RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: CCT-W10

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

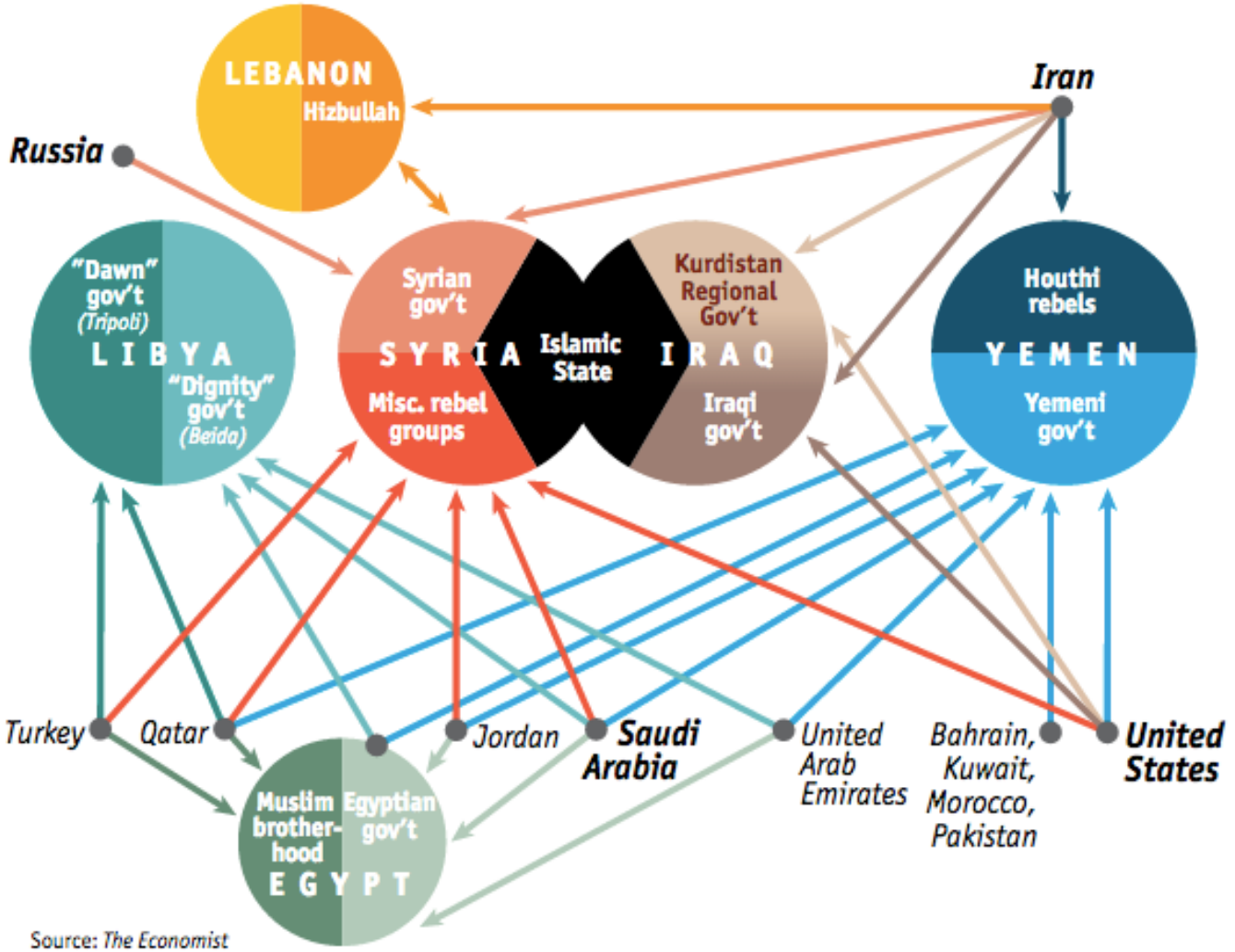
Dr. Christopher Ahlberg

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

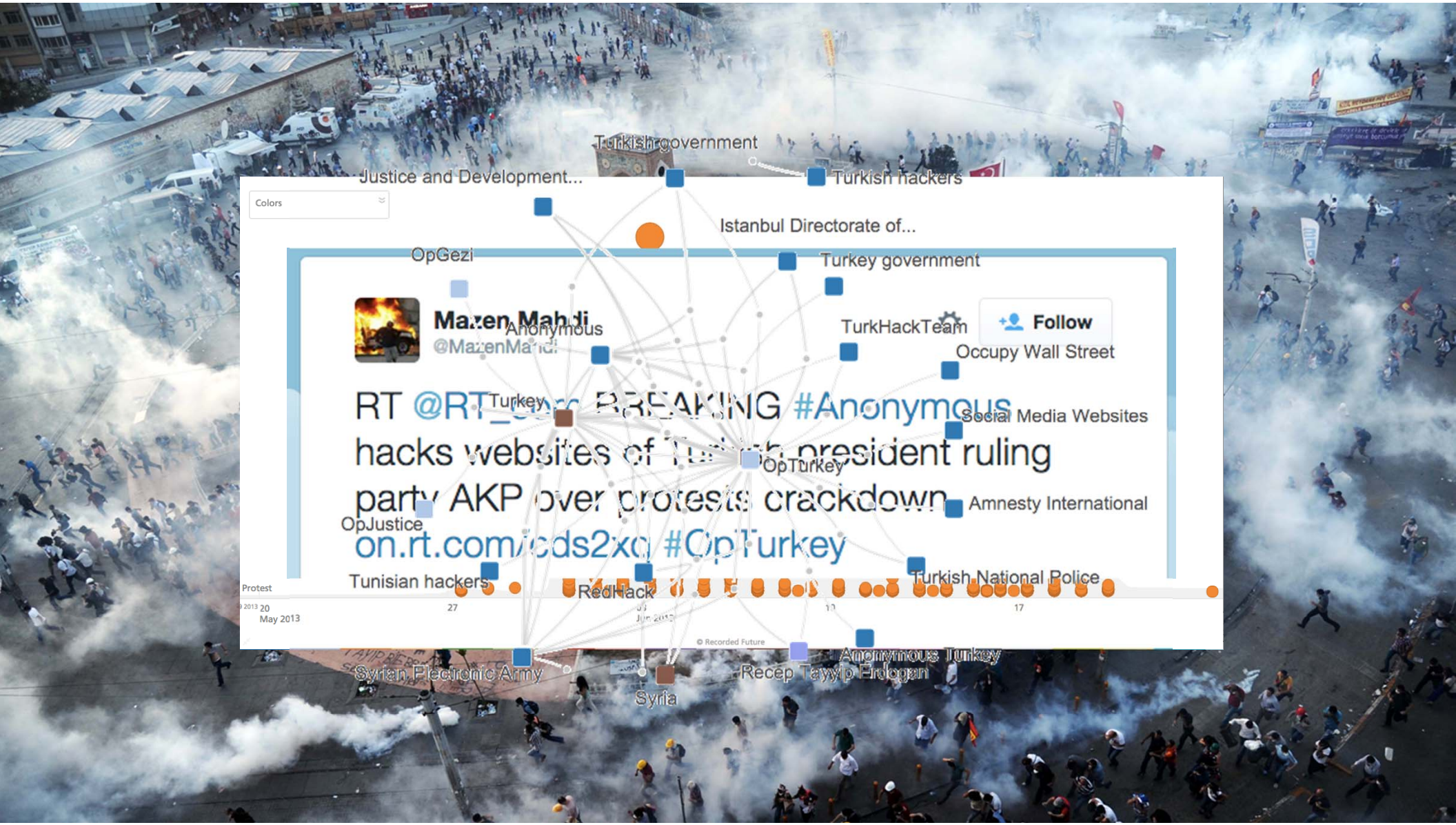
#RSAC

The main political rifts in the Middle East

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



Source: *The Economist*


Turkish government
Justice and Development...
Turkish hackers
Colors
Istanbul Directorate of...
OpGezi
Turkey government
Maxen Mahdi
@MaxenMahdi
Anonymous
TurkHackTeam
Follow
Occupy Wall Street
RT @RT_com BREAKING #Anonymous
Turkey
Social Media Websites
hacks websites of Turkish president ruling
party AKP over protests crackdown
OpTurkey
Amnesty International
OpJustice
on.rt.com/cds2xq #OpTurkey
Tunisian hackers
RedHack
Turkish National Police
Protest
20
May 2013
27
17
© Recorded Future
Anonymous Turkey
Syrian Electronic Army
Recep Tayyip Erdogan
Syria

Al Qassam Cyber Fighters (QCF)

July 2, 2012

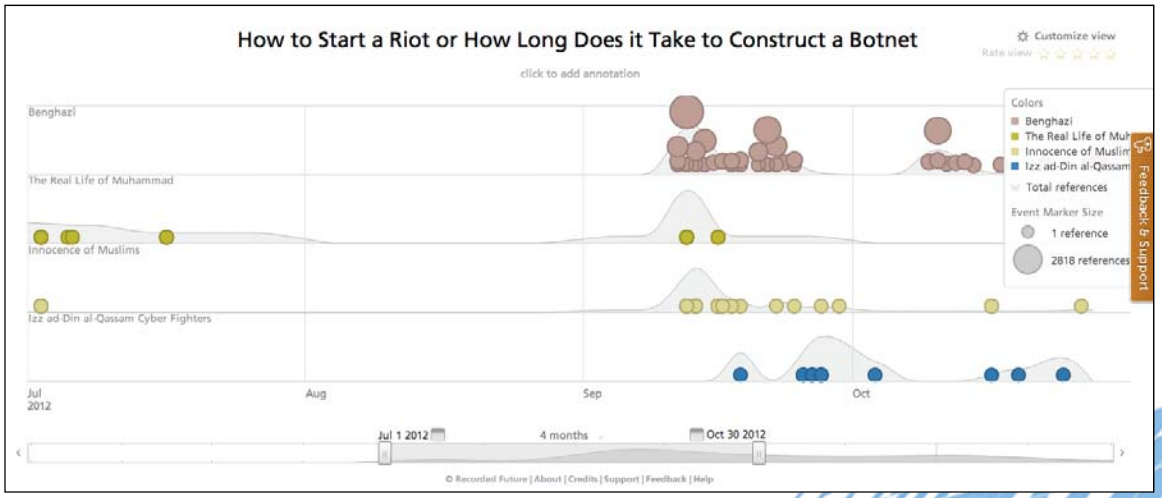
1. 'Innocence of Muslims' published on YouTube

September 11, 2012

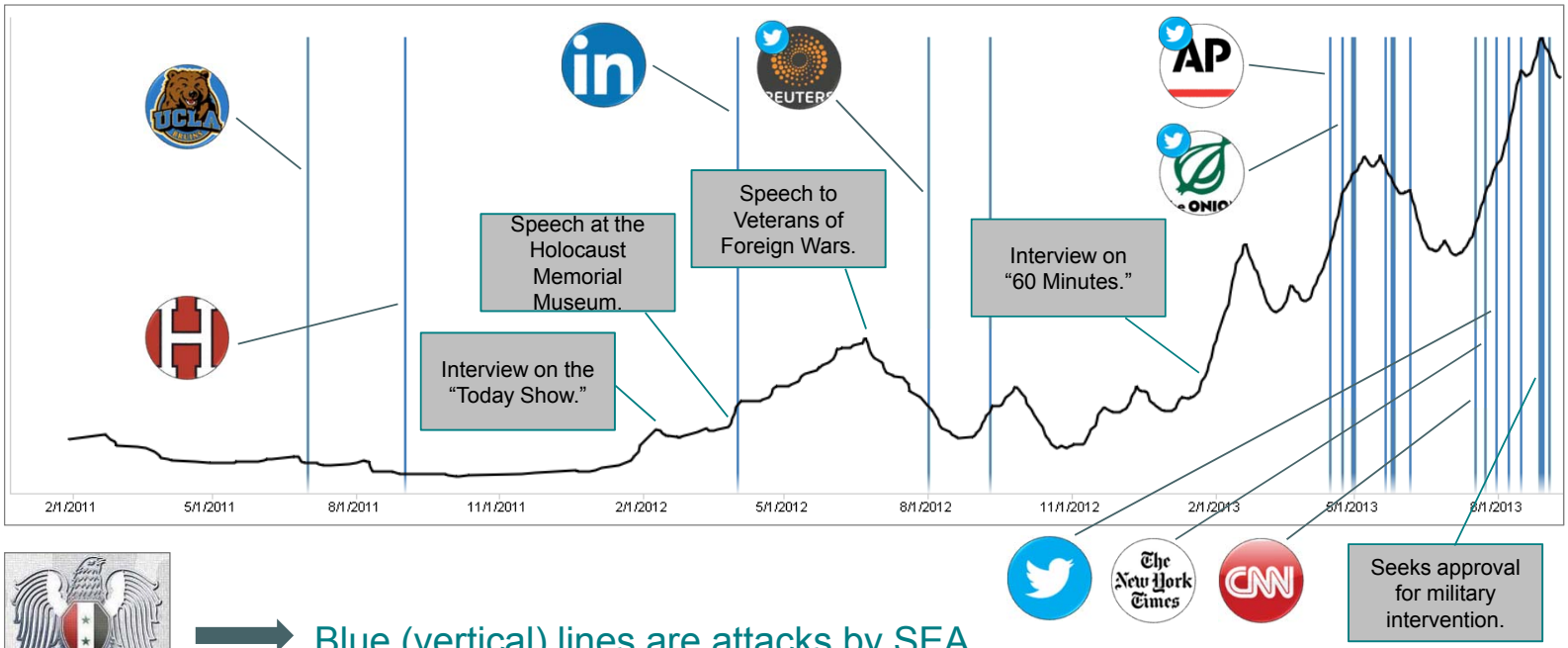
2. Reactions starts and spreads quickly

September 18, 2012

3. Al-Qassam Cyber Fighters starts Operation Ababil



Political Rhetoric Versus Cyber Attacks

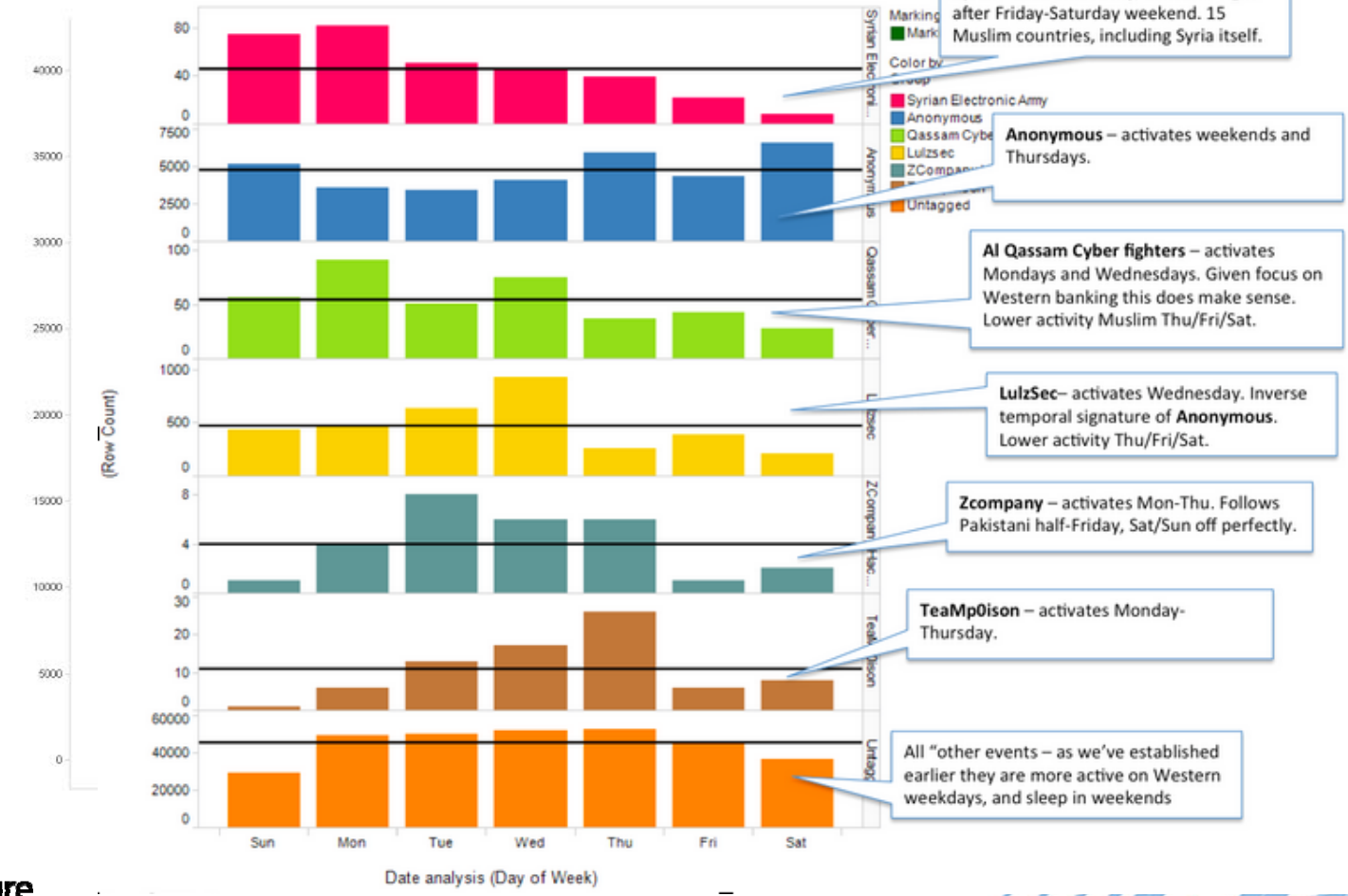


→ Blue (vertical) lines are attacks by SEA

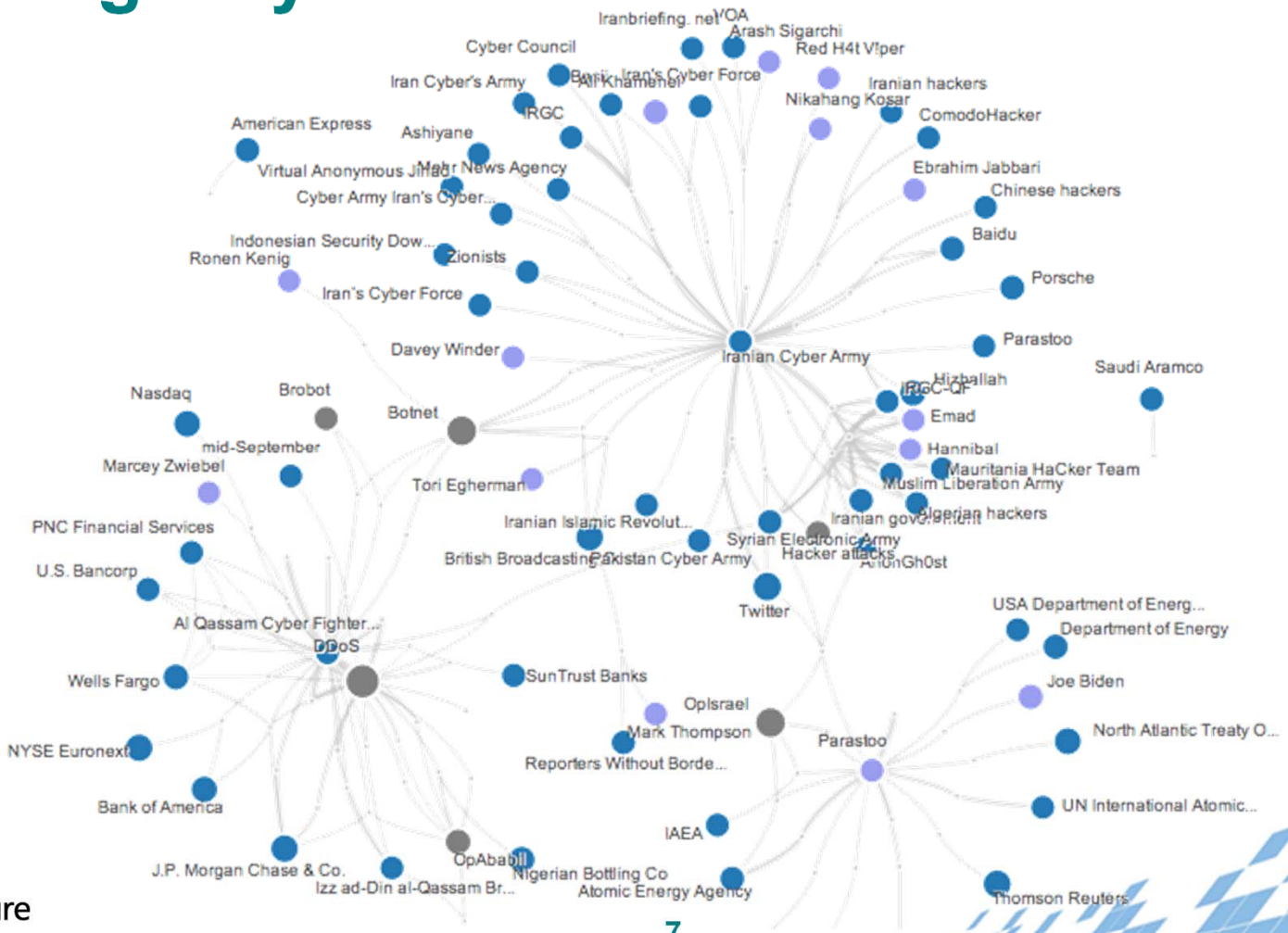
→ Black line is Barack Obama on Syria

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

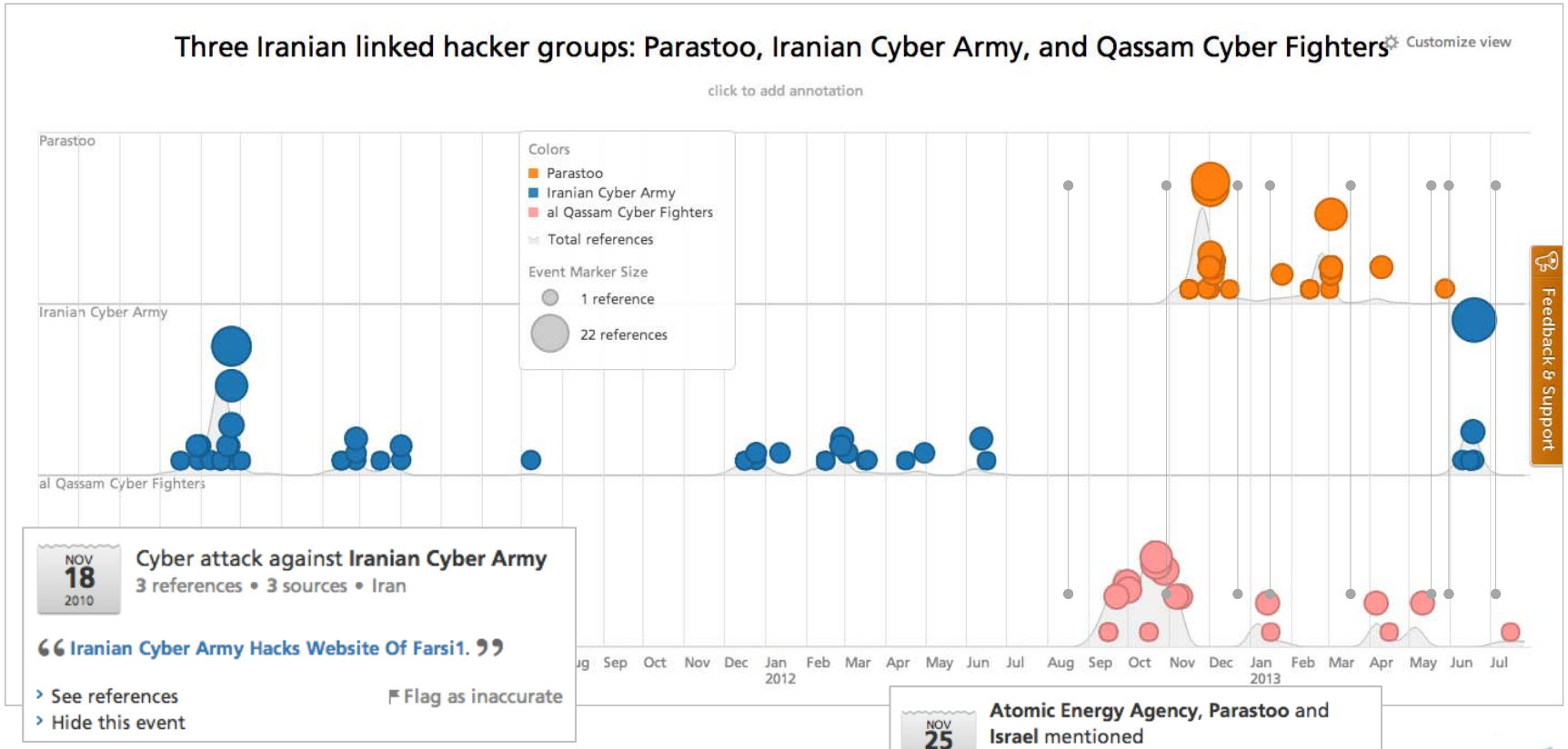
Behavior is Hard to Fake



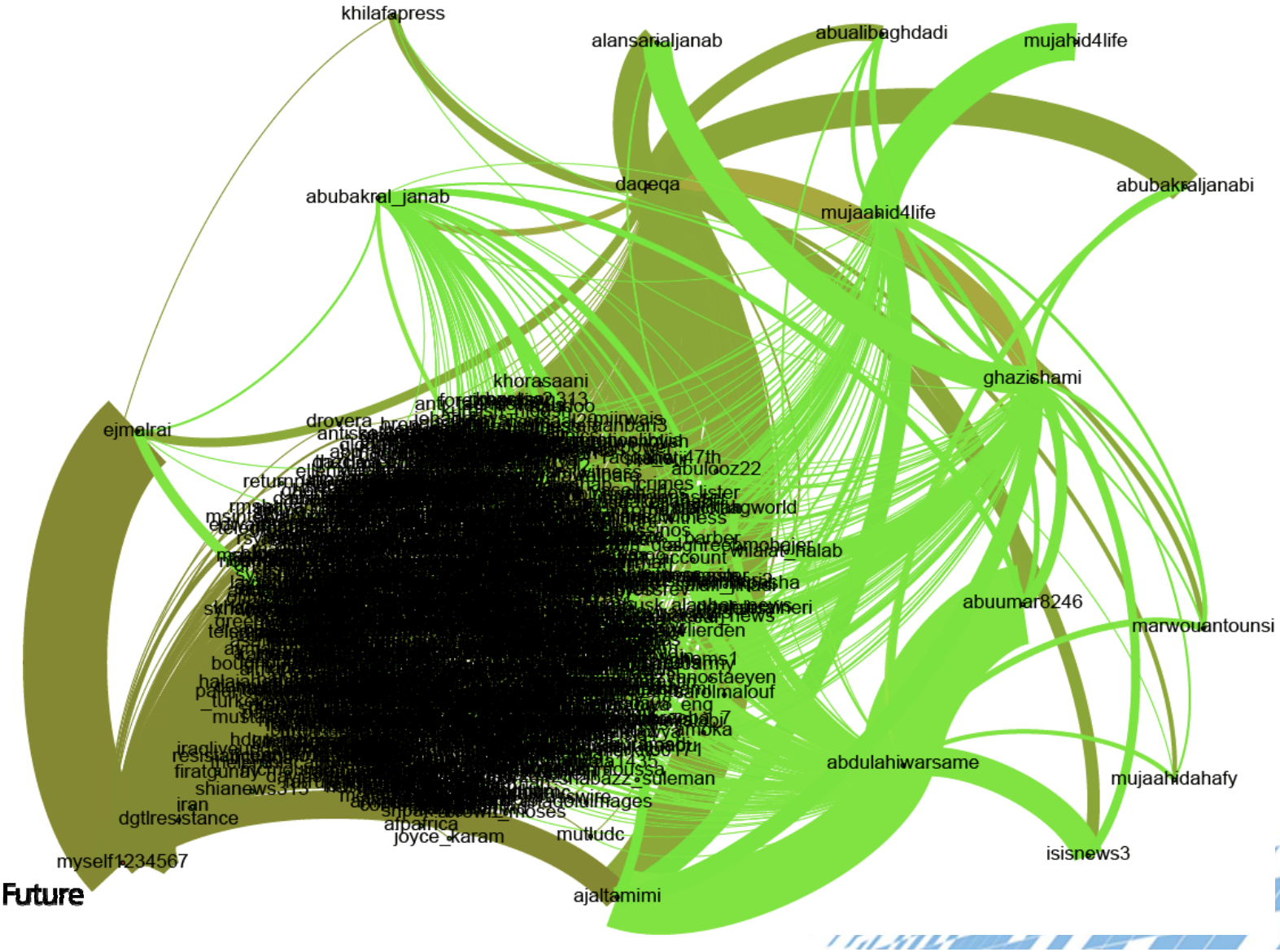
Targeting May Differ

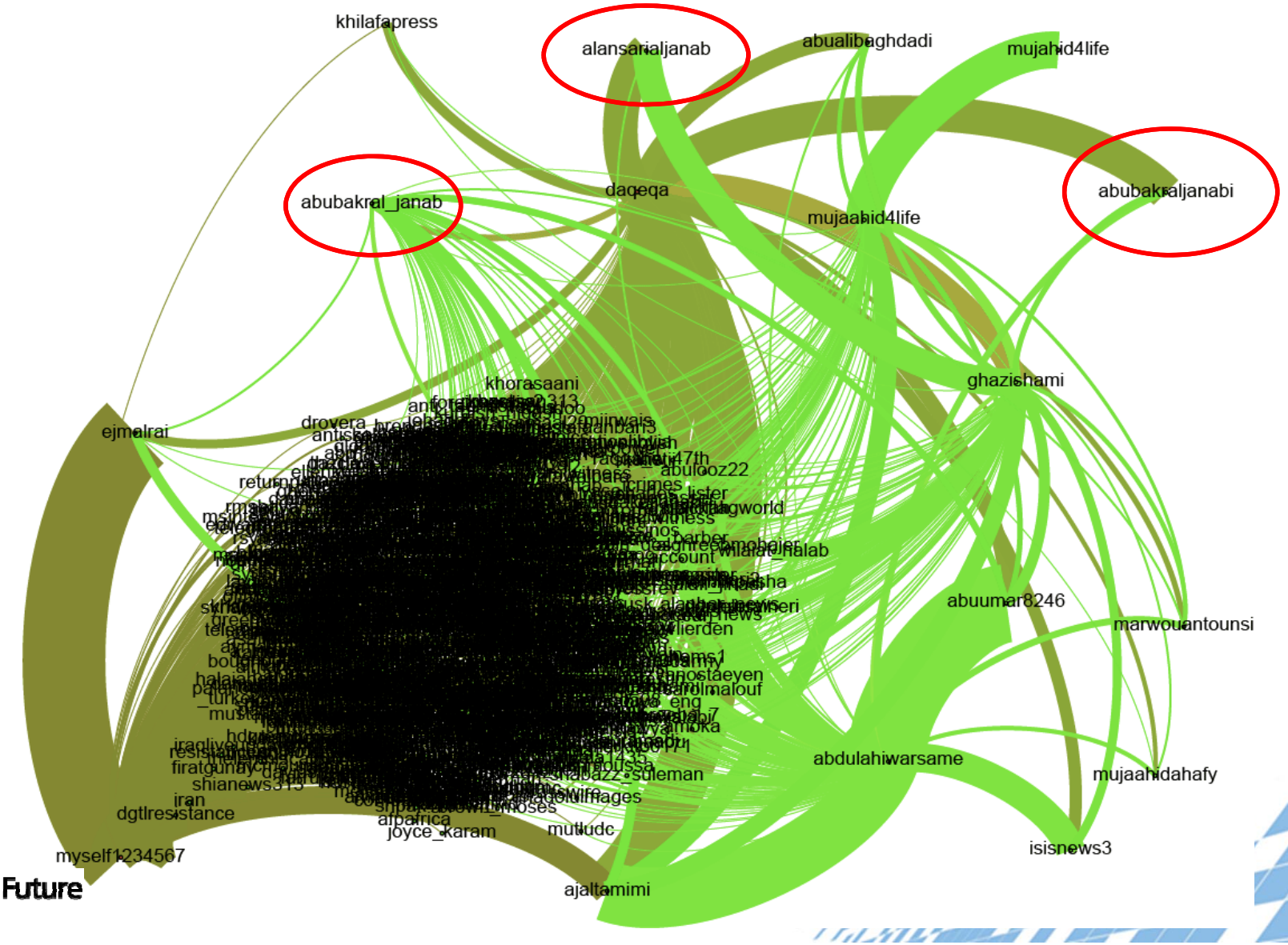


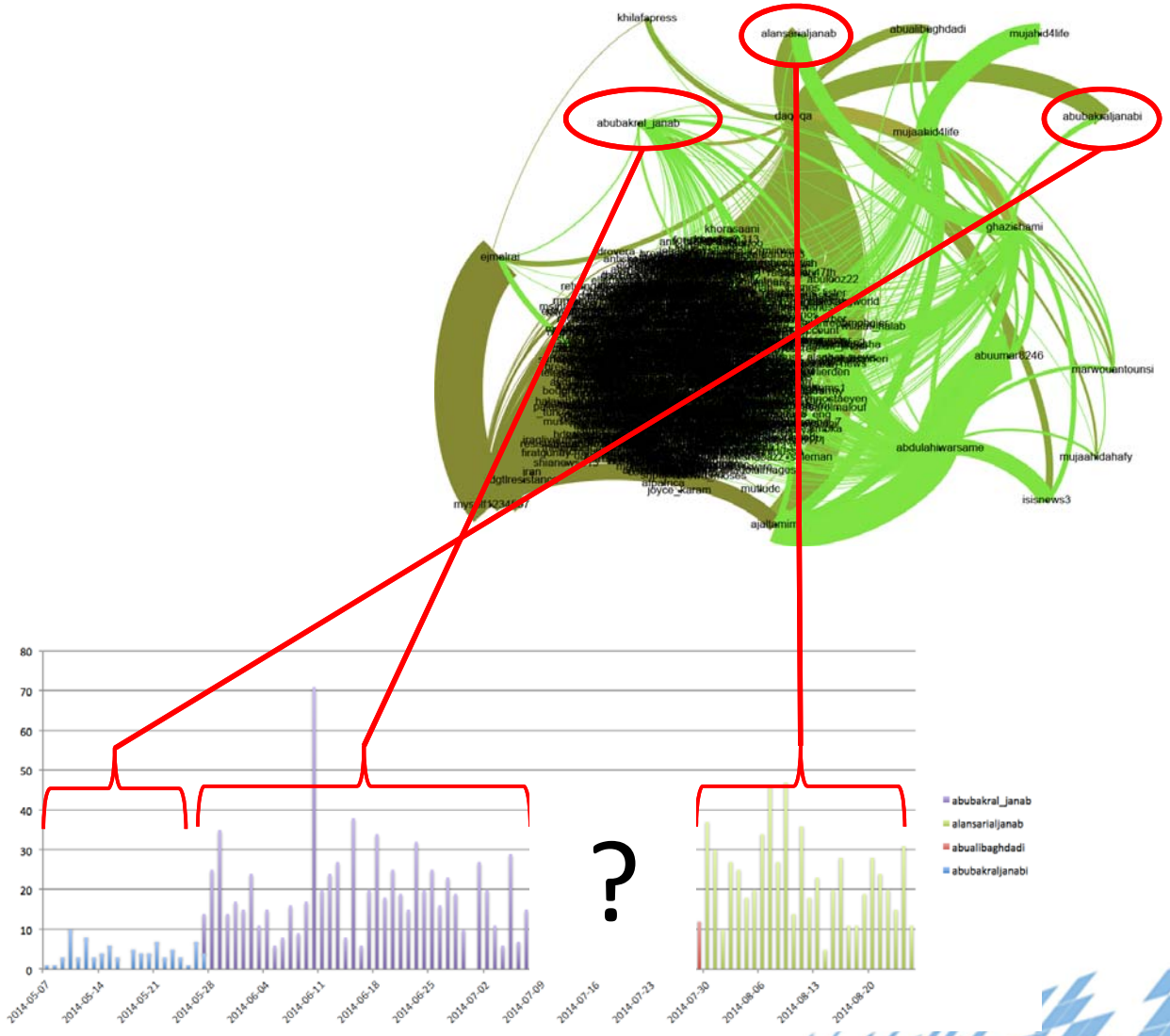
But Difficult to Escape from Time

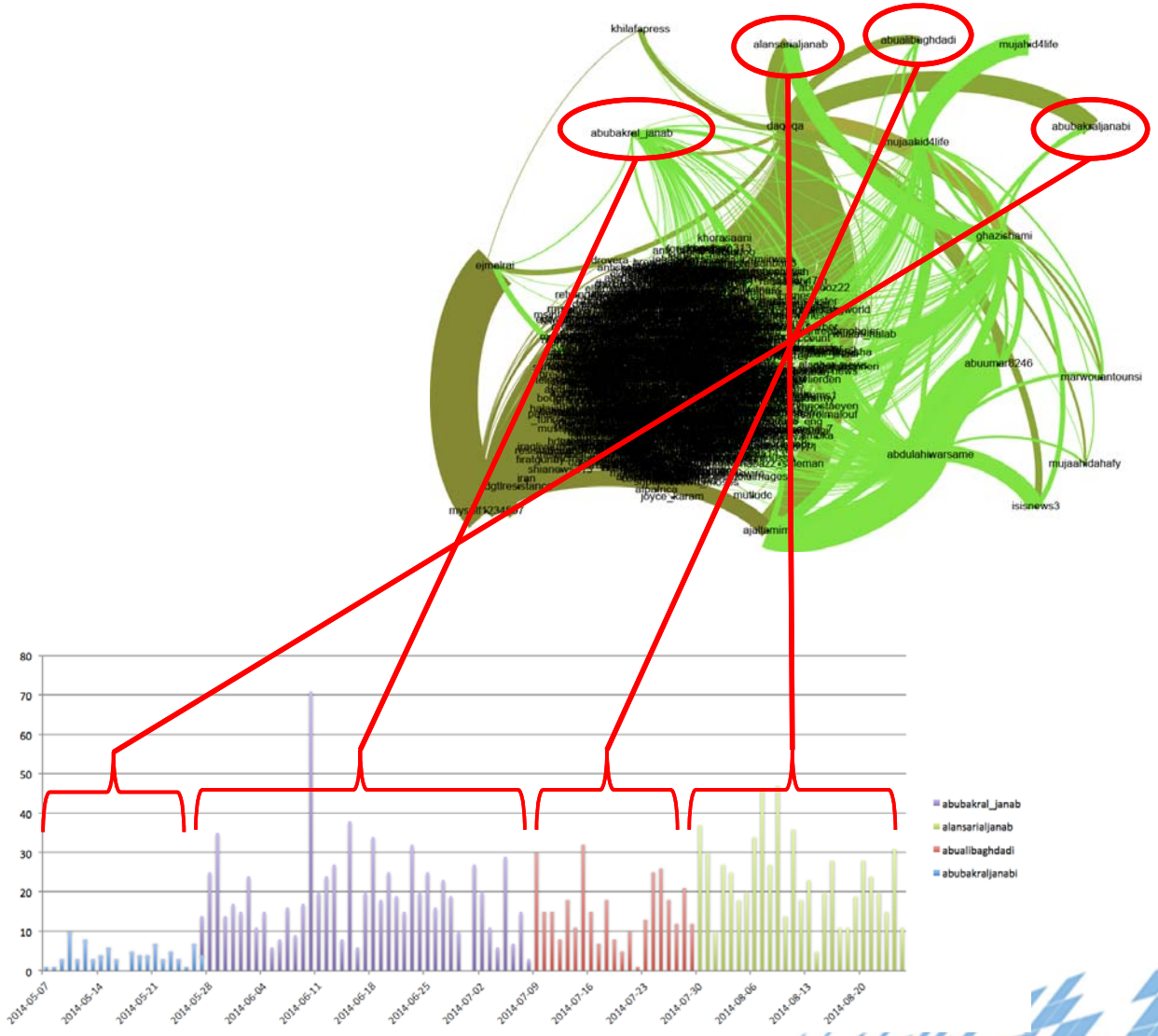


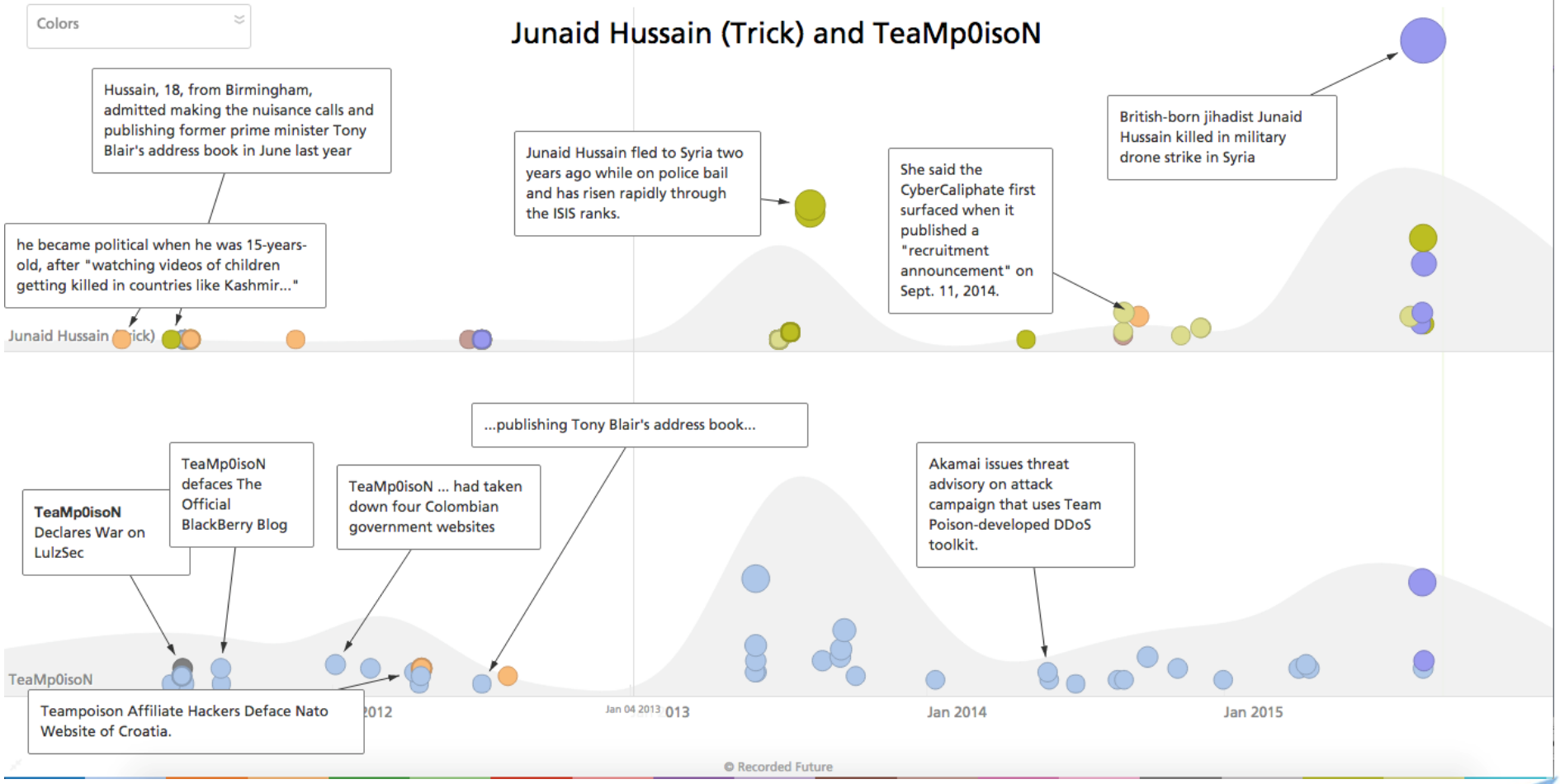

Ghazi
@abuaminah_
Follow
Takes me max 5 minutes to create a new account, email and follow 70% of old following list, and 1 day to get 500 followers. Try me.
Reply
Retweet
Favorite
More
RETWEETS
15
FAVORITES
19

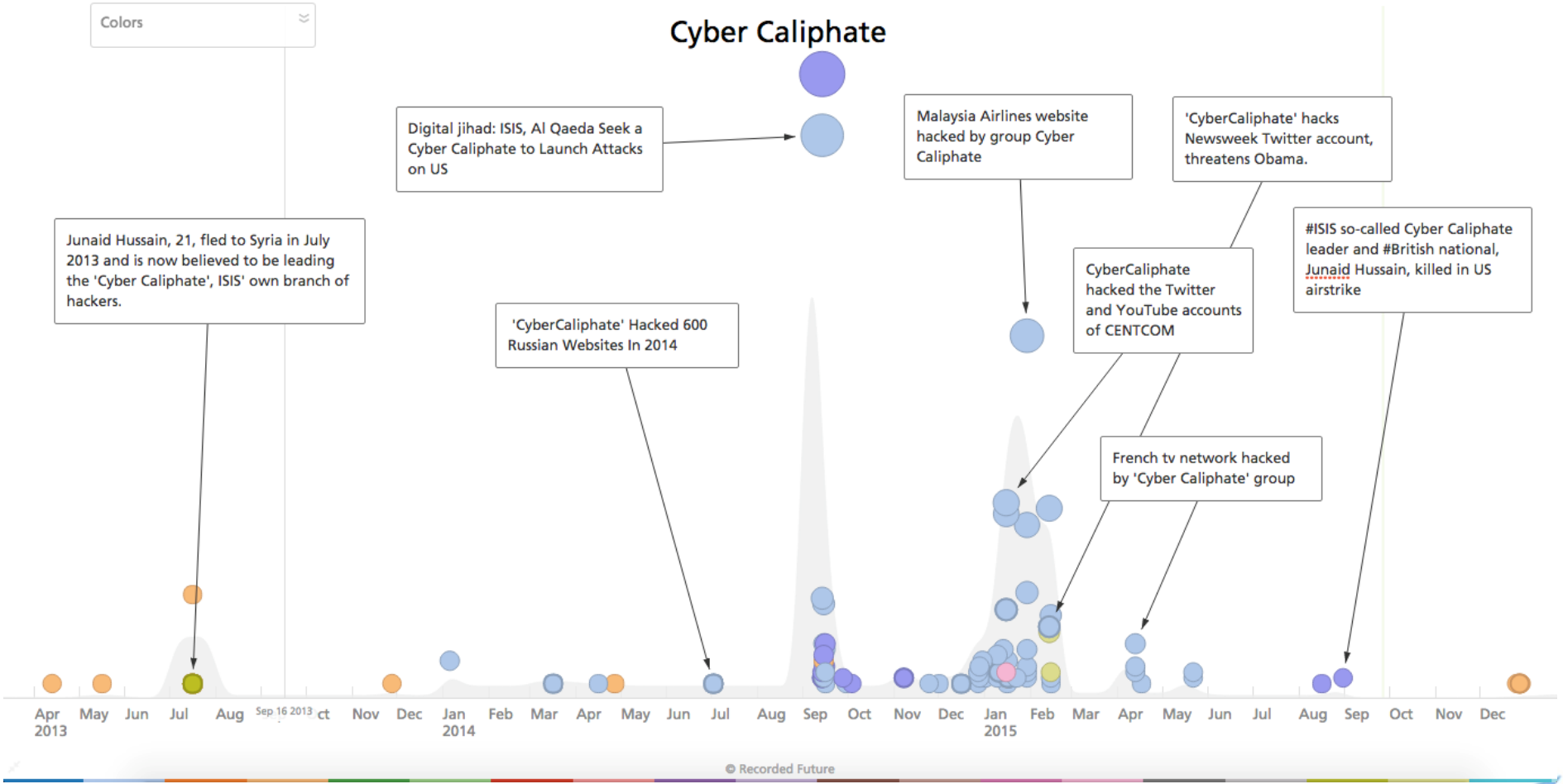

khilafapress
alansarialjanab
abualibaghdadi
mujahid4life
#RSAC
abubakral_janab
daqeqa
abubakraljanabi
mujaahid4life
khorasaani
ghazishami
ejmalrai
abuumar8246
marwouantounsi
abdulahiwarsame
mujaahidahafy
dgtlresistance
myself1234567
joyce_karam
isisnews3
ajaltamimi
Recorded Future
RSA Conference 2015
Abu Dhabi

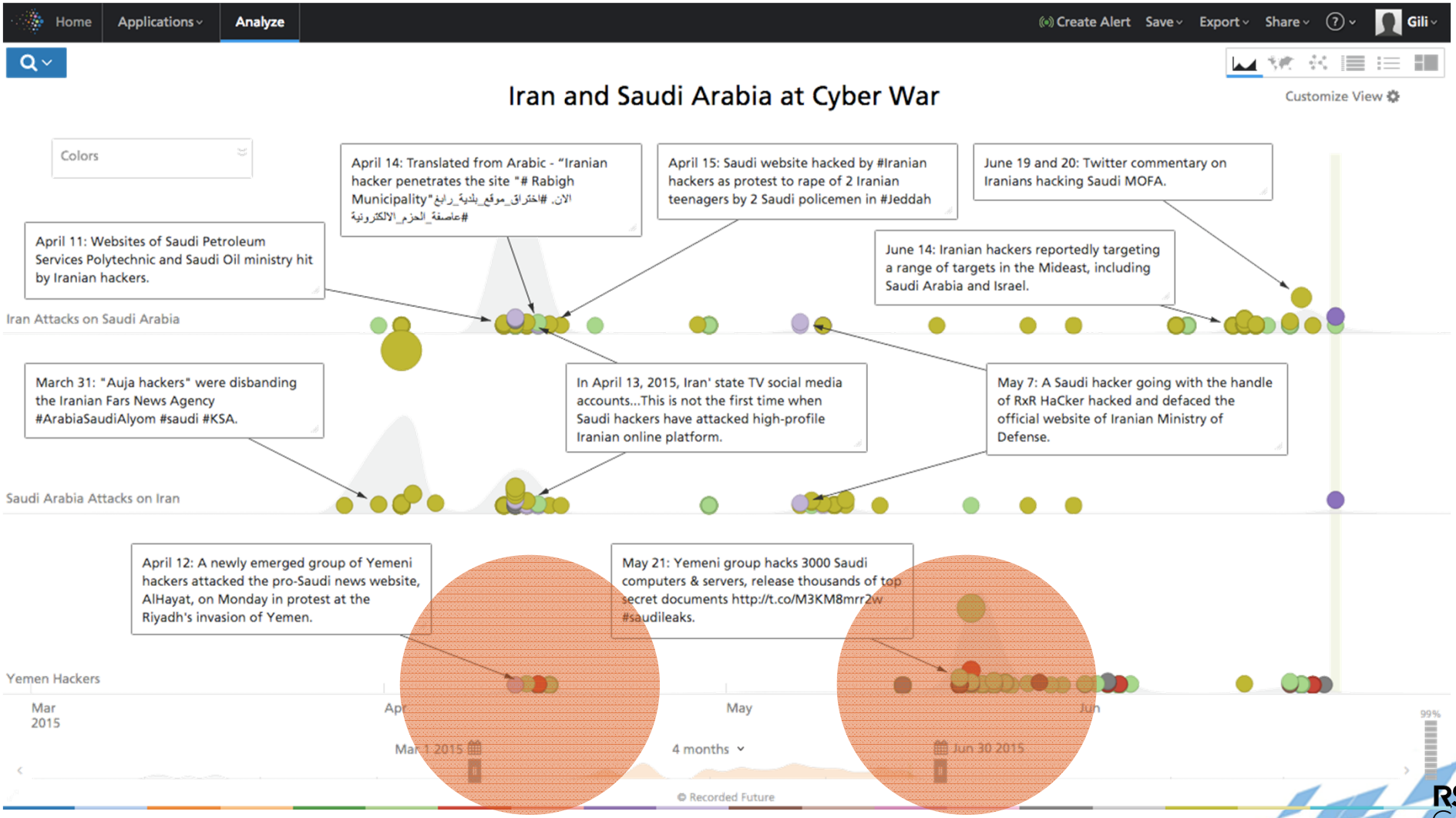

khilafapress
alansarialjanab
abualibaghdadi
mujahid4life
#RSAC
abubakral_janab
daqeqa
abubakraljanabi
mujaahid4life
khorasaani
ghazishami
ejmalrai
abuumar8246
marwouantounsi
abdulahiwarsame
mujaahidahafy
isisnews3
dgtlresistance
myself1234567
ajaltamimi
Recorded Future
RSA Conference 2015
Abu Dhabi


khilafapress
alansarialjanab
abualibaghdadi
mujahid4life
abubakral_janab
abubakraljanabi
mujaahid4life
ghazishami
abuumar8246
marwouantounsi
abdulahiwarsame
mujaahidahafy
isisnews3
joyce_karam
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

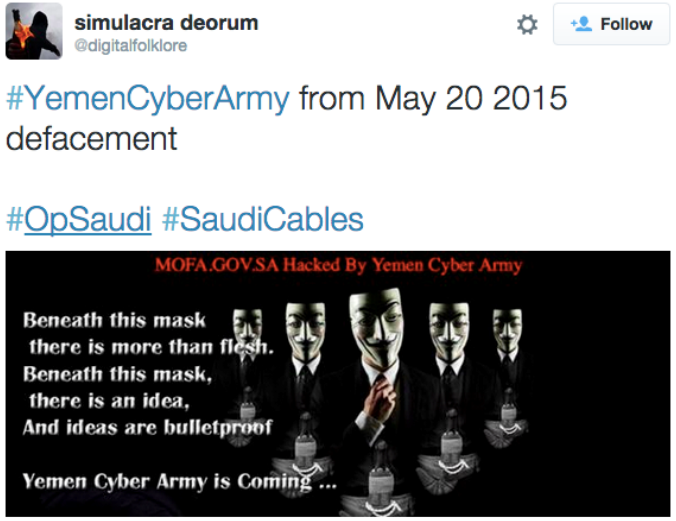

khilafapress
alansarialjanab
abualibaghdadi
mujahid4life
abubakral_janab
abubakraljanabi
mujaahid4life
ghazishami
abuumar8246
marwouantounsi
abdulahiwarsame
mujaahidahafy
isisnews3
ejmelrat
khorasaani
joyce_karam
abubakral_janab
alansarialjanab
abualibaghdadi
abubakraljanabi

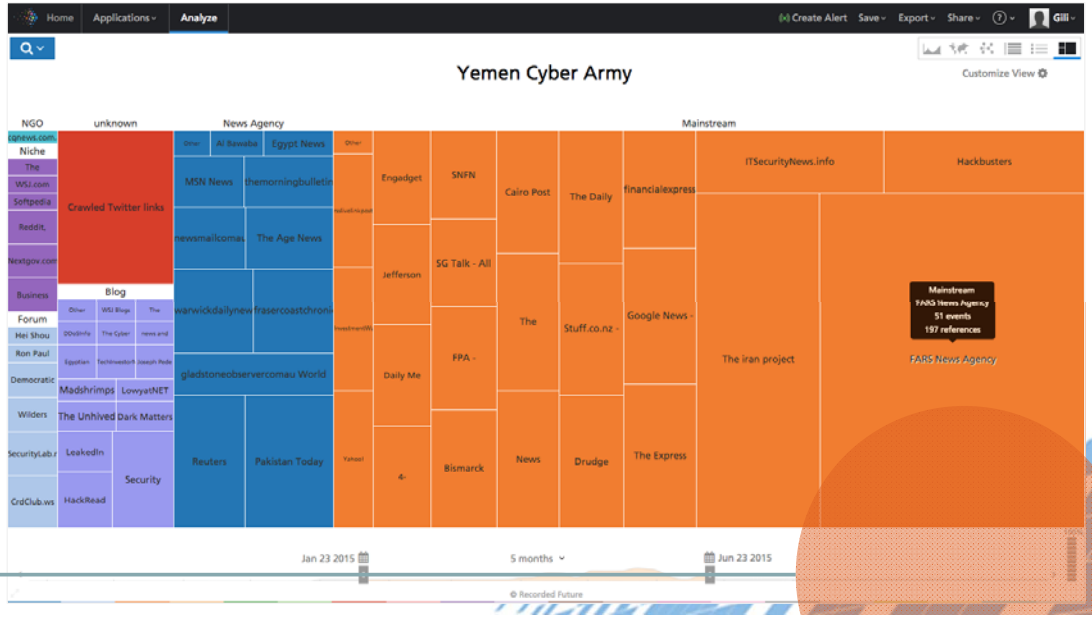

Colors
Junaid Hussain (Trick) and TeaMp0isoN
Hussain, 18, from Birmingham, admitted making the nuisance calls and publishing former prime minister Tony Blair's address book in June last year
he became political when he was 15-years-old, after "watching videos of children getting killed in countries like 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.
Jan 2014
Jan 2015
© Recorded Future


Colors
Cyber Caliphate
Digital jihad: ISIS, Al Qaeda Seek a Cyber Caliphate to Launch Attacks on US
Malaysia Airlines website hacked by group Cyber Caliphate
'CyberCaliphate' hacks Newsweek Twitter account, threatens Obama.
Junaid Hussain, 21, fled to Syria in July 2013 and is now believed to be leading the 'Cyber Caliphate', ISIS' own branch of hackers.
CyberCaliphate hacked the Twitter and YouTube accounts of CENTCOM
#ISIS so-called Cyber Caliphate leader and #British national, Junaid Hussain, killed in US airstrike
'CyberCaliphate' Hacked 600 Russian Websites In 2014
French tv network hacked by 'Cyber Caliphate' group
Apr 2013
May
Jun
Jul
Aug
Sep 16 2013
Nov
Dec
Jan 2014
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan 2015
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
© Recorded Future


Home
Applications
Analyze
Create Alert
Save
Export
Share
Gili
Iran and Saudi Arabia at Cyber War
Customize View
Colors
April 14: Translated from Arabic - "Iranian hacker penetrates the site "# Rabigh Municipality"#اختراق_موقع_بلدية_رابغ الان. #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.
Iran Attacks on Saudi Arabia
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.
Saudi Arabia Attacks on Iran
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.
Yemen Hackers
Mar 2015
May
Jun
99%
Mar 1 2015
4 months
Jun 30 2015
© Recorded Future

```
97. ##########################################################################
98. ##########################################################################
99. ##########################################################################
100.                    WE WILL PUBLISH COMPLETE DATABASES AND DOCUMENTS IN FUTURE.
101.                    FOR NOW WE SHOW YOU A LITTLE DEMO
102. ##########################################################################
103. ##########################################################################
104. ##########################################################################
105.
106.
107. Your Network Hacked By Yemen Cyber Army
108. We Are Cutting Sword of Justice
109. All Your Data is Encrypted and You Can't Access Them without Key
110. Find Out the Decryption Key This Way :
111. Number of Yemeni Children Killed in Saudi Air Attacks   +
112. Number of Yemeni Homes Destroyed By Saudi-USA Bombs   -
113. Number of Saudis Killed By Yemenis   -
114. Number of Israeli Soldiers Killed by Saudi and Arab Union in 1984!!!!
115.
116. #OPSAUDI
117. #YEMEN_UNDER_ATTACK
118. #OPKSA
```





Recorded Future

#RSAC

RSA Conference 2015 Abu Dhabi

Cutting Sword of Justice

```
97. ##############################################################################
98. ##############################################################################
99. ##############################################################################
100.                WE WILL PUBLISH COMPLETE DATABASES AND DOCUMENTS IN FUTURE.
101.                FOR NOW WE SHOW YOU A LITTLE DEMO
102. ##############################################################################
103. ##############################################################################
104. ##############################################################################
105.
106.
107. Your Network Hacked By Yemen Cyber Army
108. We Are Cutting Sword of Justice
109. All Your Data is Encrypted and You Can't Access Them without Key
110. Find Out the Decryption Key This Way :
111. Number of Yemeni Children Killed in Saudi Air Attacks   +
112. Number of Yemeni Homes Destroyed By Saudi-USA Bombs    -
113. Number of Saudis Killed By Yemenis    -
114. Number of Israeli Soldiers Killed by Saudi and Arab Union in 1984!!!!
115.
116. #OPSAUDI
117. #YEMEN_UNDER_ATTACK
118. #OPKSA
```

1. 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.
2. 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.
3. 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.
4. 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.
5.
6. Cutting Sword of Justice

وزارة الخارجية
المملكة العربية السعودية
MINISTRY OF FOREIGN AFFAIRS

Yemeni cyber capability?
QuickLeak.ir
No social media profile
Fars News

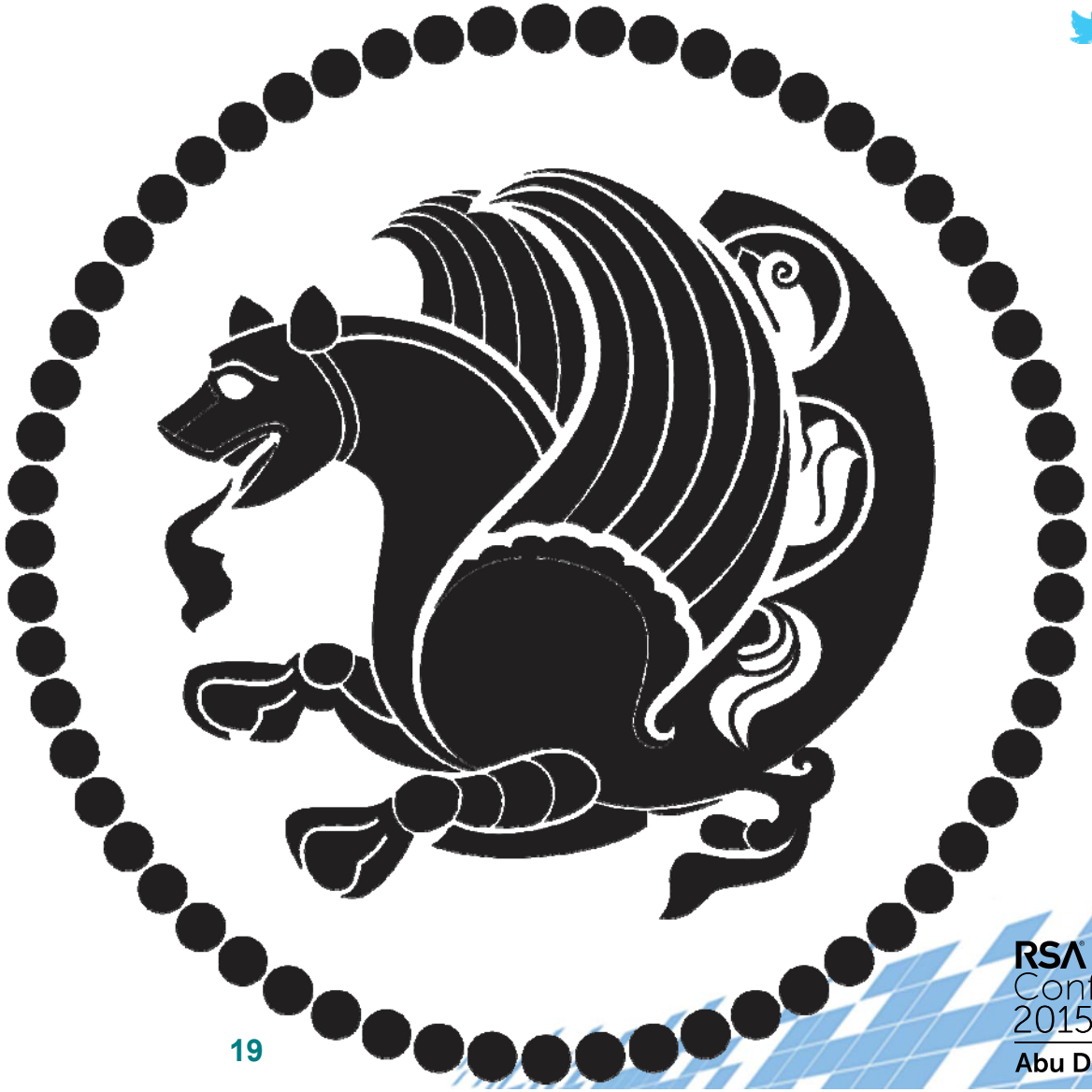
Recorded Future

ارامكو السعودية
Saudi Aramco

RSA Conference 2015
Abu Dhabi

Parastoo

Cutting
Sword of Justice



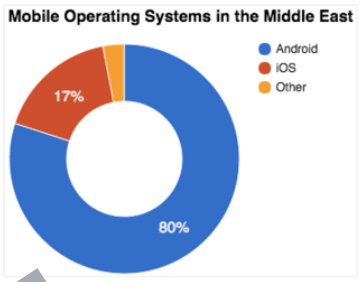
Lessons for the Defender

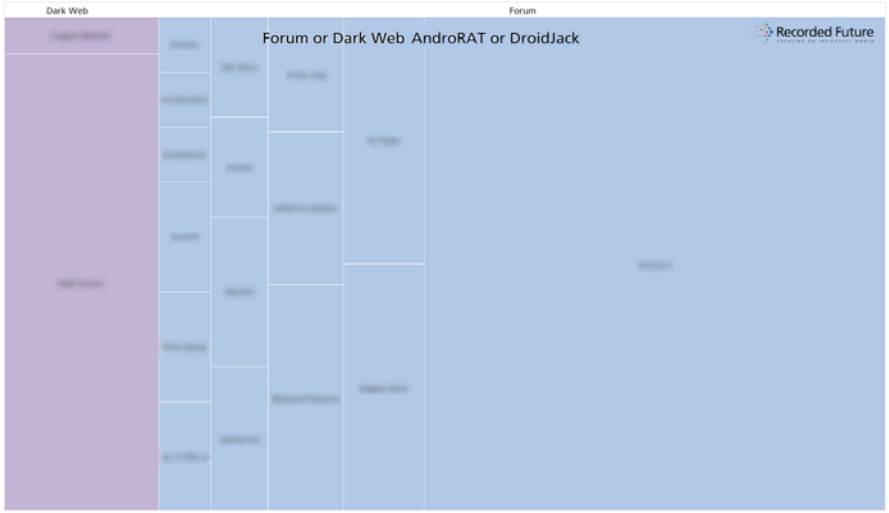
- Track geopolitical backdrop
- Know your threat
- Adjust defenses to actors
- Identify technical capabilities and indicators for actors
- Track and monitor actor behavior, key sources, and events driving them

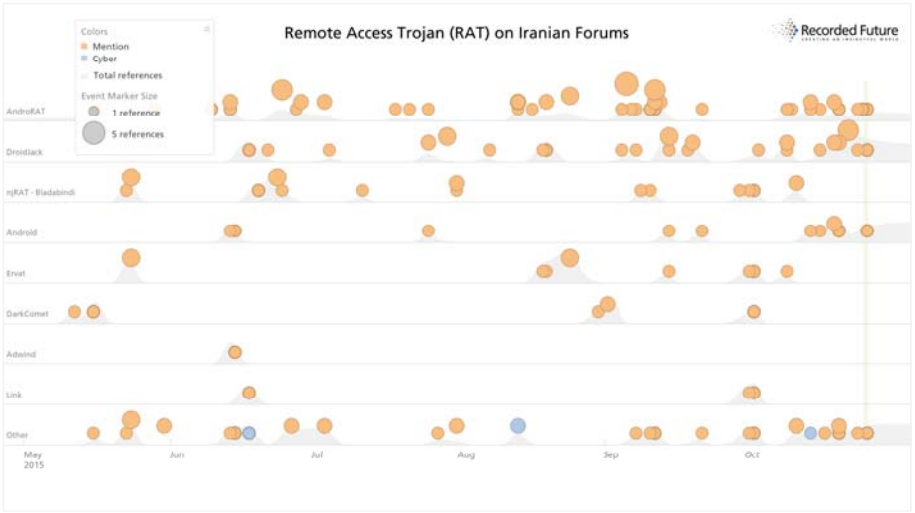
Defenders Matrix

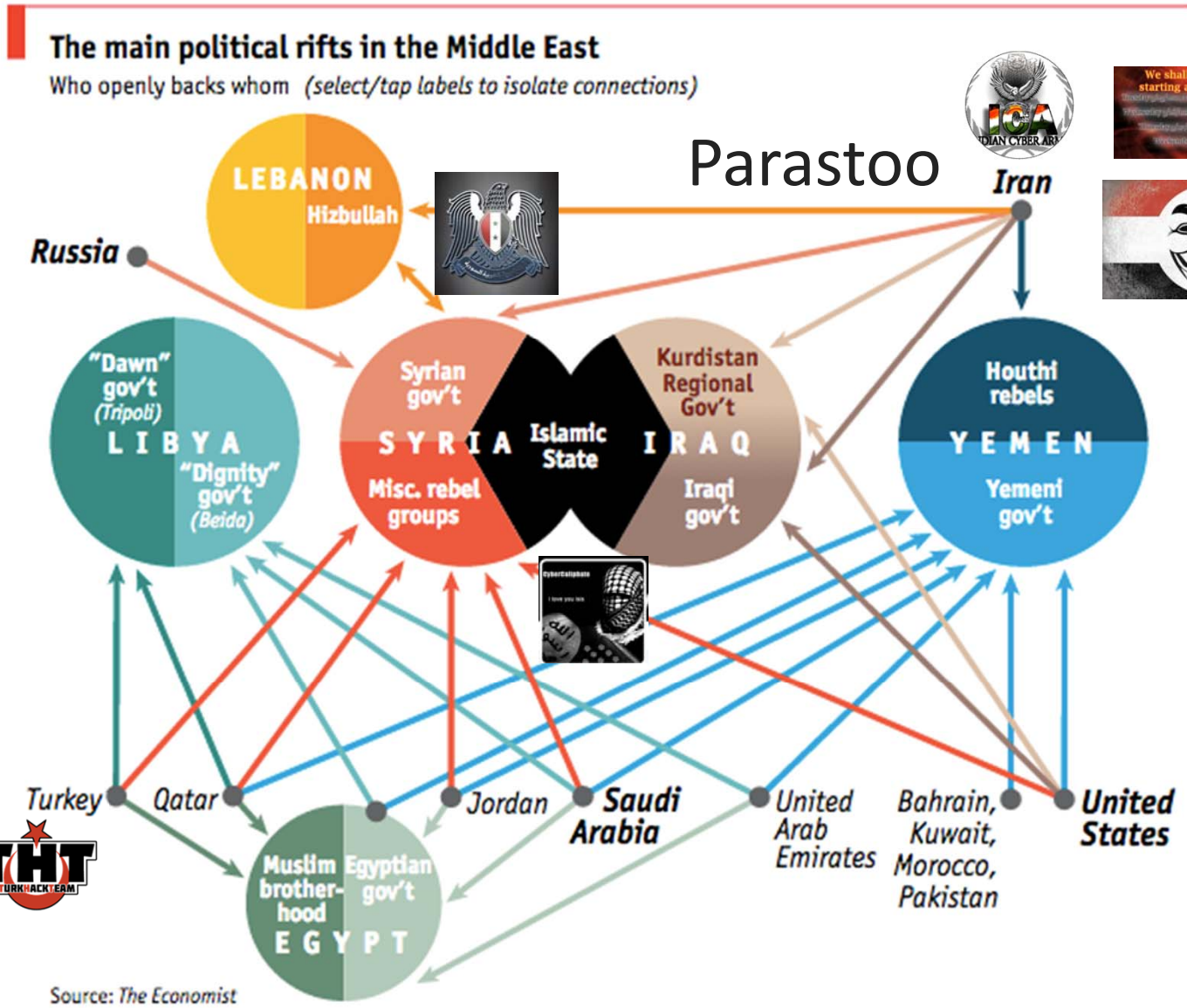
	Qassam Cyber Fighters	Iranian Cyber Army	Parastoo	Cutting Sword of Justice	Yemen Cyber Army	Cyber Caliphate	Syrian Electronic Army
Targeting	US+UK Banks	Domestic Iran, China, Azerbaijan, VOA Farsi	IAEA, US gov, Saudi, Israel	Saudi	Saudi Government	US DoD US Media Random websites	Western Media Companies
Media outlet	hilf-ol-fozoul.blogspot.com		Cryptome		Fars News Agency Wikileaks		
Social media outlet	None	None	None	None	None	Twitter	Twitter Facebook
TTPs	DDoS / Brobot	Web defacing	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	Pastebin	Quickeaks Pastebin	JustPaste.it	sea.sy archive.is

Operationalizing Intelligence








The main political rifts in the Middle East
Who openly backs whom (select/tap labels to isolate connections)
Parastoo
LEBANON
Hizbullah
Russia
Iran
"Dawn" gov't (Tripoli)
LIBYA
"Dignity" gov't (Beida)
Syrian gov't
SYRIA
Islamic State
Misc. rebel groups
Kurdistan Regional Gov't
IRAQ
Iraqi gov't
Houthi rebels
YEMEN
Yemeni gov't
Turkey
Qatar
Jordan
Saudi Arabia
United Arab Emirates
Bahrain, Kuwait, Morocco, Pakistan
United States
Muslim brother-hood
Egyptian gov't
EGYPT
Source: The Economist

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!