Eli Rohn
Department of Information Systems Engineering
Ben-Gurion University of the Negev, Beersheba, Israel

Connie M. White
Department of Information Technology
University of Southern Mississippi, Hattiesburg, MS, USA

Valeri's Knights and Prophecies

Have they been fulfilled?

Valeri's Knights and Prophecies

- Valeri and Knights
- Research Question
- Methodology
- Data
- Analysis & Discussion
- Conclusions and future work

Valeri and Knights

- Without the benefit of hindsight, Valeri and Knights (2000) made several predictions on how the Internet may be used for carrying out offensive information warfare (OIW).

OIW definition

- Offensive Information Warfare (OIW) is
  - "the set of activities carried out by individuals and/or groups with specific

    political and strategic **objectives** aimed at the

    integrity, availability and **confidentiality** of

  data collected, stored and transferred inside
  information systems connected to the Internet."

Main Assertions

- OIW will **NOT** be used by terrorists and their supporters to attack INFRASTRUCTURE because this will be very difficult.

- **OIW will be used to:**
  - Attack less protected social institutions (e.g., finance industry, government websites) to…
  - Demoralize the population at large, inflict fear of major financial and physical damages,
    - instill doubt in the ability of the government to protect
    - instill doubt in the ability of the economy to function

Main Assertions

- Let's rephrase it:

  Terrorists will favor manipulation and exploitation of data within information systems with the specific aim of **undermining the perception of trust among general users** over a cyber-attack on critical infrastructure.

The Research Question

- Have some (or all) aforementioned predictions been fulfilled?
  - If so, how?
  - If not, why (were they wrong? World not ready yet?)

Methodoloogy

Methodology

- Used data related to two recent regional conflicts
- Specific activist and terrorist groups were chosen based on their size and exposure in these two conflicts

Methodology

- Qualitative Analysis was used and a non-exhaustive search for manipulated photos was conducted.
- Data was collected by filtering out key terms using Twitter during and after the event over a two-week period.
  - For pictures, we searched various numbers and sets of hashtags using Tweetdeck
  - We also searched the web using reputable search engines and harnessed the snowball effect where one piece of information lead to another

Methodology

- For data related to cyber-attacks we tracked Twitter announcements and several media websites.

  - The collective known as **Anonymous** was the most vocal, thus getting attention not only from researchers, but from the media as well.

Data

Where we found the data

- Two 2012 conflicts in the Middle East provide abundance of data relating to OIW.
- Almost a well controlled two group experiment setup

The Two Groups "Experiment"

Target Group 1	Target Group 2
Low reliance on Web for e-finance / e-Gov	High reliance on Web for e-finance / e-Gov
High central control over infrastructure	Low central control over infrastructure
Was attacked by various groups	Was attacked by various groups
Propaganda attacks	Propaganda attacks
Cyber attacks	Cyber attacks

Where do you find them?!?

Finding target groups

Who are the target groups?
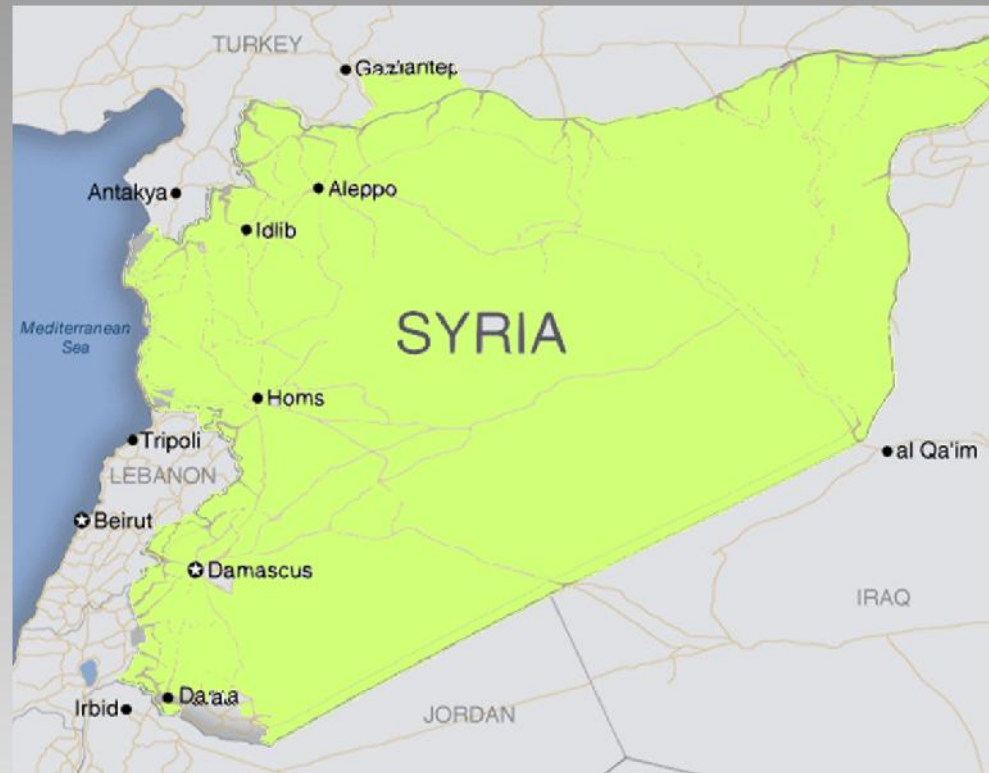
Who are the target groups?

OIW Activities

Syria / Rebels

- 2012 conflict between various rebels and the Assad regime

- Rebels use social media:
  - To belittle, mock or vilify Syria's military and regime
  - self-encouragement and support of other rebel factions

Israel / Hamas

- 11/2012 Operation Pillar of Defense – clash between Gaza's Hamas and Israel

- Hamas use social media to:
  - Belittle, mock & vilify Israel
  - Plea their alleged suffering to Western governments and NGOs

OIW Activities

Syria / Rebels

- Rebels disseminate video clips and pictures of alleged Assad atrocities.
- Anonymous launches an attack against Syrian's Internet
- Syria slows down, then shuts down Internet
- Syria shuts down cellular services for three days

Israel / Hamas

- Hamas uses Syrian pictures to claim Israel is committing war crimes (Propaganda)
- Anonymous launches an attack against Israeli institutions
- IDF uses Facebook and YouTube to post information (text & visuals) in English, Arabic and other languages
- Israeli institutions demonstrate their resilience against cyber attacks

OIW Examples – Syrian Rebels

- Syrian rebels' Omawi News presence on social media

- Syrian rebel's Ugarit on Facebook

OIW – Free Syrian Army

Syria - Free Syrian Army Front Line Clashes (December 2012)

by **Syria Baynetna** · 8 months ago · 14,180 views

HD

Syria - Free Syrian Army Heavy Clashes (December 2012)

by **Syria Baynetna** · 8 months ago · 46,370 views

The 2011--**2012 Syrian** uprising is an ongoing internal conflict in **Syria**, a part of the wider Arab Spring, that began in January ...

HD

1 week with the "free syrian army" - Feb 2012 - Arte reportage 2 of 2

by **sefraus** · 1 year ago · 28,473 views

http://www.youtube.com/watch?v=Q5qkeh4h_98&feature=plcp Suite aux vetos chinois et russe a l'ONU contre une resolution ...

4 7 2012 - Free Syrian Mujahid Army Attack

by **FreeSyrien0** · 1 year ago · 13,644 views

Assad is killing the **syrian** people, islam will bring justice, we will give every one his rights,

OIW – Free Syrian Army

OIW Examples - Hamas

- Syrian dead boy portrayed as a Palestinian killed by Israel

- Victim of Hamas portrayed as a killed by Israel

OIW examples - Hamas

- Israeli Injured Baby Portrayed by Hamas as Palestinian (with an Israeli response on the right)

- Same family died twice
  – On top – a cynical comment on FB by an Israeli

OIW - Anonymous

Presence

- Multiple Twitter Accounts
  - Leading 5 have over 2M followers
- YouTube clips
  - Hundreds, some with 2M views
- TOR (dark web) presence
- Facebook
  - Several pages

Activities

- 11/2012 launched cyber-attacks on Israeli institutions

- 11/2012 launched cyber-attacks on Syrian internet

OIW - Anonymous

Attacks against Israel

Anonymous @YourAnonNews

Dear Israel, you shut down internet. We'll shut you down.

14 Nov 12

Anonymous Press @AnonymousPress

#OpIsrael 40+ Israel'i government & military websites have been taken down inlast 3hrs #FreeGaza #Anonymous #FreePalestine V @anonnewsint

15 Nov 12

Anonymous leaks personal information of 5,000 Israeli officials
168

Anonymous hack hundreds of Israeli websites, delete Foreign Ministry database in support of Gaza 80

Attacks against Syria

Anonymous Declares War On Syrian Government Websites In Retaliation For Internet Blackout

The Huffington Post | By Meredith Bennett-Smith
Posted: 11/30/2012 12:31 pm EST Updated: 11/30/2012 2:44 pm EST

Anonymous @YourAnonNews

Government Of #Syria Cuts Country's Internet Access - #Anonymous Goes on the Warpath! securityweek.com/syrian-governm... #OpSyria #YAN

5:09 PM - 30 Nov 2012

149 RETWEETS 20 FAVORITES

Anonymous @YourAnonNews

Anonymous is attacking Assad due to the internet outage. Anonymous is not attacking Assad in support of the Free Syrian Army. #OpSyria

6:04 AM - 30 Nov 2012

290 RETWEETS 58 FAVORITES

Self-Inflicted OIW ?

According to CNET, Syrians on Twitter reported that phone lines also were down and that all 84 of Syria's IP address blocks have become unreachable, effectively removing the country from the Internet.

The Syrian government said that terrorists were behind the outages, but CloudFlare, a firm that helps accelerate Internet traffic, said it would have been extremely difficult for any type of sabotage to cause such a comprehensive blackout, according to Reuters.

Effects of OIW

Evaluation if some of the predictions made by Valeri and Knights have been fulfilled
Assessment if OIW had significant influence on attacked governments

Effects of OIW

OIW	Syria	Israel
Cyber Attack	No effect due to two main factors: Government's disinterest and little e-finance activity in Syria	No effect due to the resilience of the Israeli finance systems. Defacing of websites is seen as superficial damage
Propaganda	No effect due to government's disinterest in its public image abroad	Several key government decisions influenced by propaganda IDF creates a counter-propaganda unit

Prediction Accuracy

OIW	Prediction	Materialization	Accuracy
Cyber Attacks	Attacks on websites and information systems is preferred over attacks on infrastructure	Millions of daily attacks against Israeli web sites during 11/2012. Attacks against official Syrian websites	✔
Propaganda (images and videos)	Propaganda used to: [a] vilify the other side [b] boost morale	Hamas used a large number of pictures from the Syrian conflict and portrayed the victims as Gazans suffering from Israel's cruelty. Hamas used social networks to spread false claims, in Arabic, about its victories "against the Zionist enemy"	✔

Conclusions

And Future Work

Conclusions

- Valeri & Knight's predictions have materialized and have been shown to have been accurate

Future Work

- Reputable traditional media sources have demonstrated over time that they are not always trustworthy, as they promote, sometimes even voluntarily, OIW actions
  - This is an aspect we did not cover here and needs further research.

Future Work

- Further ramifications analysis towards the intended targets.
  - Once someone is aware that the information was propaganda, how would it make them feel towards the group who posted it?
  - Obviously, the group was posting the information to deface their enemy and to hope to gain sympathy from their external constituents. However, the opposite feeling or feelings of apprehensiveness and dishonesty may surface.

Future Work

- We intend to conduct research seeking answers to the following questions:
    - Did Israeli users will feel uneasy in engaging in e-commerce transactions?
    - Did they perceive threats to their financial assets and privacy due to the cyber-attacks?
    - Did the cyber-attack impair those elements that explain Internet's social and commercial successes?

Q & A

For additional information:

Read the published paper or

Contact
elirohn@bgu.ac.il or Connie.White@gmail.com