THE FUTURE OF CYBER TERRORISM

Matt Olsen
Co-Founder and President
IronNet Cybersecurity
@ironnetcyber
Global Jihadist Movement

- Evolution of jihadist groups
  - Rise of ISIS
  - Continued relevance of al-Qaida
- Strategic objectives
- Tactical adaptation
- Development of offensive cyber capabilities
The Rise of ISIS

- If you can kill a disbelieving American or European ... or any other disbeliever from the disbelievers waging war, including the citizens of the countries that entered into a coalition against the Islamic State, then rely upon Allah, and kill him in any manner or way however it may be. Smash his head with a rock, or slaughter him with a knife, or run him over with your car, or throw him down from a high place, or choke him, or poison him.

  – Mohammed al-Adnani, September 22, 2014
The Rise of ISIS

**Major events:**
- Attacks directed by/linked to ISIS
- Attacks inspired by ISIS
- Arrests of suspected ISIS militants or supporters

**Outlined countries are where ISIS is conducting regular military operations.**

Countries and regions in **yellow** are where ISIS has declared provinces.
Threat to Europe

TERROR DEATHS & INJURIES IN EUROPE IN 2016

- Germany: 10 dead, 48 injured
- Belgium: 32 dead, 300 injured
- France: 87 dead, 200 injured
- Turkey: 41 killed, 230 injured

PARIS TERROR ATTACKS
ISIS THREATENS NEW ROUND OF ATTACKS
Threat to the United States

ISIS inspired attacks in the United States
Increase in Violent Attacks

- Egypt: 224 dead
- Paris: 130 dead
- San Bernardino: 14 dead
- Orlando: 49 dead
Cyber threat landscape

- Nation-state level cyber capabilities
  - Russia
  - Iran
  - North Korea

- The transformation of attacks: disruptive to destructive

- Broader geopolitical context
  - Current conflicts
Increasing Sophistication of Attacks

Evolution of attacks from Nation-state actors
Where do terrorist groups fall on the cyber threat spectrum?
Terrorist Use of the Internet

- Propaganda
  - Inspire Magazine
  - Dabiq
  - Rumiyah

- Recruitment
  - Online forums
  - Direct communications

- Mobilization and Command-and-Control
  - Encrypted texts
Cyberterrorism is the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change.
ISIS Cyber: Early Organization

- 2014: Takeover of Twitter accounts
- CENTCOM and Newsweek
Junaid Hussain, British national, fled the UK to join ISIS in 2013.
The Islamic State Hacking Division emerged in early 2015. Affiliated with the Cyber Caliphate.

Hacking attacks launched in support of ISIS:
- Generated publicity for ISIS
- Attacks not sophisticated
ISIS Case Study: Ardit Ferizi

- June 2015: Ferizi gained system administrator access to a U.S. company with identifying information about 1300 military and government personnel.
- Ferizi provided the personal information to Junaid Hussain to publish a “hit list” for ISIS.
Hussain posted a Tweet with a document: “We are in your emails and computer systems, watching and recording your every move, we have your names and addresses ... passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!”

Ferizi sentenced to 20 years for material support to ISIS
September 2015, the self-proclaimed "Islamic Cyber Army" (ICA) hacking group tweets its first official statement.
“We send this message to America and Europe; we are the hackers of the Islamic State, the electronic war has not begun yet.”
Merger of Jihadist Groups

- April 2016, the Caliphate Cyber Army (CCA) announces the creation of a new collective under the name “United Cyber Caliphate.”
"After relying on Almighty Allah and by his grace, incorporation between Islamic State Hackers Teams...To expand in our operations. To hit ‘em deeper. We announce our new #Team #UnitedCyberCaliphate."
Cyberterrorism: Looking Ahead

- Organization shows signs of consolidation and coordination
- Sophisticated use of social media and propaganda has spurred development of offensive cyber capabilities
- ISIS targets:
  - Government
  - Financial entities
  - Media
- Use of publicly available hacking tools
Cyberterrorism: Looking Ahead

- Recruitment of savvy hackers
  - Gaza Hacking Forum – primary jihadi hacking forum
- Skill level remains low – compared to nation-states
- Upward trajectory – looking to improve skills and amplify preexisting strategies
Cyberterrorism: Looking Ahead

- Threat of combined kinetic and cyber attacks
- Jihadists have discussed aspirations to target critical infrastructure
- Launching damaging cyberattacks does not require a large team, and by recruiting or training a group with a higher level of skill, jihadists could have asymmetric impact.
Lessons for Government and Companies

- Lessons of 9/11 applied to cyber threats
  - Team effort
  - Build expertise
  - Harden defenses

- What you can do today
  - Threat awareness
  - Cooperation with federal agencies and first responders
  - Resilience