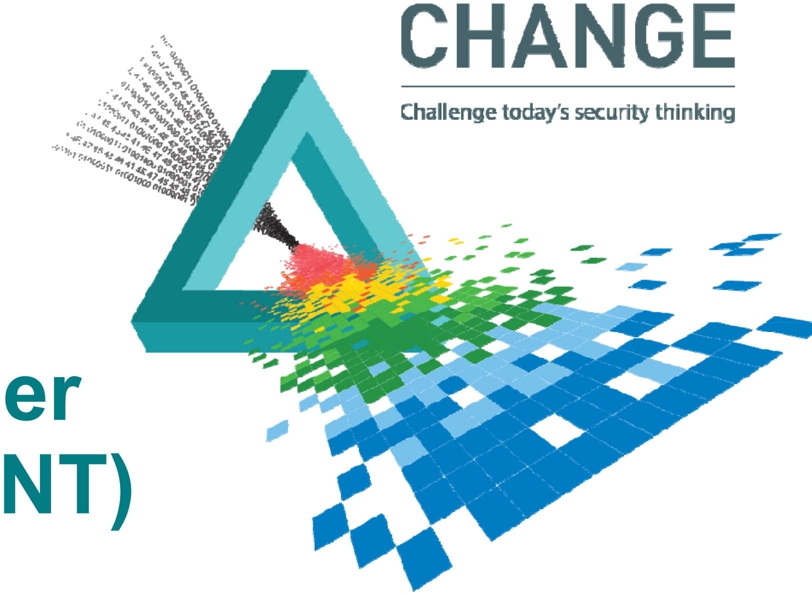
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking



SESSION ID: CCT-W10

Escalating Middle Eastern Cyber Tension: An Open Source (OSINT) Analysis

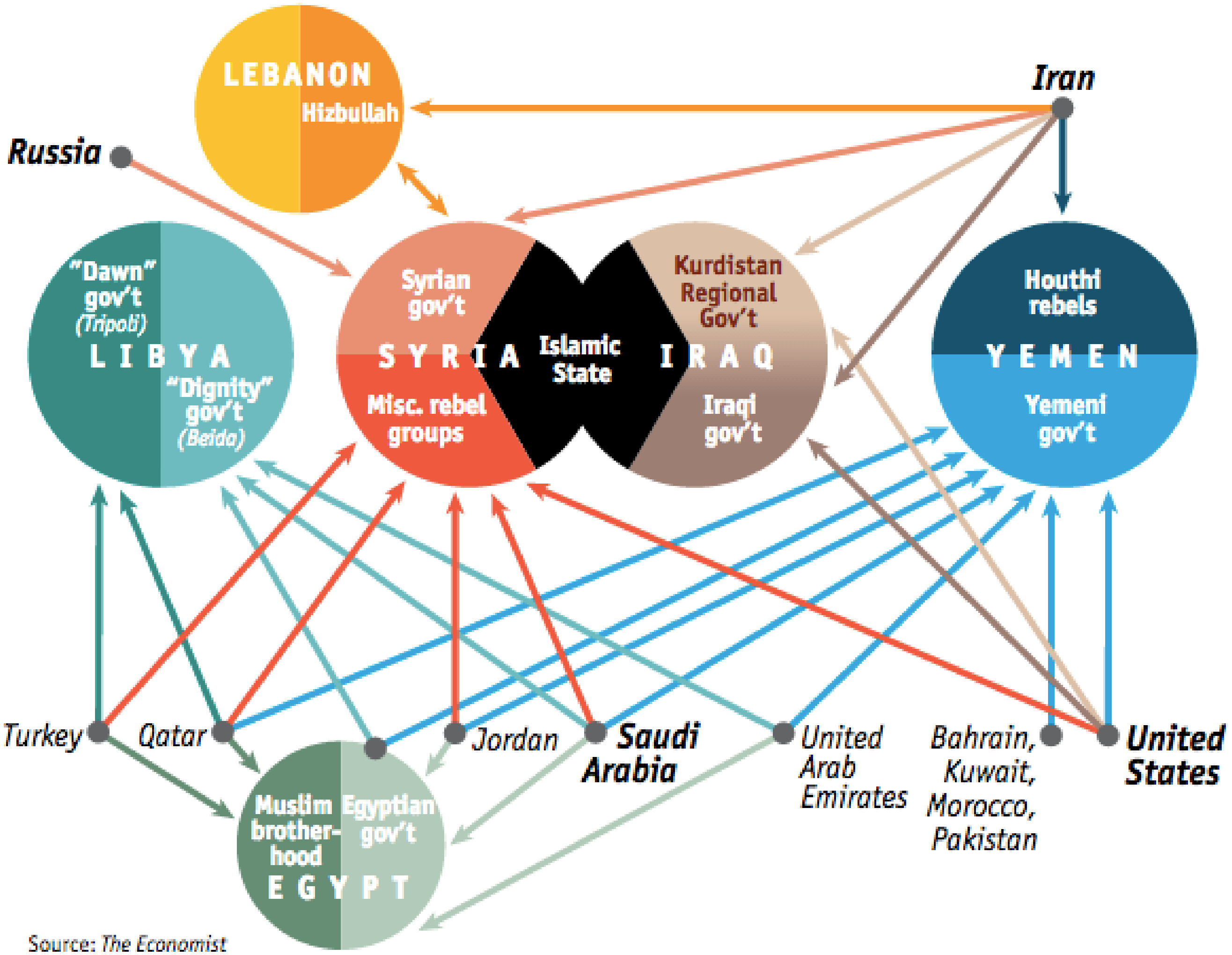
Dr. Christopher Ahlberg

CEO/Co-founder
Recorded Future
@cahlberg | c@recordedfuture.com | www.recordedfuture.com

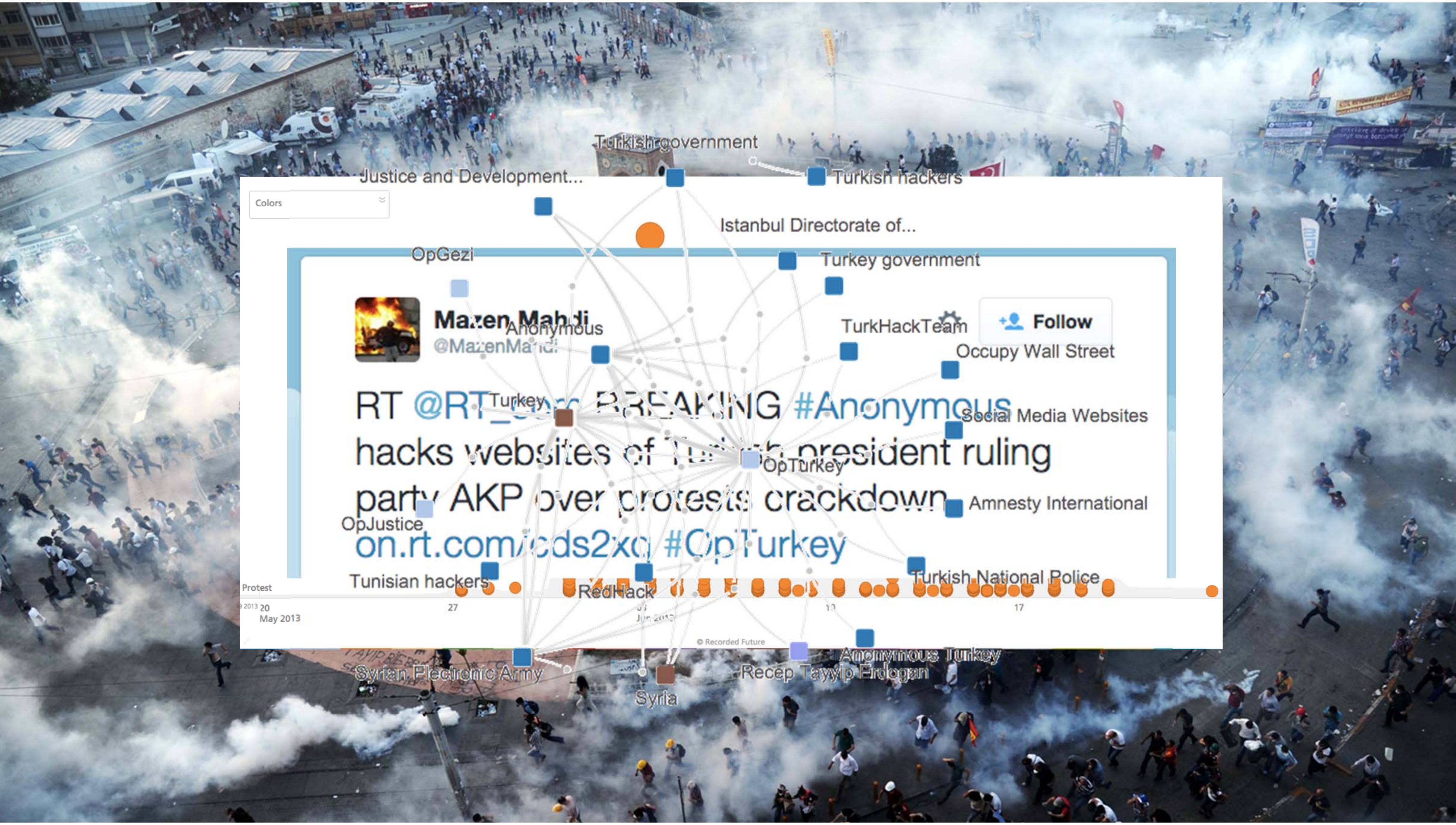
#RSAC

The main political rifts in the Middle East

Who openly backs whom *(select/tap labels to isolate connections)*



Source: *The Economist*



Mazen Mahdi
@MazenMahdi

Follow

RT @RT_com: BREAKING #Anonymous hacks websites of Turkish president ruling party AKP over protests crackdown on.rt.com/cds2xq #OpTurkey

Al Qassam Cyber Fighters (QCF)

July 2, 2012

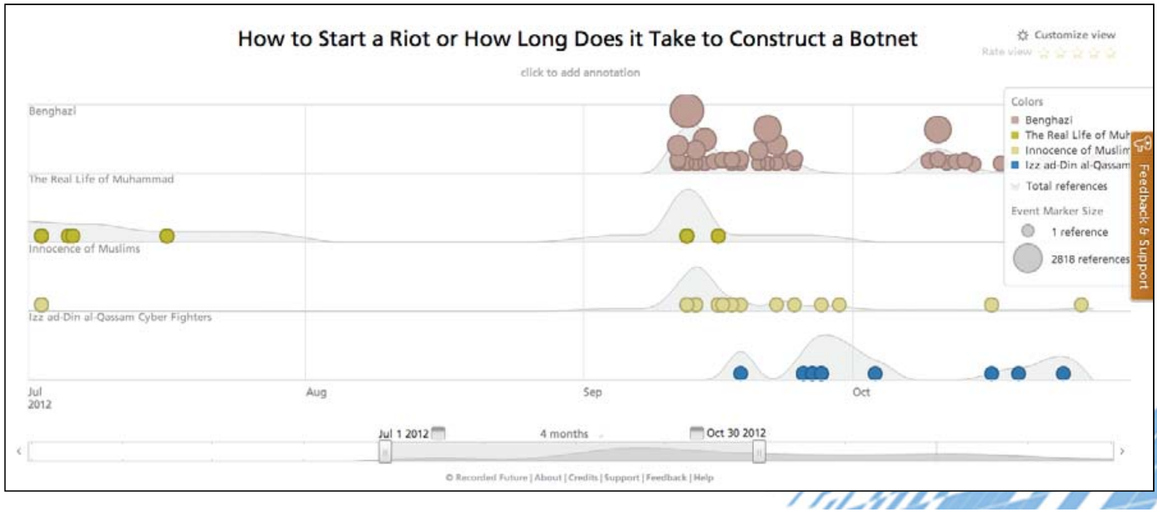
1. ‘Innocence of Muslims’ published on YouTube

September 11, 2012

2. Reactions starts and spreads quickly

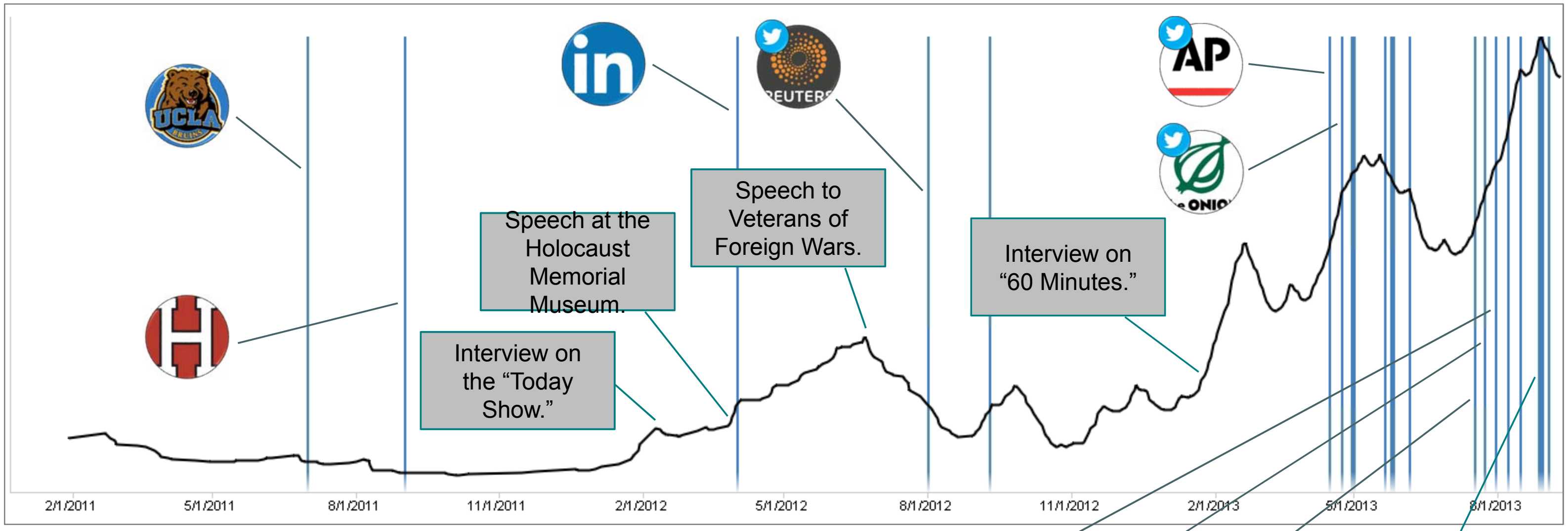
September 18, 2012

3. Al-Qassam Cyber Fighters starts Operation Ababil



How to Start a Riot or How Long Does it Take to Construct a Botnet

Political Rhetoric Versus Cyber Attacks



Speech at the Holocaust Memorial Museum.

Speech to Veterans of Foreign Wars.

Interview on "60 Minutes."

Interview on the "Today Show."

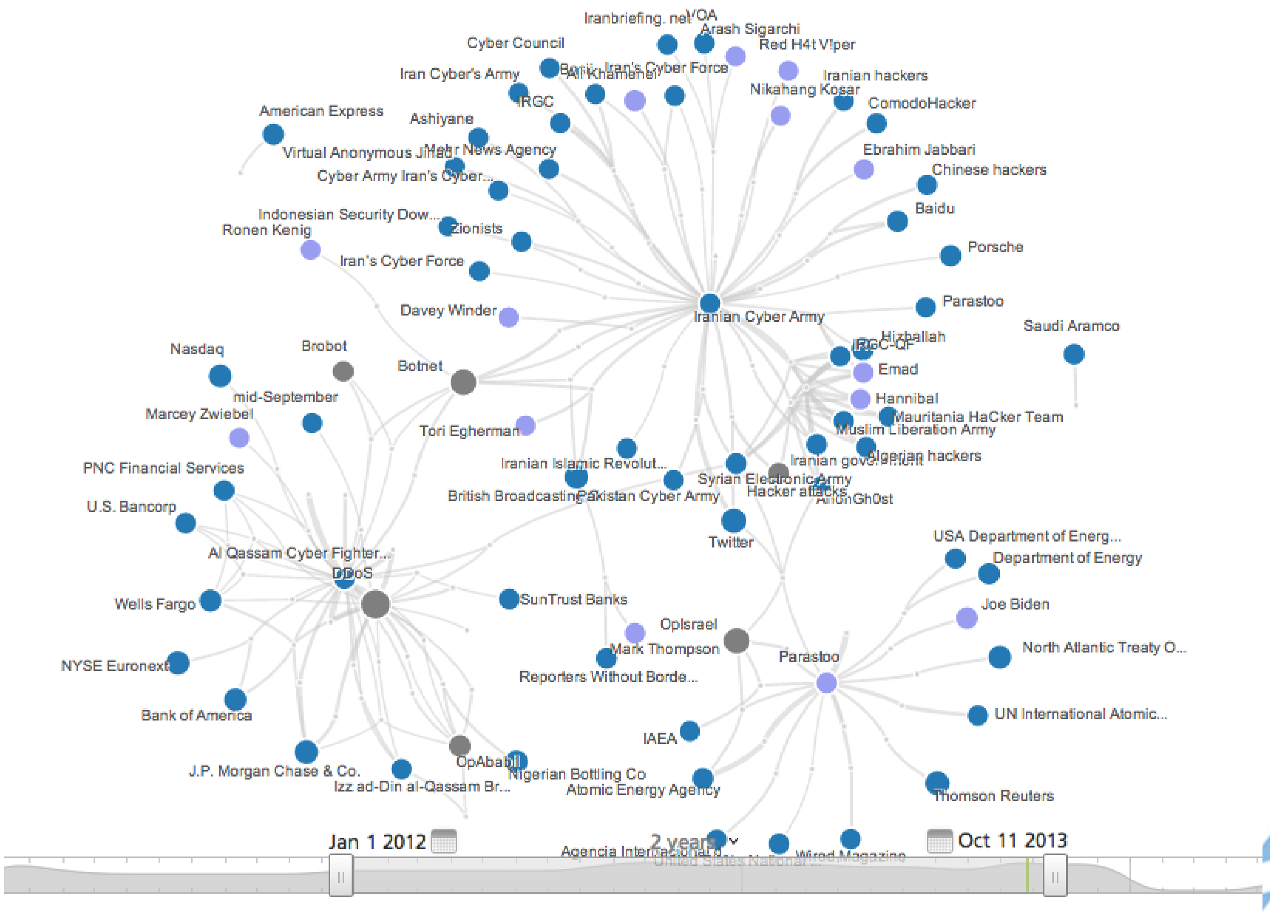
Seeks approval for military intervention.

Blue (vertical) lines are attacks by SEA

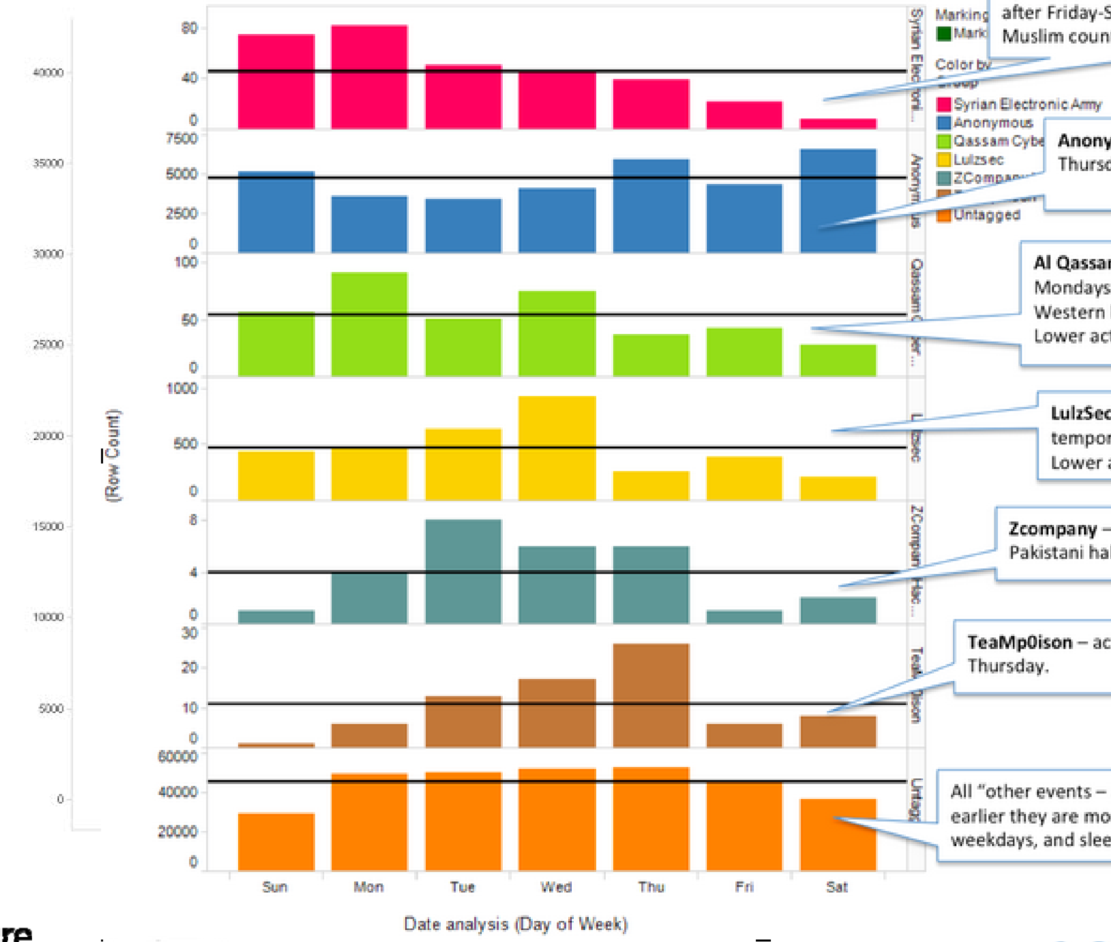
Black line is Barack Obama on Syria

Political focus driving attacks?
Attacks following media focus?
Attacks causing media focus?
Raising the bar on targets over time?

Targeting May Differ



Behavior is Harder to Fake



Syrian Electronic Army, activates right after Friday-Saturday weekend. 15 Muslim countries, including Syria itself.

Anonymous – activates weekends and Thursdays.

Al Qassam Cyber fighters – activates Mondays and Wednesdays. Given focus on Western banking this does make sense. Lower activity Muslim Thu/Fri/Sat.

LulzSec– activates Wednesday. Inverse temporal signature of **Anonymous**. Lower activity Thu/Fri/Sat.

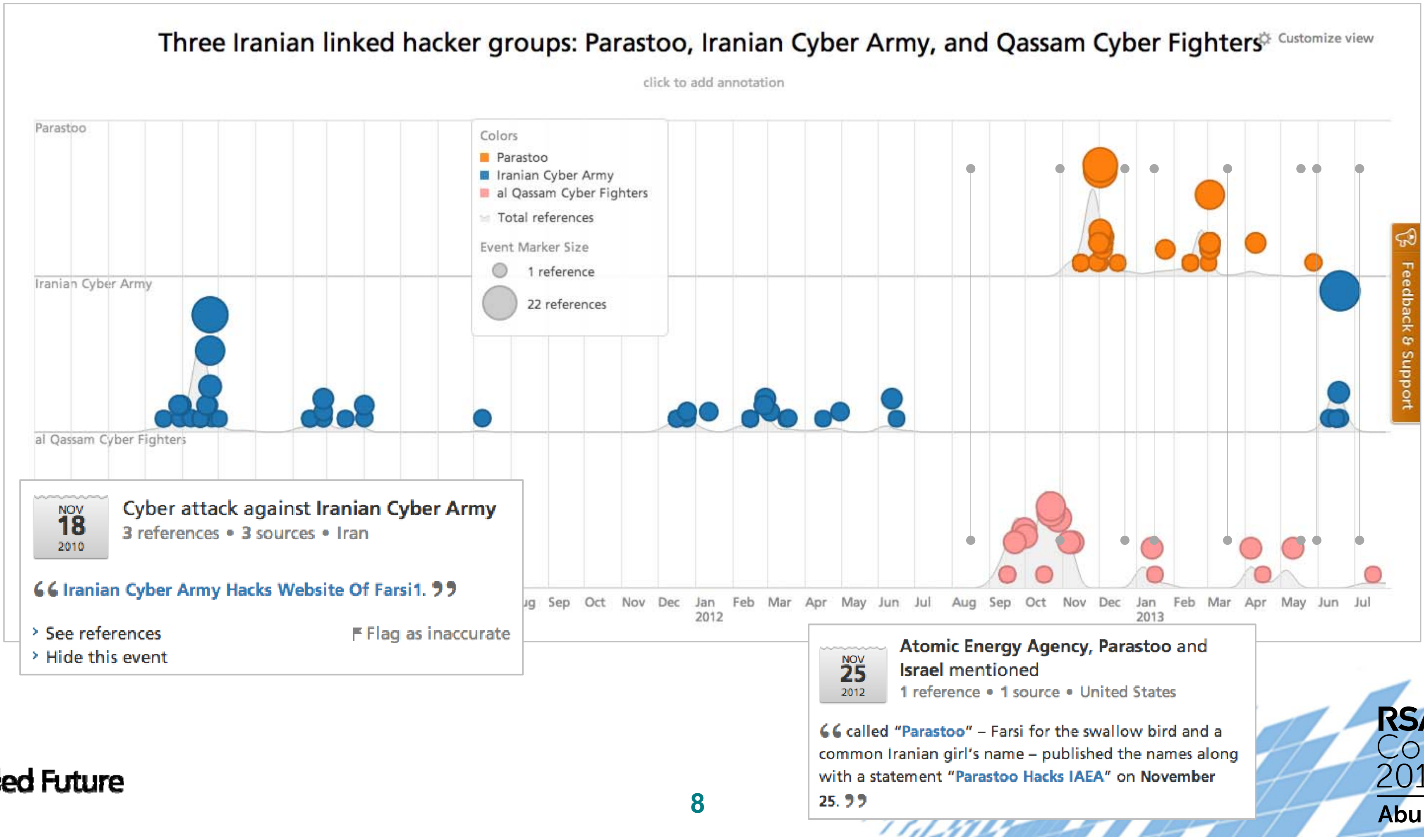
Zcompany – activates Mon-Thu. Follows Pakistani half-Friday, Sat/Sun off perfectly.

TeaMp0ison – activates Monday-Thursday.

All "other events – as we've established earlier they are more active on Western weekdays, and sleep in weekends

Recorded Future

And Patterns Lay Open in the Clear



NOV 18 2010

Cyber attack against Iranian Cyber Army

3 references • 3 sources • Iran

“Iranian Cyber Army Hacks Website Of Farsi1.”

› See references
› Hide this event

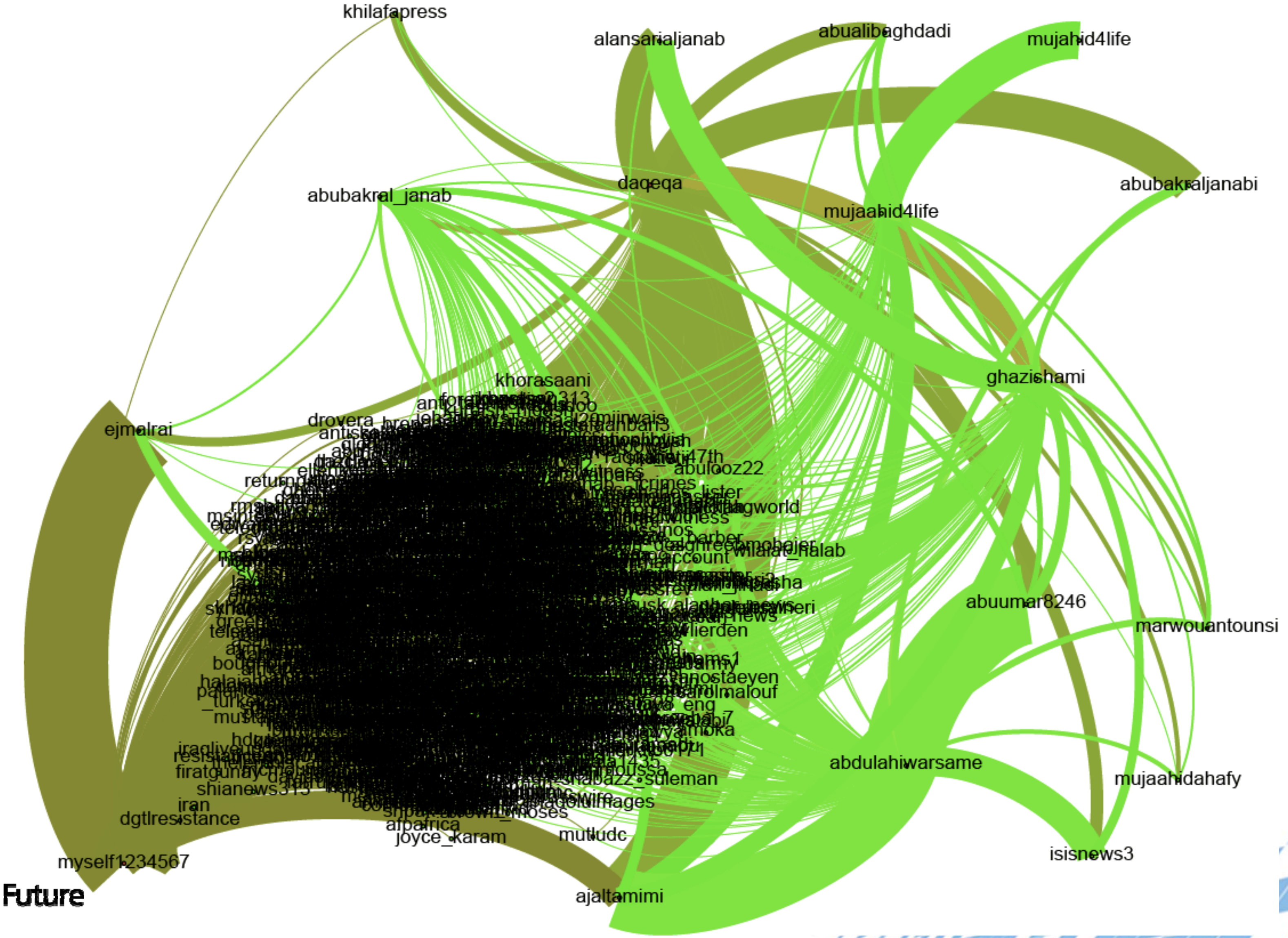
Flag as inaccurate

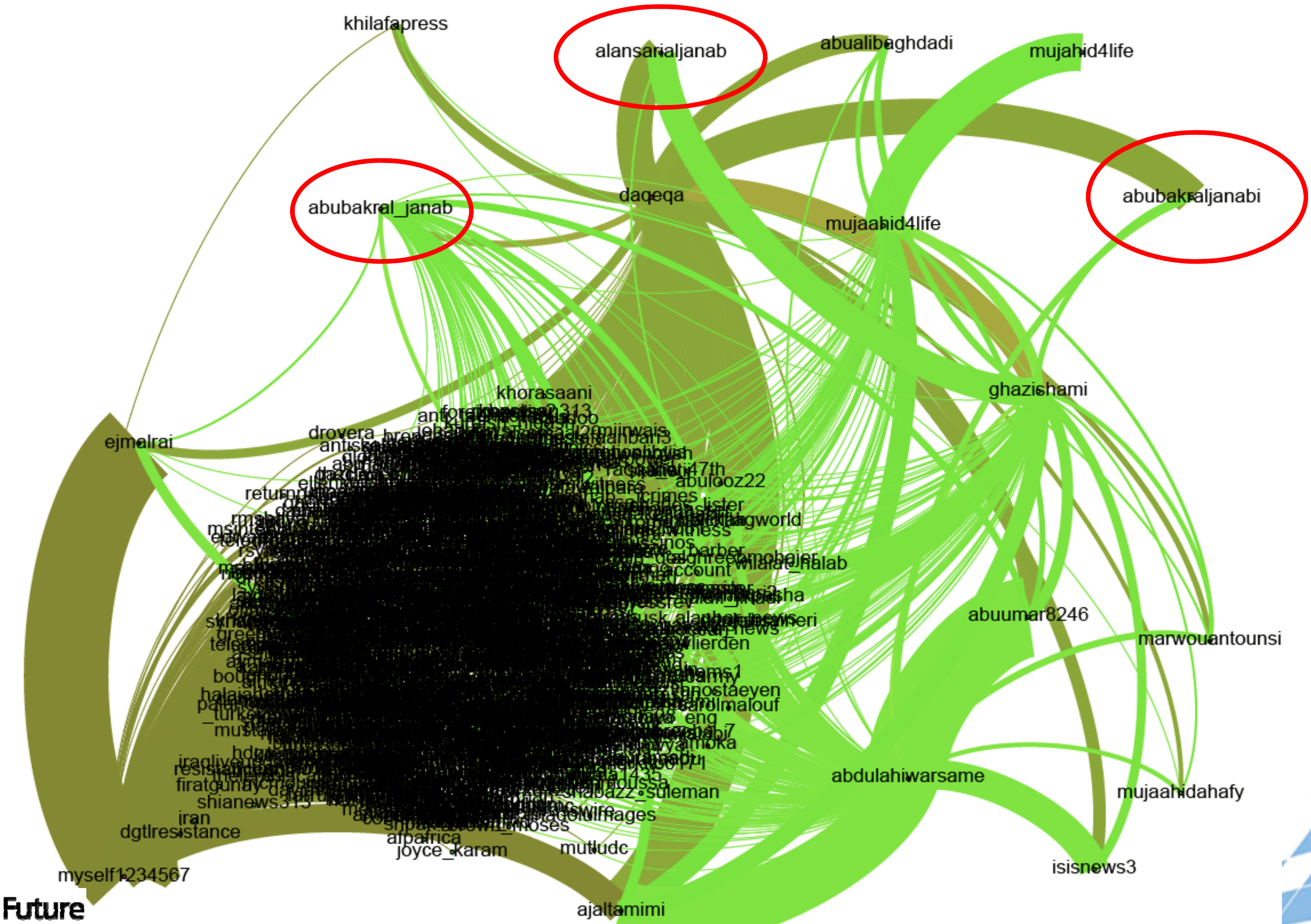
NOV 25 2012

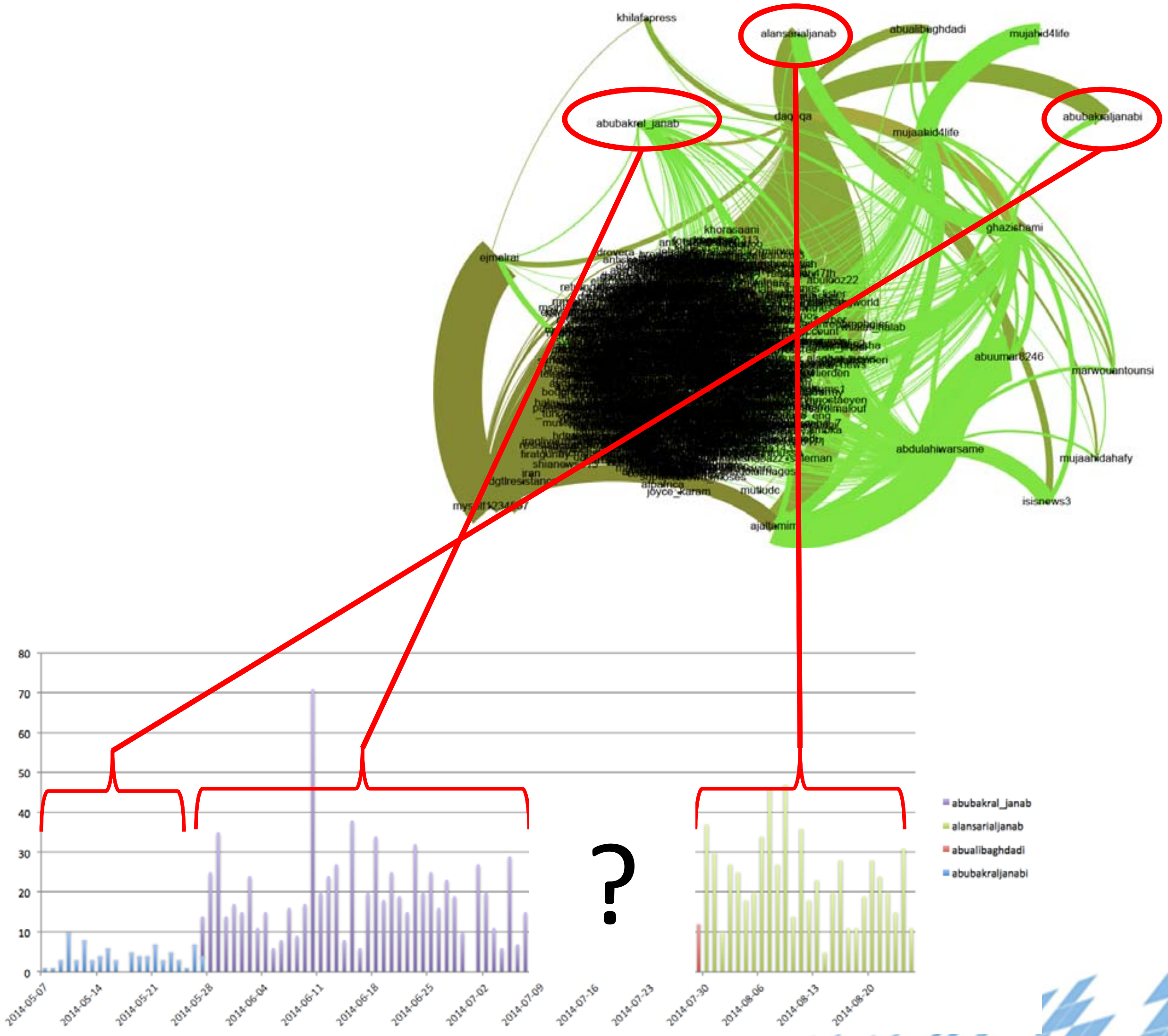
Atomic Energy Agency, Parastoo and Israel mentioned

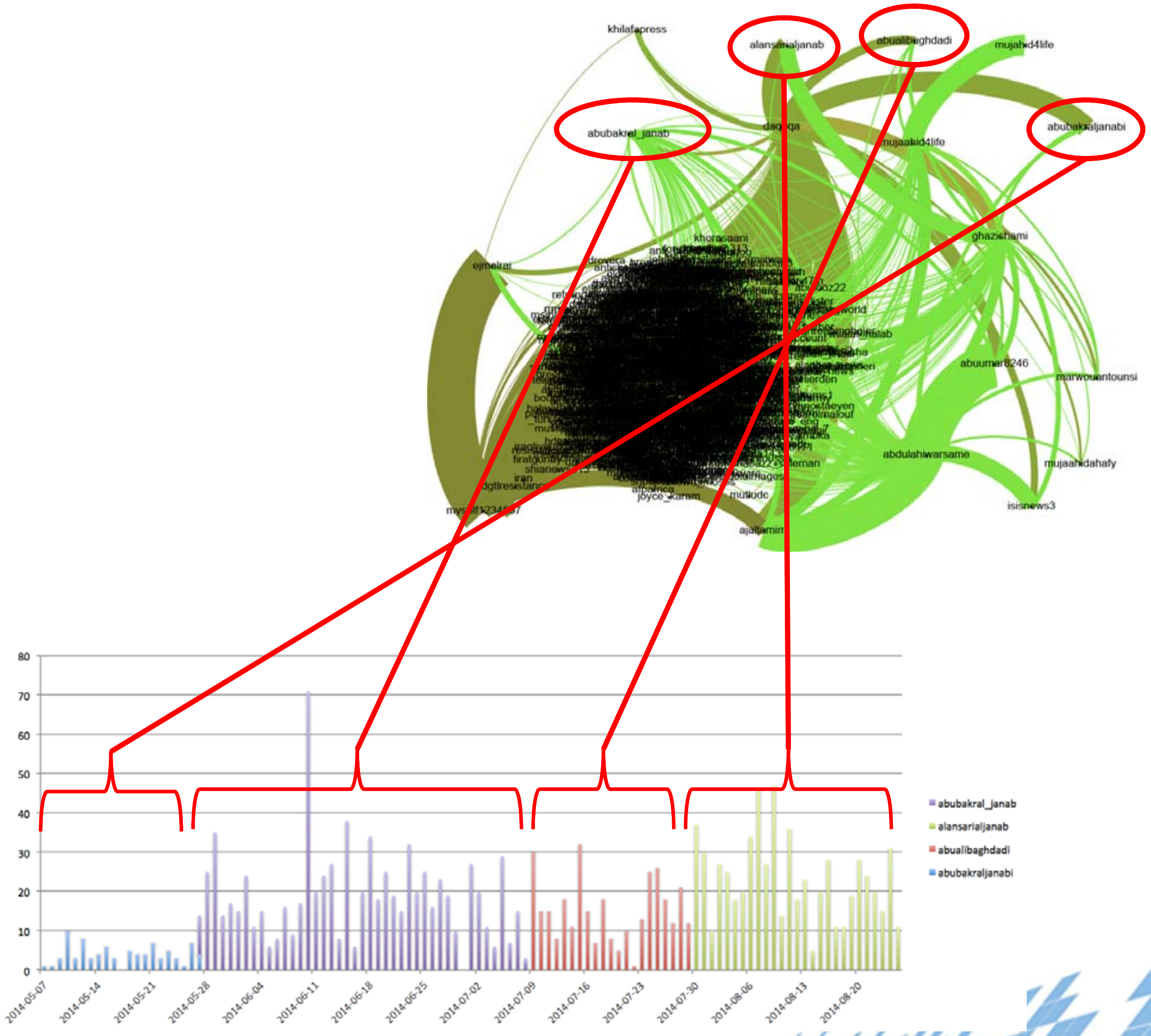
1 reference • 1 source • United States

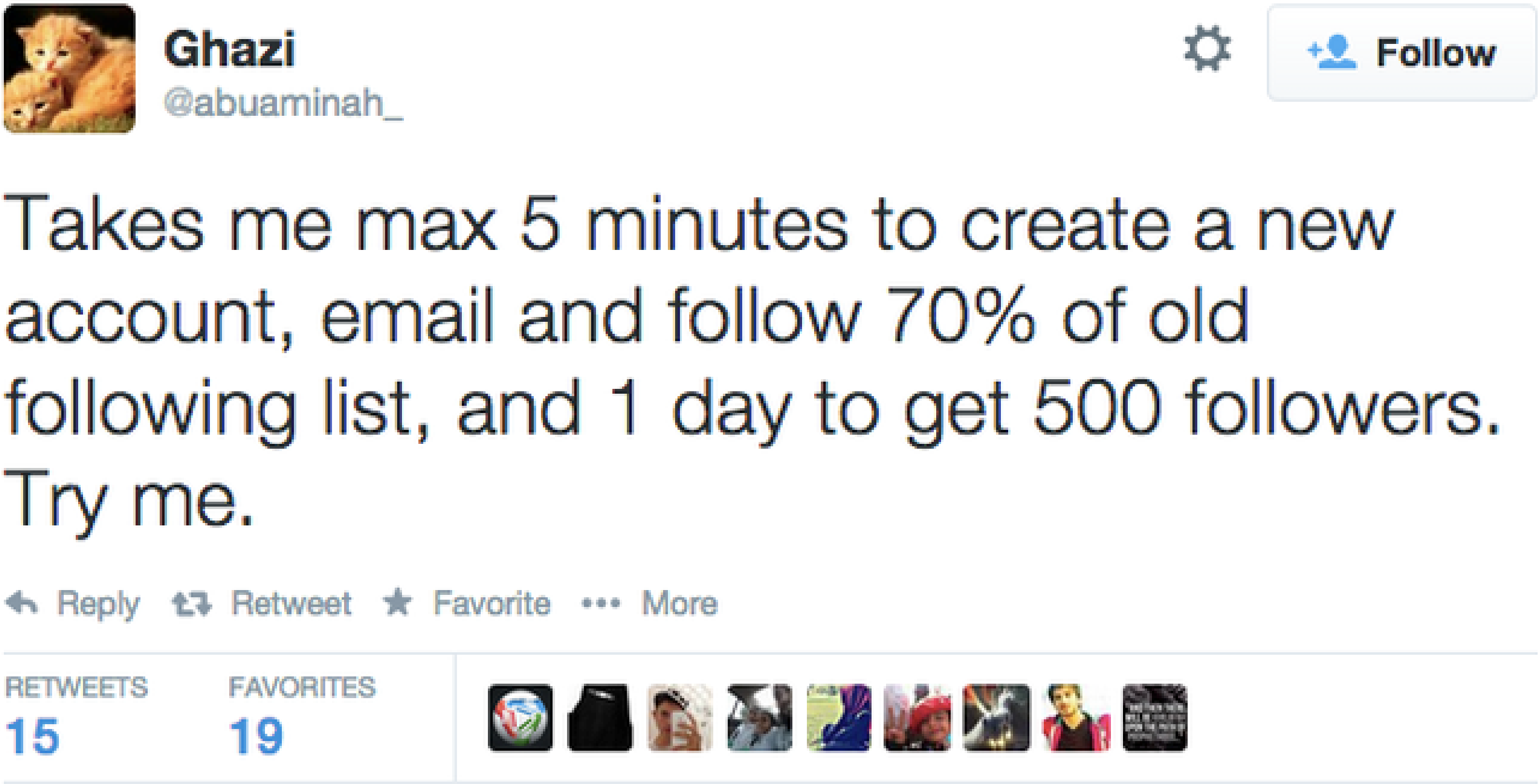
“called “Parastoo” – Farsi for the swallow bird and a common Iranian girl's name – published the names along with a statement “Parastoo Hacks IAEA” on November 25.”


khilafapress
alansarialjanab
abualibaghdadi
mujahid4life
abubakral_janab
daqeqa
mujaahid4life
abubakraljanabi
khorasaani
ghazishami
ejmalrai
drovera
abulooz22
wilaiat_halab
abuumar8246
marwouantounsi
abdulahiwarsame
mujaahidahafy
isisnews3
shianews313
iran
dgtlresistance
myself1234567
afpafrica
joyce_karam
mutludc
ajaltamimi


khilafapress
alansarialjanab
abualibaghdadi
mujahid4life
abubakral_janab
daqeqa
mujaahid4life
abubakraljanabi
khorasaani
ejmalrai
drovera
ghazishami
abulooz22
wilaiat_halab
abuumar8246
marwouantounsi
abdulahiwarsame
mujaahidahafy
isisnews3
dgtlresistance
iran
shianews313
myself1234567
afpafrica
joyce_karam
mutludc
ajaltamimi


khilafapress
alansarialjanab
abualibaghdadi
mujahid4life
abubakral_janab
daqiqa
mujaahid4life
abubakraljanabi
khorasaani
ghazishami
ejmalrai
abulooz22
abuumar8246
marwouantounsi
abdulahiwarsame
mujaahidahafy
isisnews3
joyce_karam
mutludc
ajaltamimi
myself1234567
dgtlresistance
iran
shianews
firatgunby
80
70
60
50
40
30
20
10
0
2014-05-07
2014-05-14
2014-05-21
2014-05-28
2014-06-04
2014-06-11
2014-06-18
2014-06-25
2014-07-02
2014-07-09
2014-07-16
2014-07-23
2014-07-30
2014-08-06
2014-08-13
2014-08-20
?
abubakral_janab
alansarialjanab
abualibaghdadi
abubakraljanabi

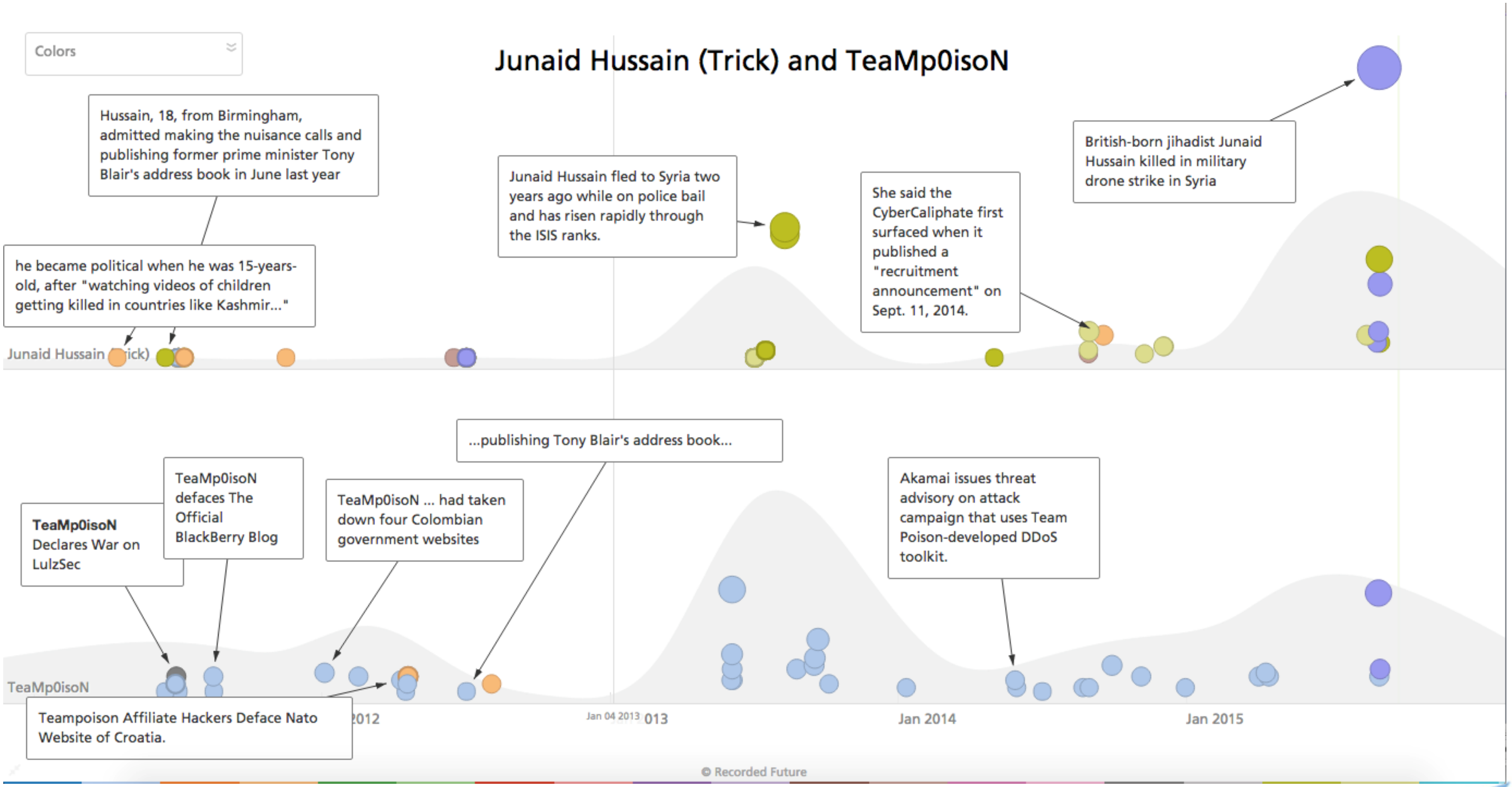

khilafapress
alansarialjanab
abualibaghdadi
mujahid4life
abubakral_janab
daqiqa
mujaahid4life
abubakraljanabi
ghazishami
ejmalrai
khorasaani
abuumar8246
marwouantounsi
abdulahiwarsame
mujaahidahafy
isisnews3
joyce_karam
mutludc
80
70
60
50
40
30
20
10
0
2014-05-07
2014-05-14
2014-05-21
2014-05-28
2014-06-04
2014-06-11
2014-06-18
2014-06-25
2014-07-02
2014-07-09
2014-07-16
2014-07-23
2014-07-30
2014-08-06
2014-08-13
2014-08-20
abubakral_janab
alansarialjanab
abualibaghdadi
abubakraljanabi



Ghazi
@abuaminah_

Takes me max 5 minutes to create a new account, email and follow 70% of old following list, and 1 day to get 500 followers. Try me.

RETWEETS 15
FAVORITES 19



Junaid Hussain (Trick) and TeaMp0isoN

Hussain, 18, from Birmingham, admitted making the nuisance calls and publishing former prime minister Tony Blair's address book in June last year

he became political when he was 15-years-old, after "watching videos of children getting killed in countries like Kashmir..."

Junaid Hussain fled to Syria two years ago while on police bail and has risen rapidly through the ISIS ranks.

She said the CyberCaliphate first surfaced when it published a "recruitment announcement" on Sept. 11, 2014.

British-born jihadist Junaid Hussain killed in military drone strike in Syria

...publishing Tony Blair's address book...

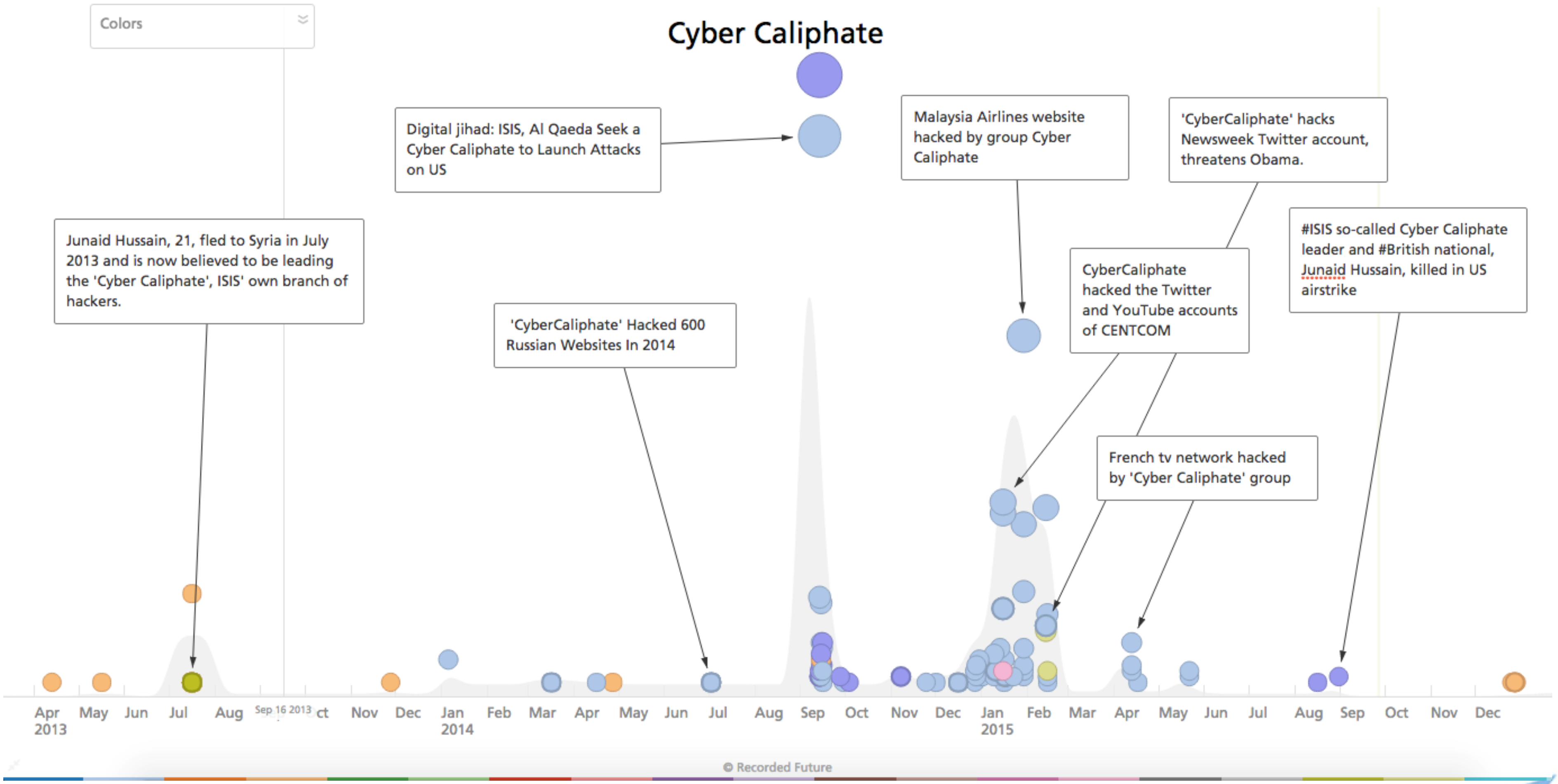
TeaMp0isoN Declares War on LulzSec

TeaMp0isoN defaces The Official BlackBerry Blog

TeaMp0isoN ... had taken down four Colombian government websites

Akamai issues threat advisory on attack campaign that uses Team Poison-developed DDoS toolkit.

Teampoison Affiliate Hackers Deface Nato Website of Croatia.



Cyber Caliphate

Junaid Hussain, 21, fled to Syria in July 2013 and is now believed to be leading the 'Cyber Caliphate', ISIS' own branch of hackers.

Digital jihad: ISIS, Al Qaeda Seek a Cyber Caliphate to Launch Attacks on US

'CyberCaliphate' Hacked 600 Russian Websites In 2014

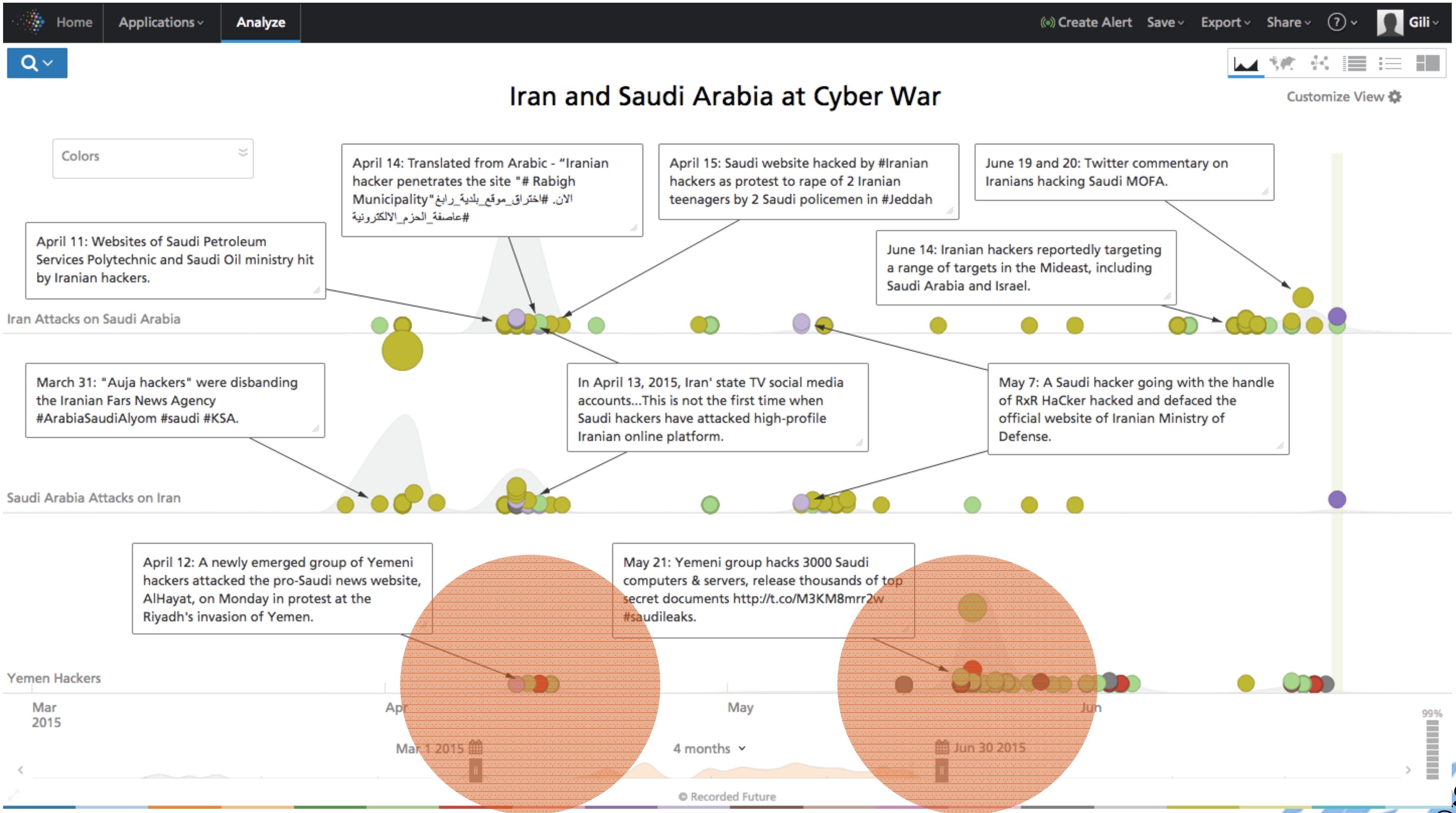
Malaysia Airlines website hacked by group Cyber Caliphate

'CyberCaliphate' hacks Newsweek Twitter account, threatens Obama.

CyberCaliphate hacked the Twitter and YouTube accounts of CENTCOM

French tv network hacked by 'Cyber Caliphate' group

#ISIS so-called Cyber Caliphate leader and #British national, Junaid Hussain, killed in US airstrike



Iran and Saudi Arabia at Cyber War

April 14: Translated from Arabic - “Iranian hacker penetrates the site "# Rabigh Municipality"الان. #اختراق_موقع_بلدية_رابغ
#عاصفة_الحزم_الالكترونية

April 15: Saudi website hacked by #Iranian hackers as protest to rape of 2 Iranian teenagers by 2 Saudi policemen in #Jeddah

June 19 and 20: Twitter commentary on Iranians hacking Saudi MOFA.

April 11: Websites of Saudi Petroleum Services Polytechnic and Saudi Oil ministry hit by Iranian hackers.

June 14: Iranian hackers reportedly targeting a range of targets in the Mideast, including Saudi Arabia and Israel.

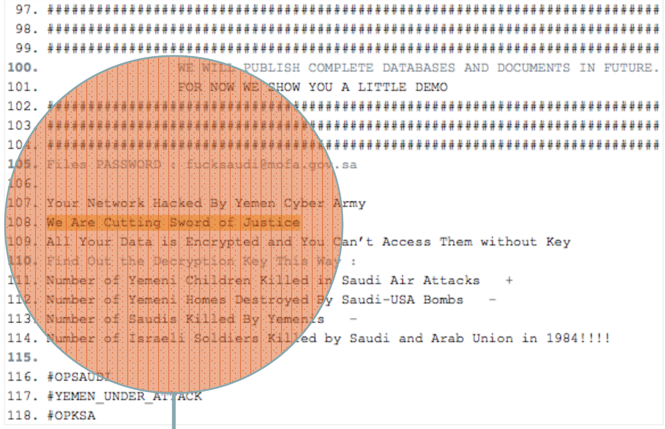
March 31: "Auja hackers" were disbanding the Iranian Fars News Agency #ArabiaSaudiAlyom #saudi #KSA.

In April 13, 2015, Iran' state TV social media accounts...This is not the first time when Saudi hackers have attacked high-profile Iranian online platform.

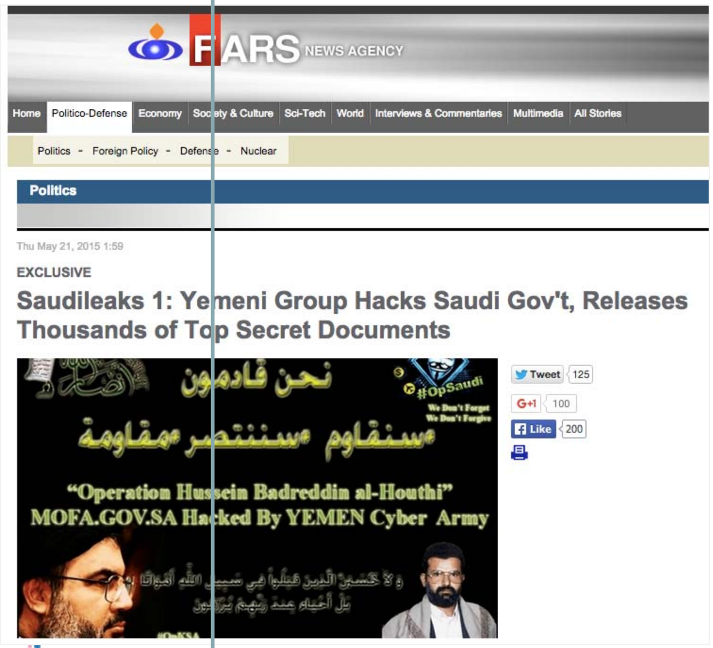
May 7: A Saudi hacker going with the handle of RxR HaCker hacked and defaced the official website of Iranian Ministry of Defense.

April 12: A newly emerged group of Yemeni hackers attacked the pro-Saudi news website, AlHayat, on Monday in protest at the Riyadh's invasion of Yemen.

May 21: Yemeni group hacks 3000 Saudi computers & servers, release thousands of top secret documents http://t.co/M3KM8mrr2w #saudileaks.



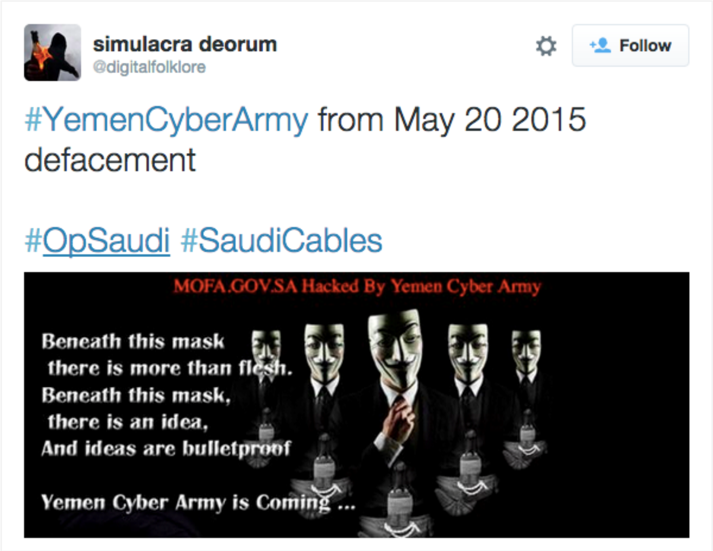
```
##########################################################################
##########################################################################
##########################################################################
             WE WILL PUBLISH COMPLETE DATABASES AND DOCUMENTS IN FUTURE.
             FOR NOW WE SHOW YOU A LITTLE DEMO
##########################################################################
##########################################################################
##########################################################################
Files PASSWORD : fucksaudi@mofa.gov.sa

Your Network Hacked By Yemen Cyber Army
We Are Cutting Sword of Justice
All Your Data is Encrypted and You Can't Access Them without Key
Find Out the Decryption Key This Way :
Number of Yemeni Children Killed in Saudi Air Attacks    +
Number of Yemeni Homes Destroyed By Saudi-USA Bombs    -
Number of Saudis Killed By Yemenis    -
Number of Israeli Soldiers Killed by Saudi and Arab Union in 1984!!!!

#OPSAUDI
#YEMEN_UNDER_ATTACK
#OPKSA
```



Thu May 21, 2015 1:59

EXCLUSIVE

Saudileaks 1: Yemeni Group Hacks Saudi Gov't, Releases Thousands of Top Secret Documents

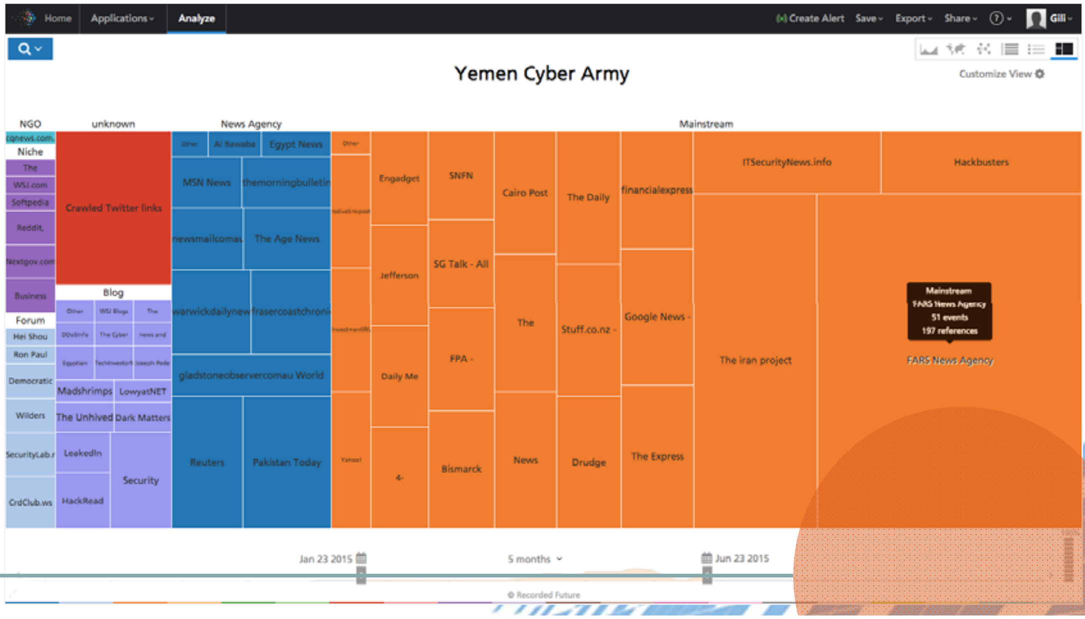


simulacra deorum
@digitalfolklore

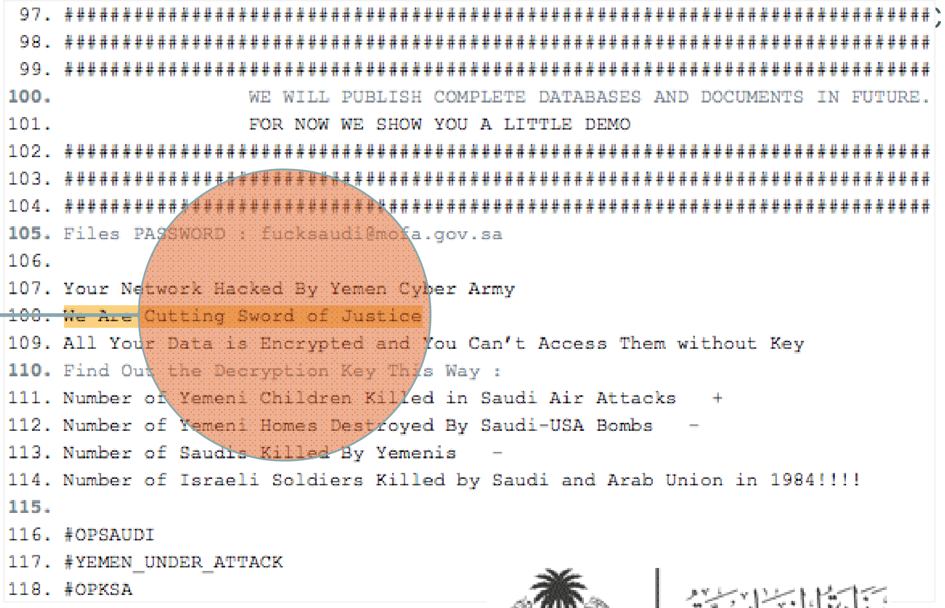
#YemenCyberArmy from May 20 2015 defacement

#OpSaudi #SaudiCables

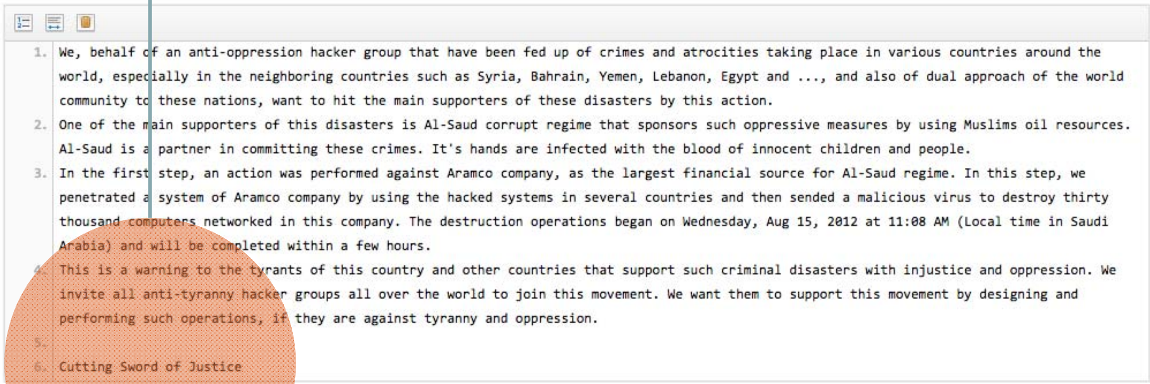
MOFA.GOV.SA Hacked By Yemen Cyber Army
Beneath this mask
there is more than flesh.
Beneath this mask,
there is an idea,
And ideas are bulletproof
Yemen Cyber Army is Coming ...



Cutting Sword of Justice



```
########################################################################
########################################################################
########################################################################
                WE WILL PUBLISH COMPLETE DATABASES AND DOCUMENTS IN FUTURE.
                FOR NOW WE SHOW YOU A LITTLE DEMO
########################################################################
########################################################################
########################################################################
Files PASSWORD : fucksaudi@mofa.gov.sa

Your Network Hacked By Yemen Cyber Army
We Are Cutting Sword of Justice
All Your Data is Encrypted and You Can't Access Them without Key
Find Out the Decryption Key This Way :
Number of Yemeni Children Killed in Saudi Air Attacks   +
Number of Yemeni Homes Destroyed By Saudi-USA Bombs   -
Number of Saudis Killed By Yemenis   -
Number of Israeli Soldiers Killed by Saudi and Arab Union in 1984!!!!

#OPSAUDI
#YEMEN_UNDER_ATTACK
#OPKSA
```



We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.

One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.

In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.

This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.

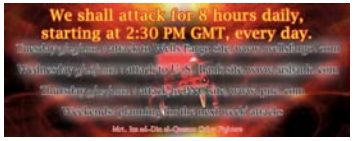
Cutting Sword of Justice

Yemeni cyber capability?

QuickLeak.ir

No social media profile

Fars News



We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day.

Tuesday [illegible]: attack to Wells Fargo site, www.wellsfargo.com

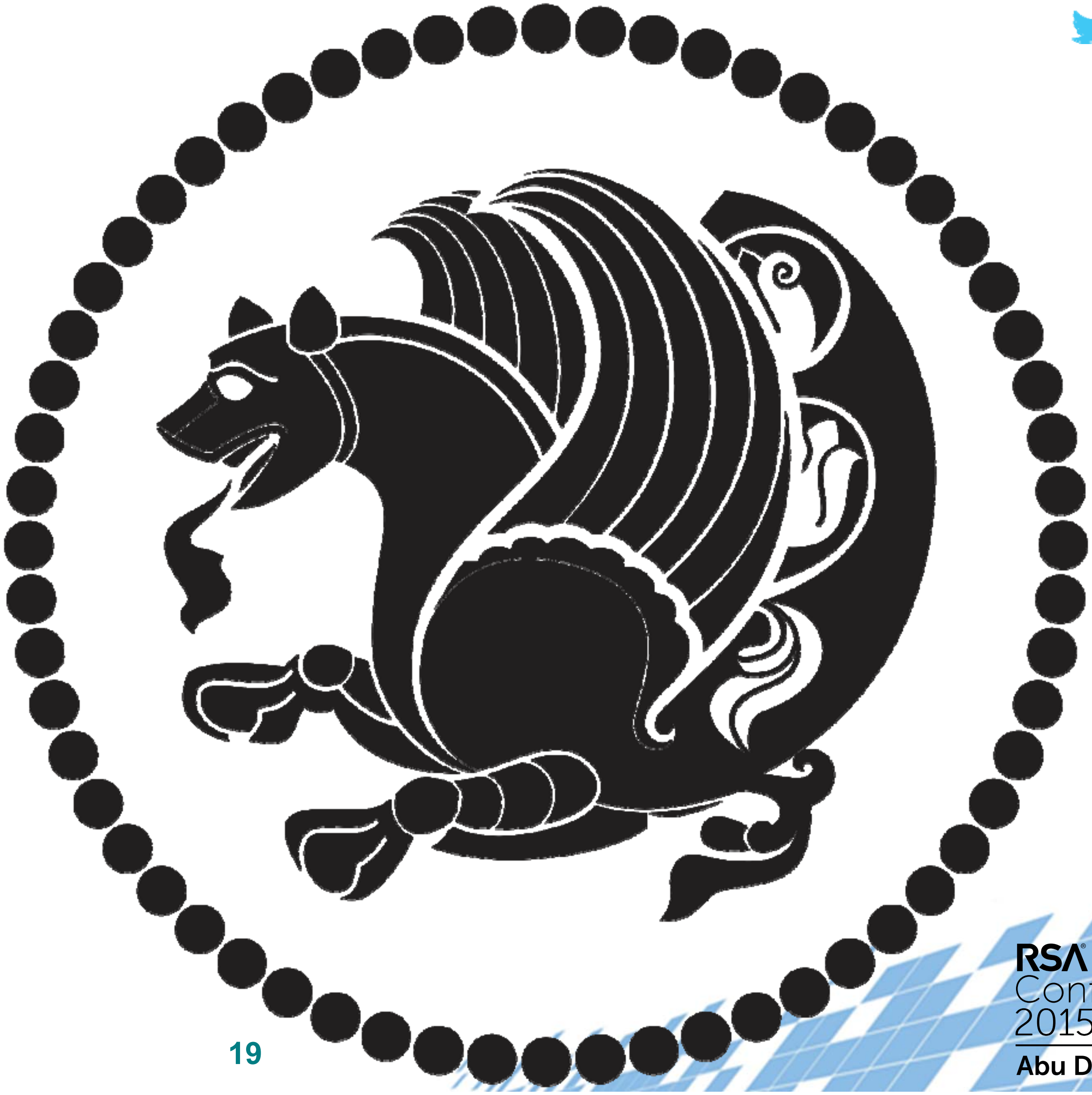
Wednesday [illegible]: attack to U.S. Bank site, www.usbank.com

Thursday [illegible]: attack to PNC site, www.pnc.com

Weekends: planning for the next week's attacks

Mrt. Izz ad-Din al-Qassam Cyber Fighters

Parastoo



Cutting
Sword of Justice

Recorded Future

Defenders Matrix

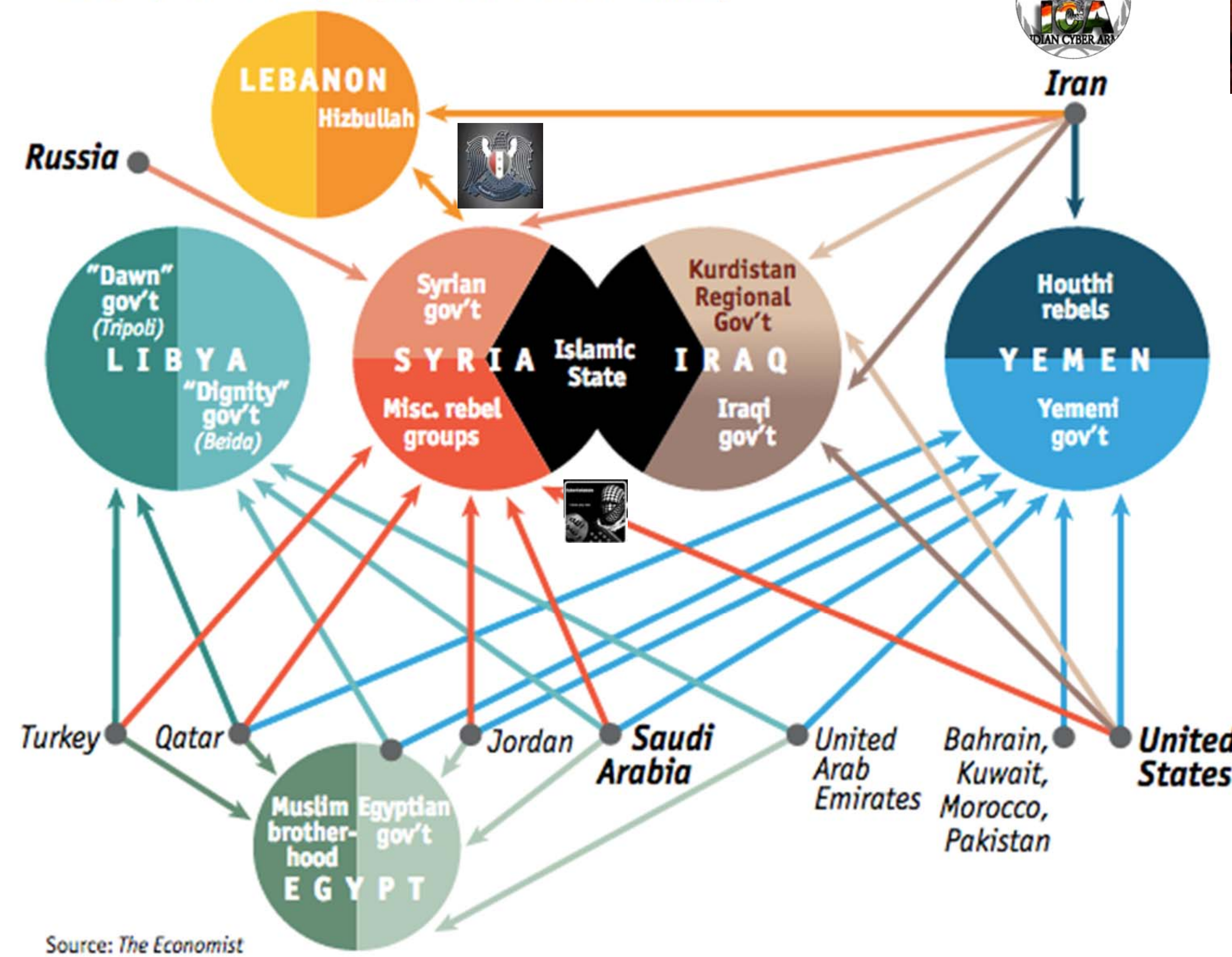
	Qassam Cyber Fighters	Iranian Cyber Army	Parastoo	Cutting Sword of Justice	Yemen Cyber Army	Cyber Caliphate	Syrian Electronic Army
Targeting	US+UK Banks	Domestic Iran, China, Azerbaijan, VOA Farsi	IAEA, US gov, Saudi, Israel	Saudi	Saudi Government	US DoD US Media Random websites	Western Media Companies
Media outlet	hilf-ol-fozoul. blogspot.com				Fars News Agency Wikileaks		
Social media outlet	None	None	None	None	None	Twitter	Twitter Facebook
TTPs	DDoS / Brobot	Web befacing	Web defacing	Destructive malware / Shamoon	Defacing Document exfiltration	Twitter defacing/message publication	Phishing platform + defacing RATs
Pre-announced attacks	Yes	No	Yes	No	No	No	No
Dropbox	Pastebin		Quickleaks/Cryptome	Pastebin	Quickeaks Pastebin	JustPaste.it	sea.sy archive.is

Lessons for the Defender

- Track geopolitical backdrop
- Know your threat
- Adjust defenses to actors
- Identify technical capabilities and indicators for actors
- Track and monitor actor behavior, key sources, and events driving them

The main political rifts in the Middle East

Who openly backs whom (*select/tap labels to isolate connections*)



Source: *The Economist*

We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day.

Conclusions

- Middle East Actors have distinct behavior
  - Geopolitics sets the agenda
  - Chasing shadows
  - War by proxy
  - Actors have defined targeting, infrastructure, behavior, etc.
- Defender recommendations
  - OSINT can be used to monitor and stay ahead
  - Carefully map actor threat profile to operational stance
  - Be on your toes!