

# *Prospective Incidence of Terrorism on Cyber Security*

## *Threats & Countermeasures*

Rami Efrati – July 2018

Rami.Efrati @ gmail.com

# Israel - One of the Most Cyber-Attacked Countries

- Terror and Cyber-Terror
  - Are components of the national defense strategy
- Solutions on the national level
  - Israeli National Cyber Directorate
  - National & sectorial CSIRTs / ISACs
  - Cyber defense national educational programs
- Government directed incentives to the private sector
  - Funds via the Innovation Authority
  - Cyberspark in Be'er-Sheba



Prime Minister's Office  
National Cyber Directorate

**Quick, Focused & Coordinated Response To New Threats**

# Cyber-Terrorism – The Israeli Perspective

- Terrorism uses “Cyber” as yet another weapon
  - Cyber-terrorism must be treated as kinetic
  - Treat the physical aspects as well as digital
- Leveraging innovation to fight terrorism
  - New attack domain requires new approaches
  - Out of the box thinking
  - Disruptive solutions



US Central Command's  
Facebook page defacement by ISIS



Banner of ISIS cyber unit encouraging  
single-person attacks

Search Query



Summary Posts Media Interests Usage Topics Events Authors Sites Groups Graph

@100011409534130 -fac...

1000 Friends

☐ Labels ☒ Images  
☒ Closeness ☐ Cliques  
☐ Move

Search

Select All

- ☒ Alan Salifu (186)
- ☒ amir.cornar.3572846 (186)
- ☒ list.legio (186)
- ☒ tam.postjeri (151)
- ☒ andillah.arnauti (150)
- ☒ Arjend-Begolli (142)
- ☒ Enes1.A (148)
- ☒ abdul.barr.S (139)
- ☒ qemir.uderjoll.5 (136)
- ☒ Afron Enen (134)

Connection Degree

1

Zoom

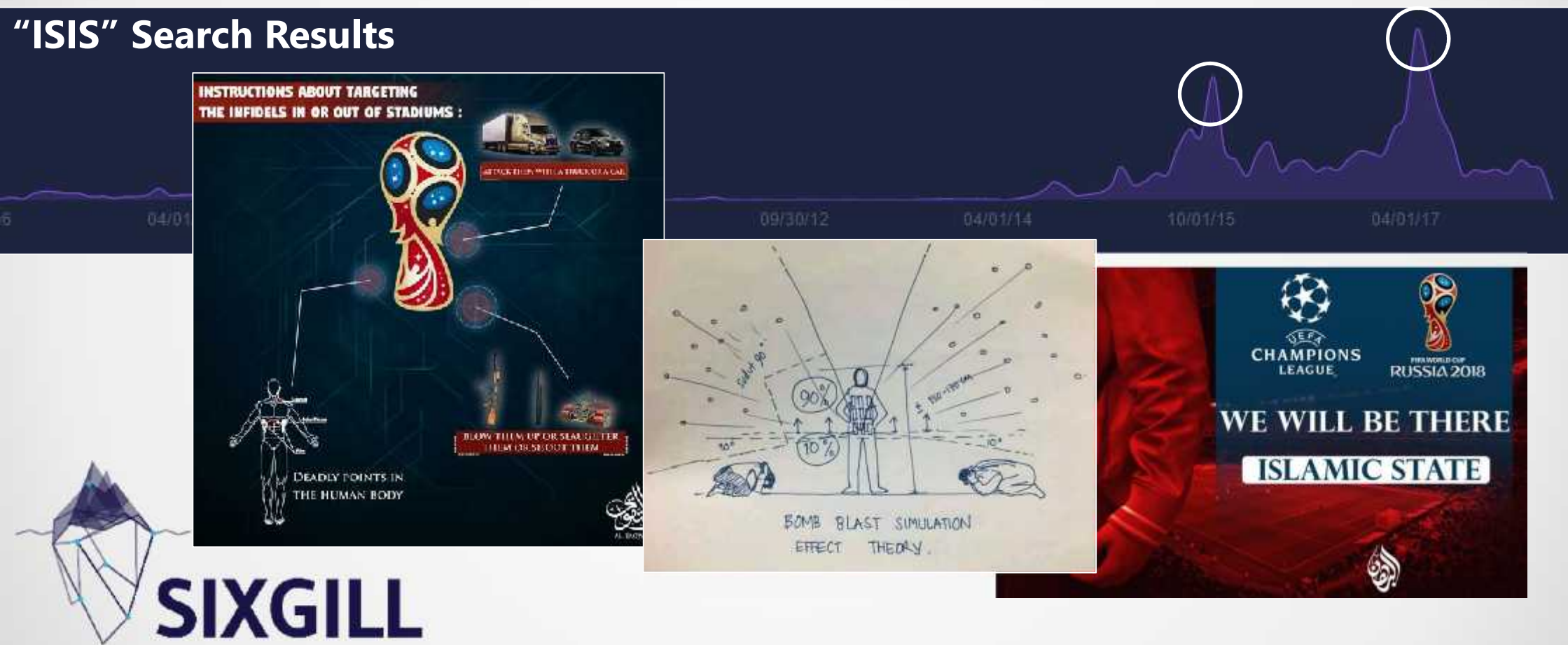


Nodes: 1000  
Links: 10811  
Cliques: 17  
Max: 8  
Min: 1



# ISIS Threat Monitoring

## "ISIS" Search Results



Confidential and Proprietary

# ISIS Threat Monitoring



*Confidential and Proprietary*

# ISIS Weaponized UAVs





# Cyber-Terrorism – Current Threats

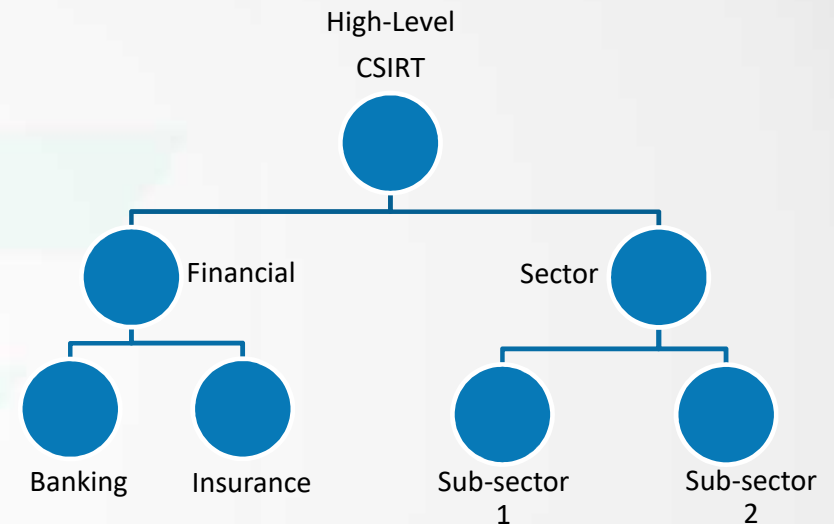
- Moving from attacking IT-systems to OT-systems
  - Human lives
  - Environmental implications
- Weaponization of cyber
  - Based on published vulnerabilities
- Lowering of technological barriers
  - Technologies & hackers for hire

## Cyber-Terrorism – Current Threats (...continued)

- Low digital foot-print
  - Difficult to find information on attackers & attacks
  - Difficulty in profiling
- Scaling up
  - From local attacks to nation-wide events
  - From simple attacks to complex scenarios
- Artificial Intelligence (AI) armed cyber adversaries

# Proposed Countermeasures

- Cyber Stance
  - Norms, standards, and regulations
- Unified CSIRT\*
  - Per sector
  - Hierarchical
- Improve & Support Sharing
  - Expand on the NIS Directive\*\*
  - Base on **Europol & Eurojust**
  - Automated sharing of information system
  - Using **ENISA** to support efforts



\* Computer Security Incident Response Team (CSIRT)

\*\* The Directive on security of network and information systems (NIS Directive)

# More Proposed Countermeasures

- Centralized & Distributed Cyber Task-Force
  - Comprised of professionals in each field
  - Forensic services to affected nations and organizations
  - Legal aspects
- Setting Goals
  - For members & organizations
  - Similar and based on NIS Directive\*
- Intelligence
  - Increase focus on social-media
  - Own tools & systems
  - EEs
  - Sharing & cooperation

\* The Directive on security of network and information systems (NIS Directive)



## Even More Ideas

- Joint Exercises
  - General & per-sector
  - Lessons learned
- Education & Awareness
  - Public sector – schools, general media, etc.
  - Academia – higher-education, research, publications
  - Private sector – training, etc.
- EU Cyber Labs
  - Per-sector
  - Sharing data with collegial labs and with CSIRTs
  - Test-beds for new technologies and strategies

# *Prospective Incidence of Terrorism on Cyber Security*

Thank you !

Rami.Efrati@gmail.com