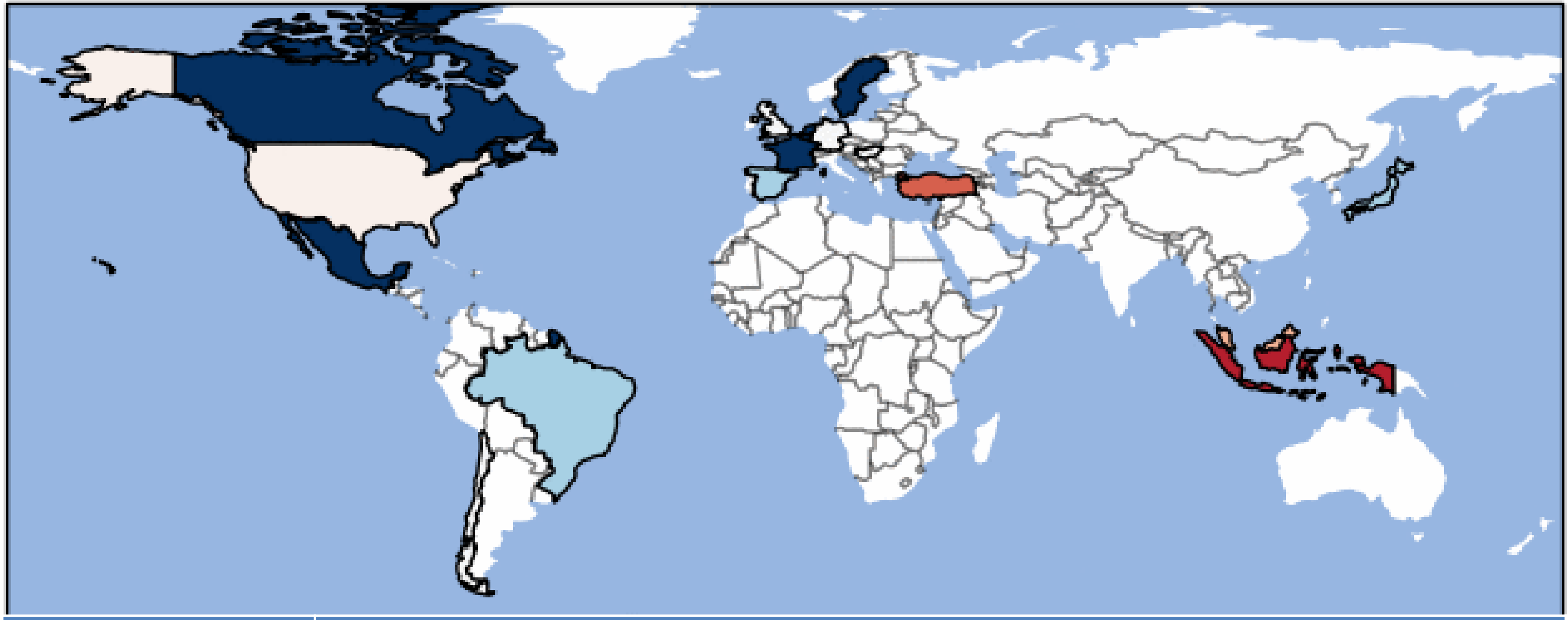
WORK IN PROGRESS

03/2013 - 08/2013



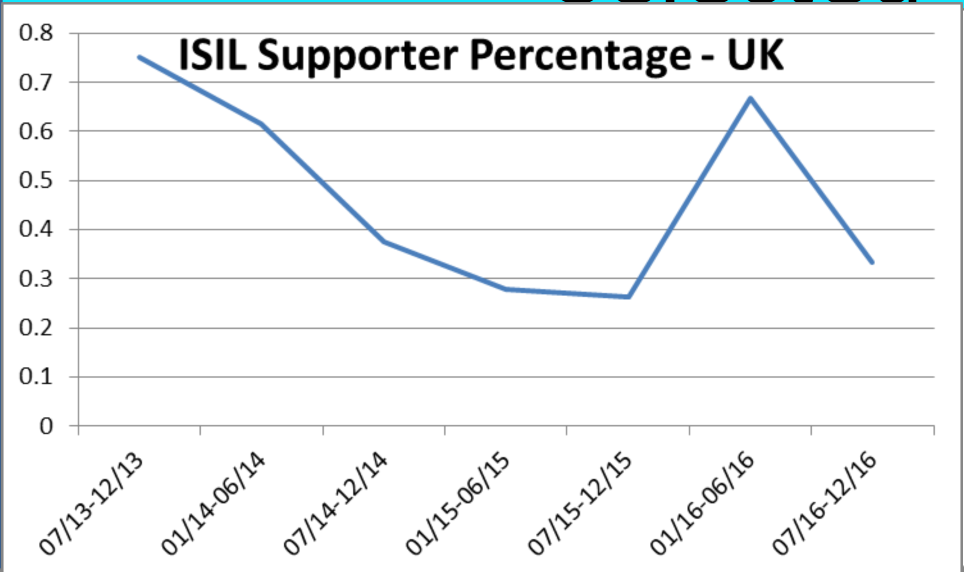
TIME FRAME	MOST SENTIMENT IN FAVOR OF ISIL (in decreasing order)
Mar-Sep 2013	Hungary, Germany, Malaysia, Chile, Indonesia
May-Oct 2016	Thailand, Tunisia, Ireland, Malaysia, UK, Indonesia

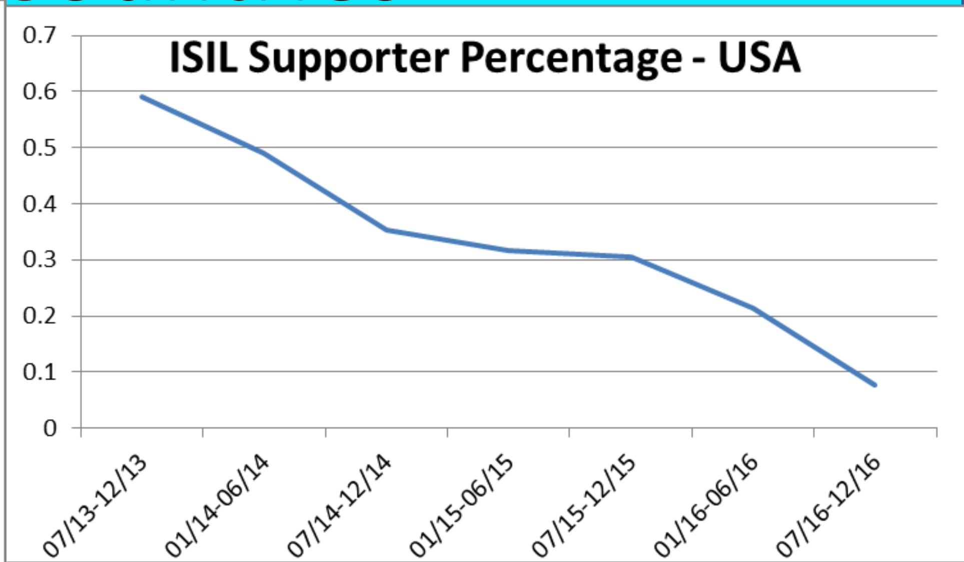
Fraction of ISIL Supporters on Twitte

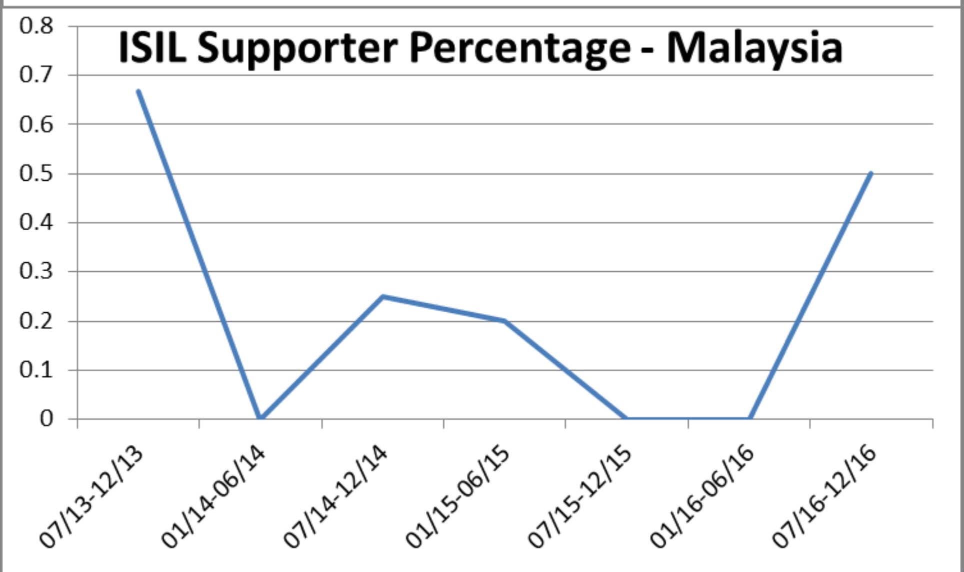


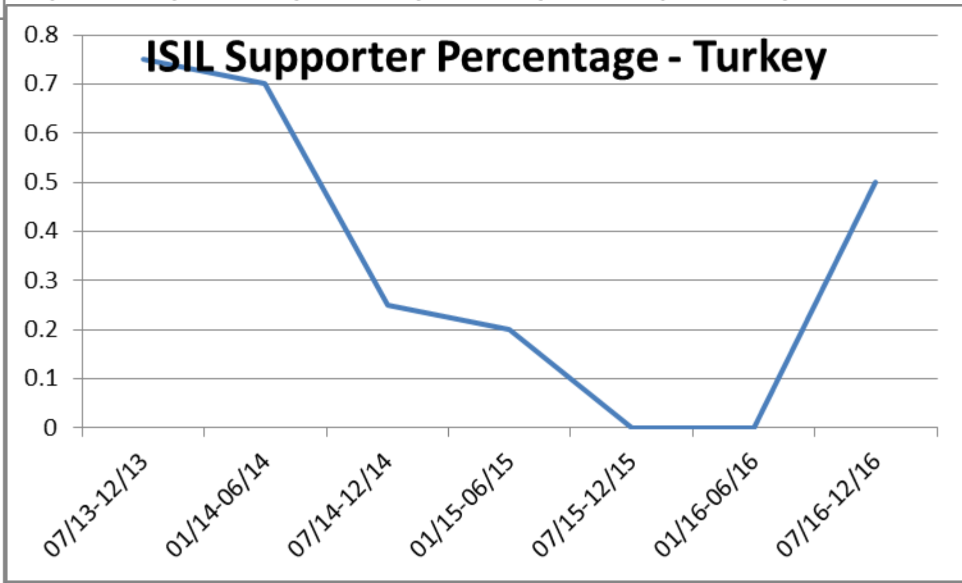
TIME FRAME	MOST FRACTION OF SUPPORTERS FOR ISIL (in decreasing order)
Mar-Sep 2013	Indonesia, Turkey, Malaysia, USA, Germany
May-Oct 2016	Indonesia, Ireland, Thailand, Tunisia, Turkey, Malaysia, UK [all tied]

ISIL Supporter Percentage in Selected Countries









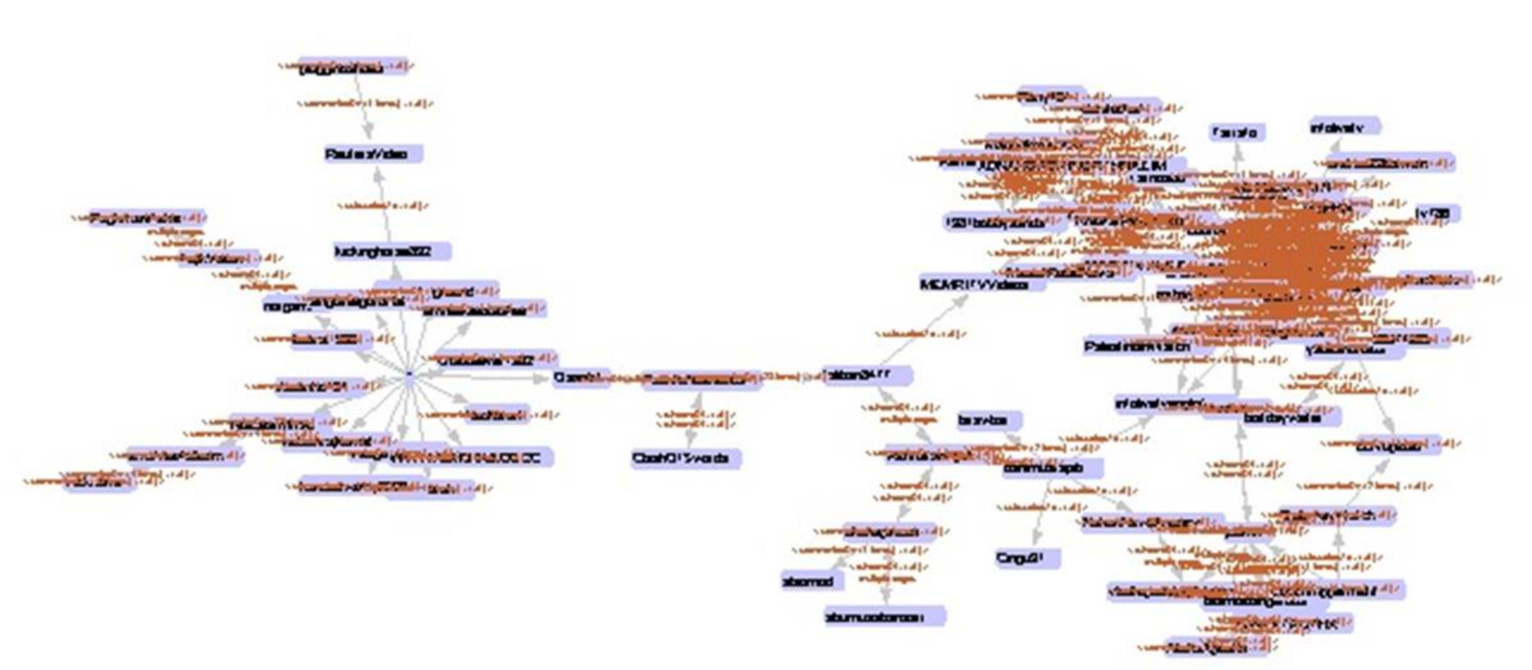
YouTube Data

- Total videos crawled: **1,320,039**
- Total users examined: **1,850,763**
  - Number of users who uploaded videos: **16,048**
- Total comments: **4,109,724**
  - posted by **972,705** distinct users

- Interactions among users:
  - **423,513** subscriptions to other users' content
  - **2,237,422** friendships
  - **1,913,858** "commenting" interactions

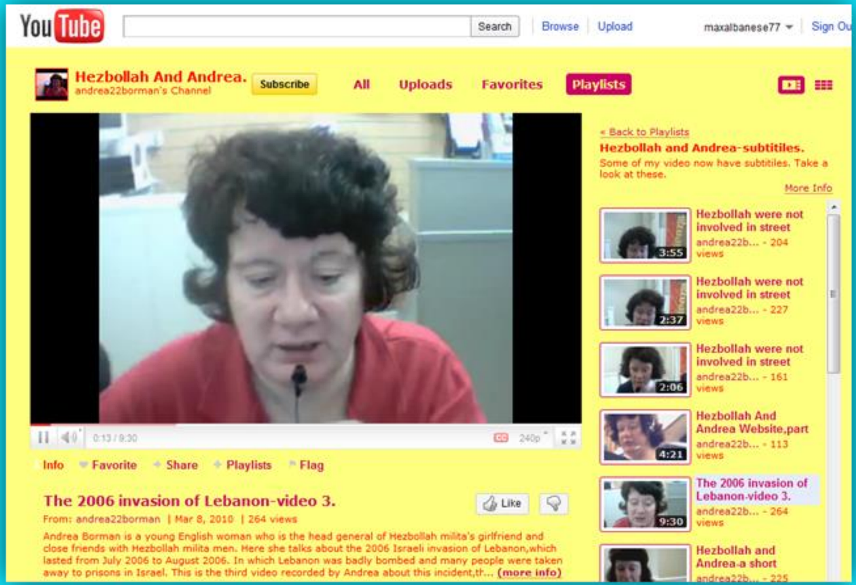
YouTube Data

- Relationships between YouTube users sympathetic to a given terrorist group: Except for a small number of isolated users, there is a large cluster of highly connected users, and several smaller satellite clusters of moderately connected users



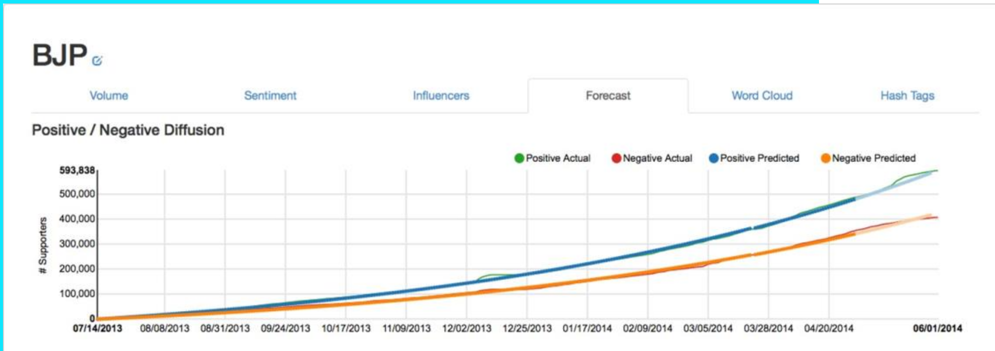
YouTube Data

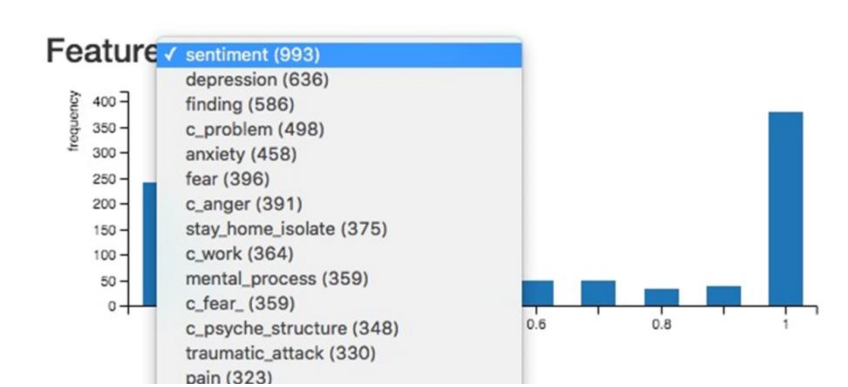
- Our system determined that YouTube user `andrea22borman` must be extremely relevant to Hezbollah
- Andrea Borman is allegedly romantically linked to a senior Hezbollah operative



Next Steps

- **Predict how support for or emotion about a terror group will spread through an online social network. Develop optimal counter-messaging schemes.**
- **Who are the key influencers in the social network?**





BJP

Volume | Sentiment | Influencers | Forecast | Word Cloud | Hash Tags

Screen Name	Followers	Tweets	Topic(s)	Status	Score
SqnLdrHusain	5047	94	bjp		0.00004421
newsxonline	890646	217	bjp	News Organization	0.00004346
yumroni	6970	79	bjp	Potential Bot	0.00004229
SukhSandhu	389061	56	bjp	Potential Bot	0.00004176
jiya043	8081	54	bjp		0.00004118
dilipvamanan	39764	186	bjp		0.00004040
STForeignDesk	15347	38	bjp		0.00003987
ItsShrishti	20161	33	bjp		0.00003975
AmeyaKambli	6372	35	bjp		0.00003952
dot_lawyer	10746	23	bjp		0.00003951
AlSalamanty	2716	42	bjp		0.00003929
AbhayIndia	89762	113	bjp		0.00003879

Sentimetrix has developed such *diffusion modeling* techniques in other domain (political tracking, health care) and predicted spread and key influencers.

Talk Outline

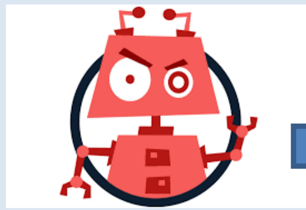
- **STONE Shaping Terrorist Organization Network Efficacy [joint with A. Mannes, F. Spezzano]**
  - **Quantifying Terror Network Lethality**
  - **Predicting Successors of a Removed Terrorist**
  - **Identifying Who to Remove**
- **Social Media Analytics of ISIL Activity [ongoing]**
  - **Twitter [with S. Kumar]**
  - **YouTube [with M. Albanese]**

- **The Upcoming Threat Landscape**
  - **Next 2-4 Years: Bots, Ransomware, Banking Trojans, Bitcoin & Cryptocurrencies**
  - **4-10 Years: ICS/SCADA, IoT Attacks**

Next 2-4 Years: Terrorist Financing

SMS-Fraud

FakeInstaller
JiFake
OpFake



Bitcoin

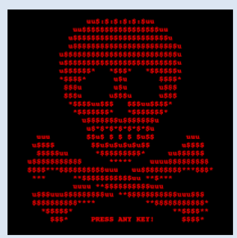
Payment channel!

Also hacked , e.g.

- Mt. Gox
- Poloniex

Ransomware

Locky
CryptoLocker
Wirelocker



Banking Trojans

Carbanak
Cobalt
Dridex
Dyre
OpFake

Next 5-10 Years: Terrorist Attacks

ICS-SCADA Threats

- Stuxnet hits Iranian nuclear centrifuges
- German steel mill hit in 2014
- Havex RAT targets Object Linking & Embedding for Process Control used in turbines, pumps etc
- Blacken targets uses of GE’s Cimplicity SCADA software

IoT-based Threats

- In October 2016, a Mirai based IoT attack brought down *Dyn*, a provider to Reddit, Twitter, Netflix,…
- In Sep 2016, researchers at Tencent successfully showed how the Tesla could be hacked, allowing them to gain some control over the brakes.

Conclusion

- **Terrorist groups (esp. ones with state support) will find new and innovative ways to carry out their activities and attacks.**
- **Social media will be increasingly leveraged through the use of**
  - **Bots, fake accounts, social media fraud, malware distribution**
- **Cyberattacks will be used in the next several years for everything from:**
  - **Financing**
  - **Physical attacks**
- **Cryptocurrencies will be increasingly used**

Contact Information

V.S. Subrahmanian
Dept. of Computer Science & UMIACS
University of Maryland
College Park, MD 20742.
Tel: 301-405-6724
Email: vs@cs.umd.edu
Web: www.cs.umd.edu/~vs/