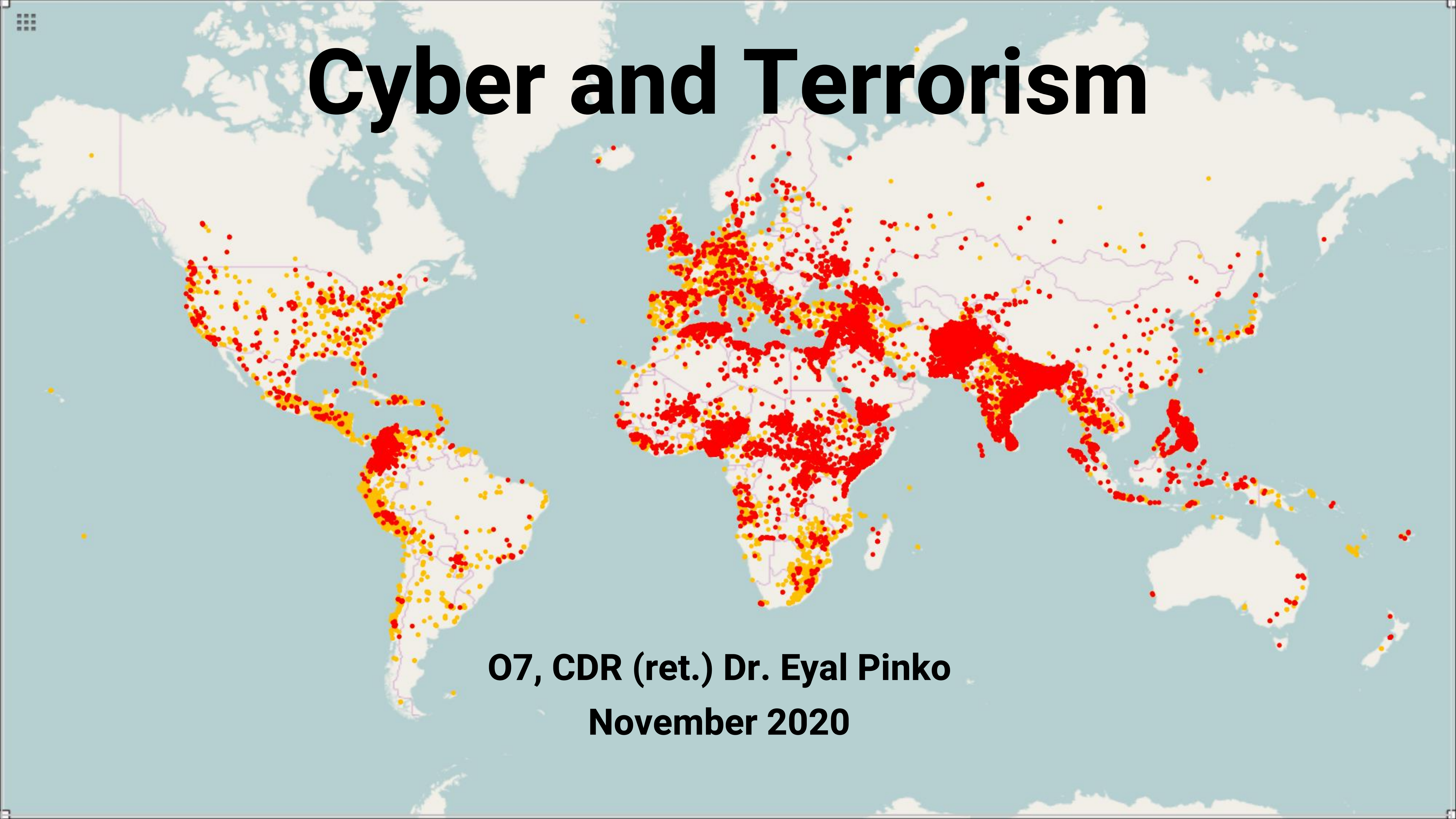
Cyber and Terrorism



O7, CDR (ret.) Dr. Eyal Pinko

November 2020

- Terror
- Cyber space and terror

Terror

What: Violent struggle

How: Against civilians

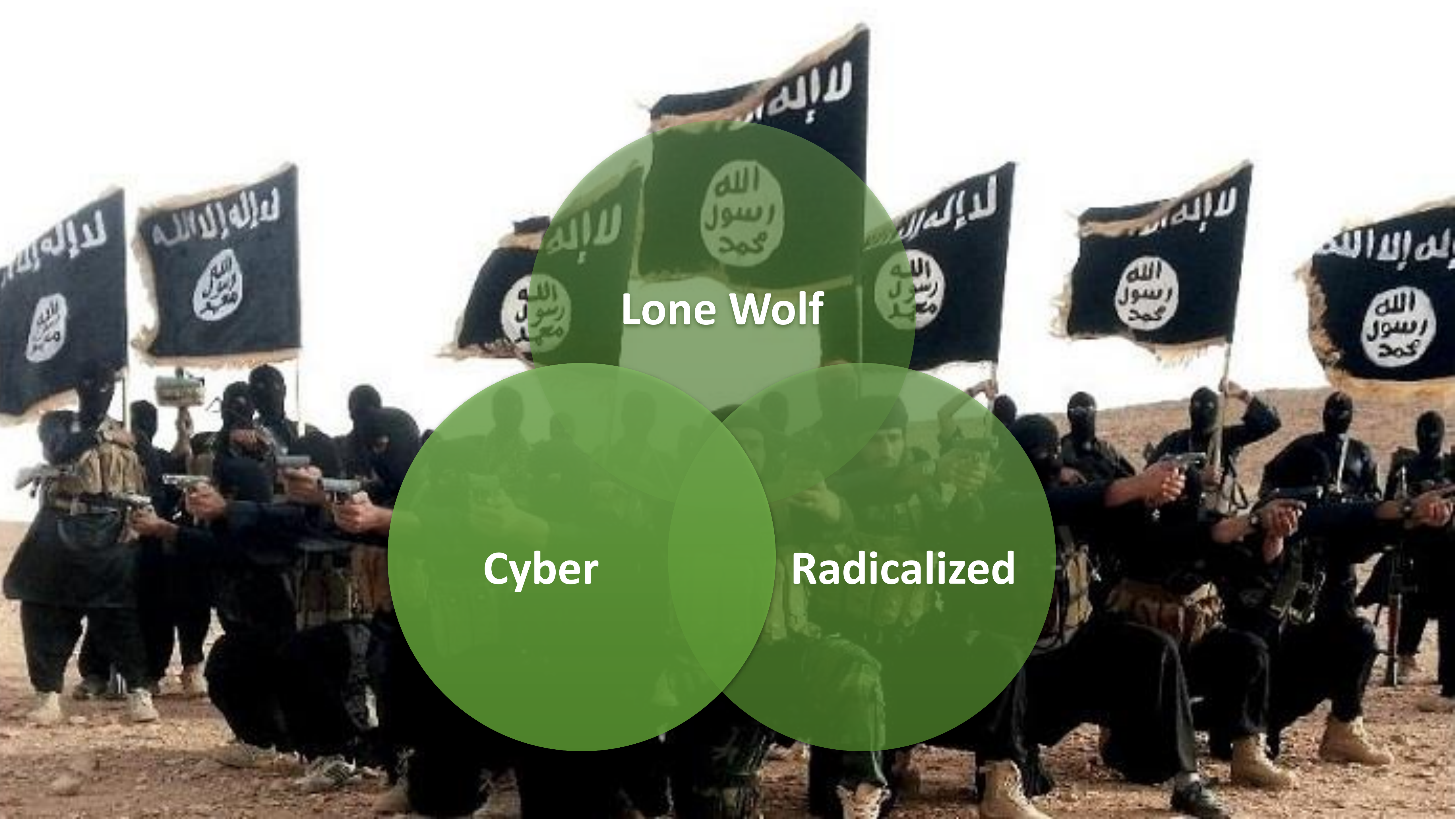
Why: Political/social purposes

Whom: Non-State actors (also by states?)

Roots of Terror

- Ethnic (Tzahania, Kurds)
- Governmental change (Red brigade, Italy)
- Religious
- Politics and economics (ISIS)
- Proxy (Hezbollah, Yemen Houthi)
- Social (poorness)

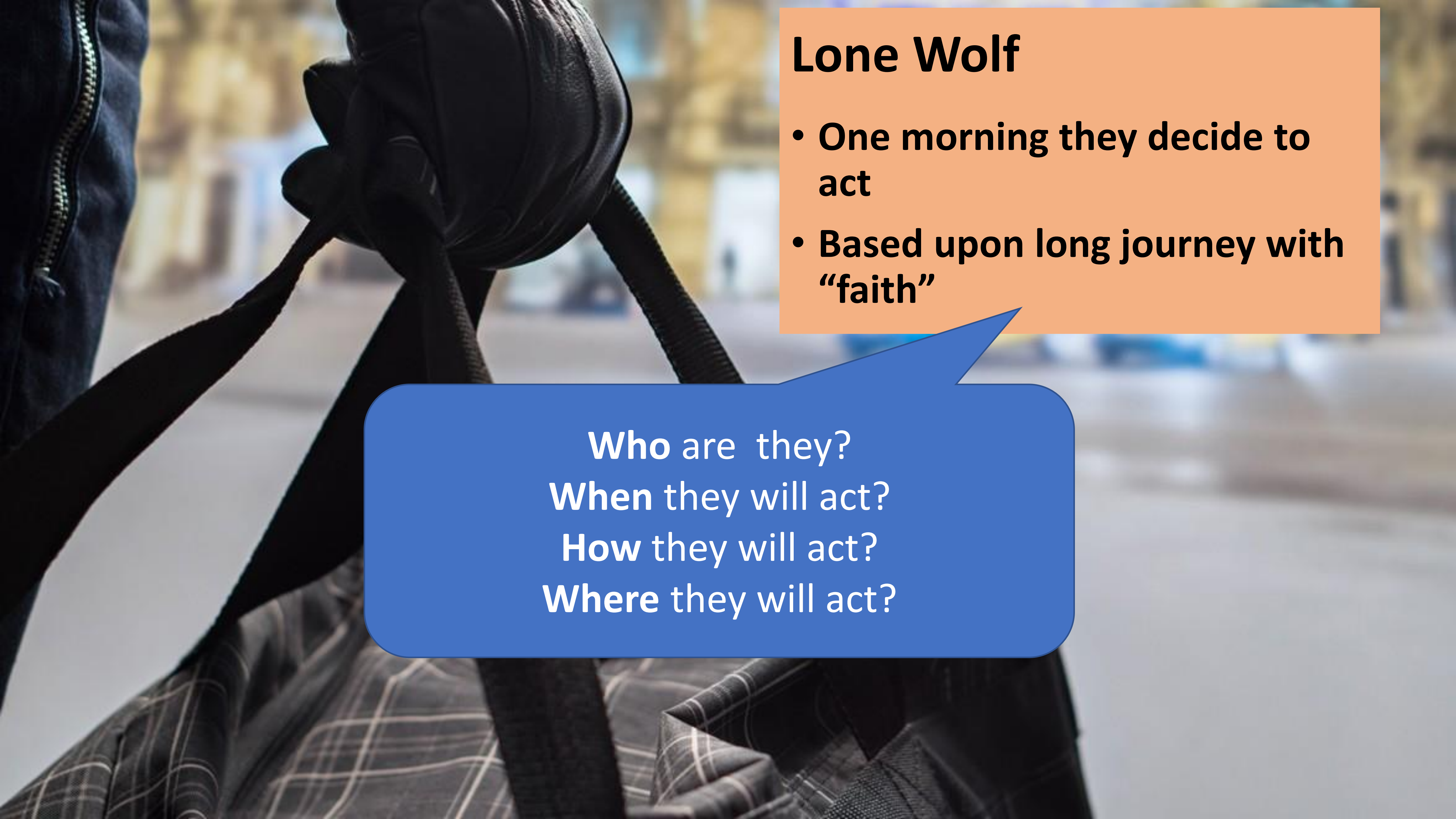
Characteristics of the New-Age Terror



Lone Wolf

Cyber

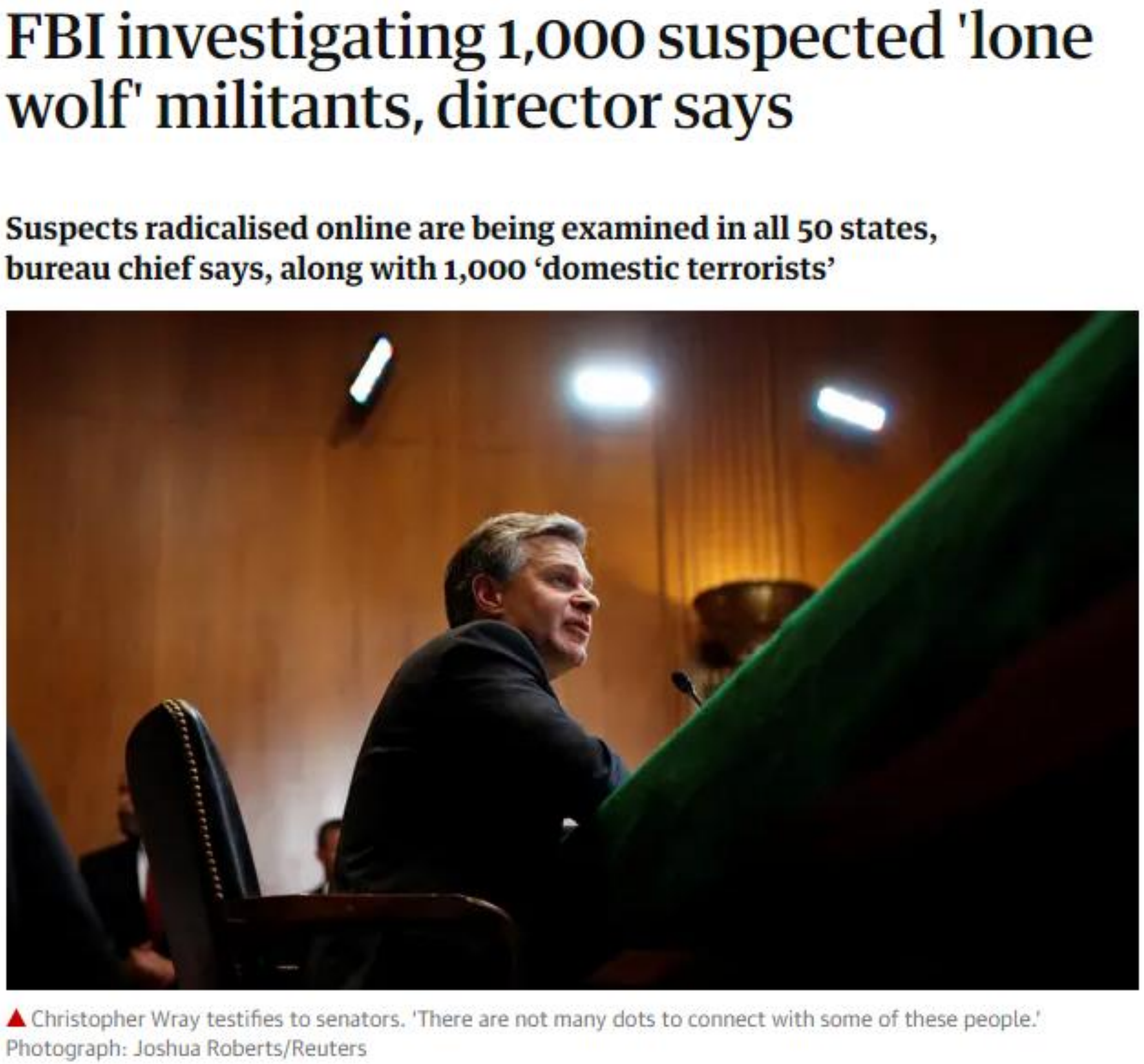
Radicalized



Lone Wolf

- One morning they decide to act
- Based upon long journey with “faith”

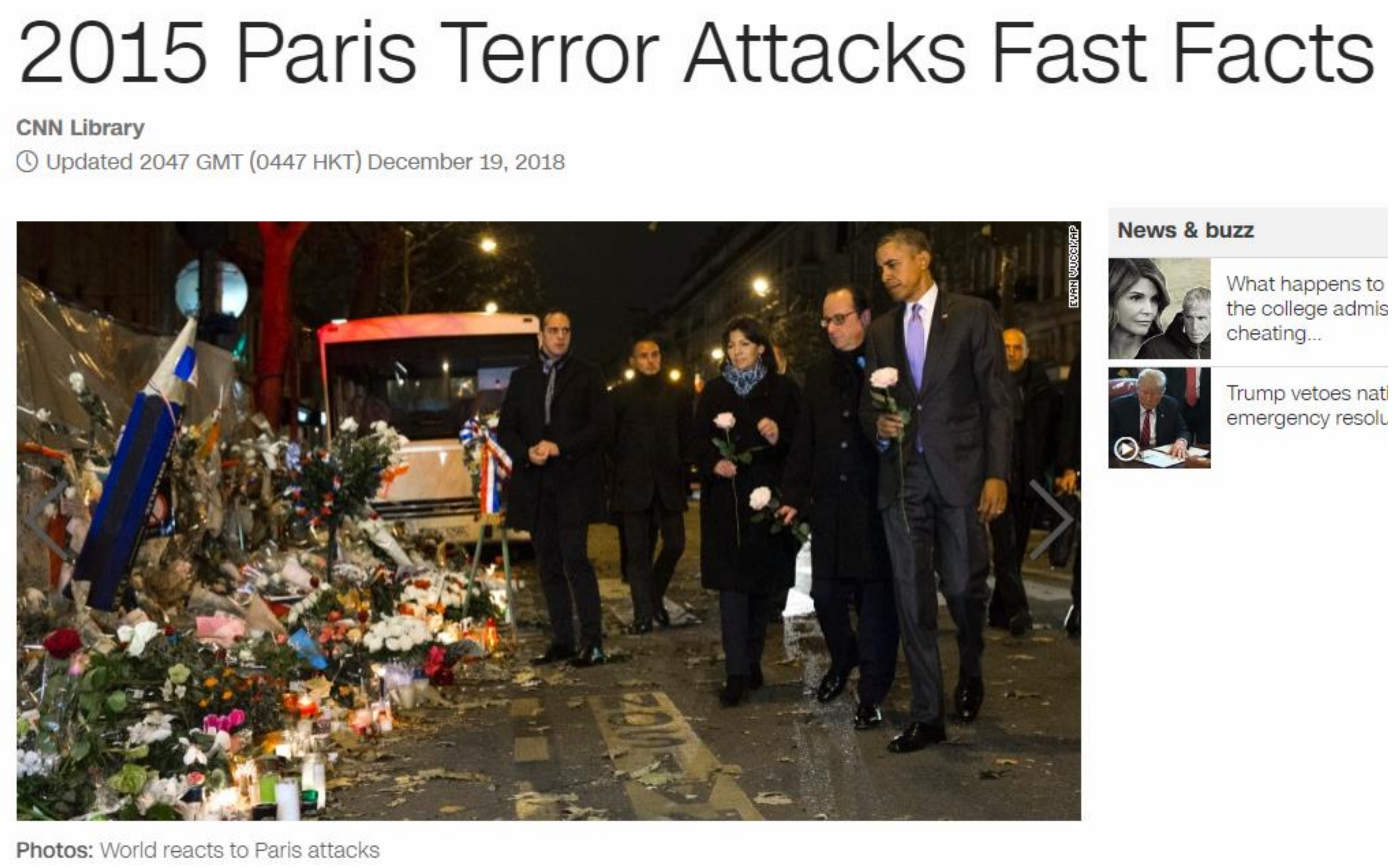
Who are they?
When they will act?
How they will act?
Where they will act?



FBI investigating 1,000 suspected 'lone wolf' militants, director says

Suspects radicalised online are being examined in all 50 states, bureau chief says, along with 1,000 'domestic terrorists'

▲ Christopher Wray testifies to senators. 'There are not many dots to connect with some of these people.' Photograph: Joshua Roberts/Reuters



2015 Paris Terror Attacks Fast Facts

CNN Library

Updated 2047 GMT (0447 HKT) December 19, 2018

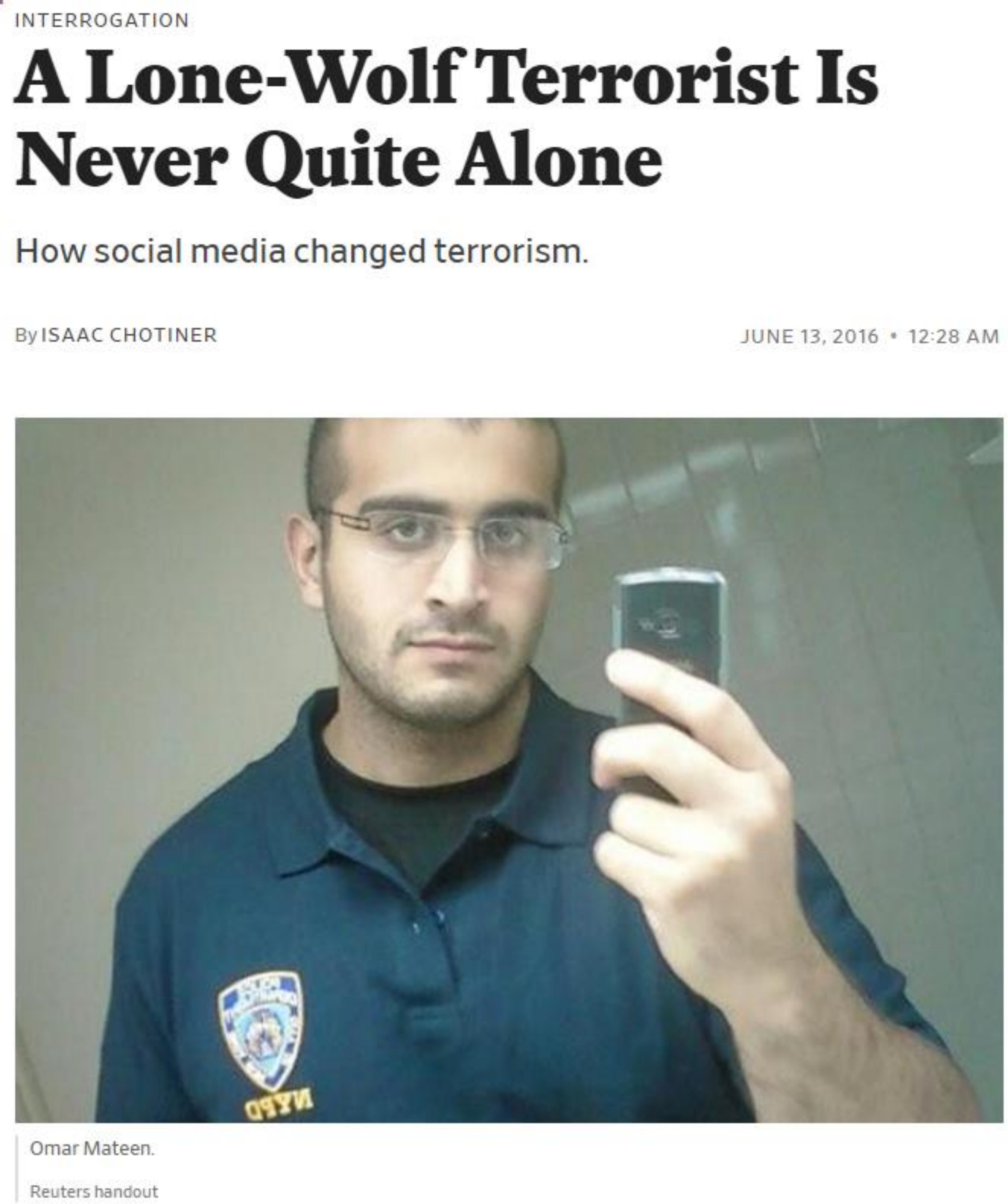
EVAN VUCCI/AP

Photos: World reacts to Paris attacks

News & buzz

What happens to the college admis cheating...

Trump vetoes nati emergency resolu



INTERROGATION

A Lone-Wolf Terrorist Is Never Quite Alone

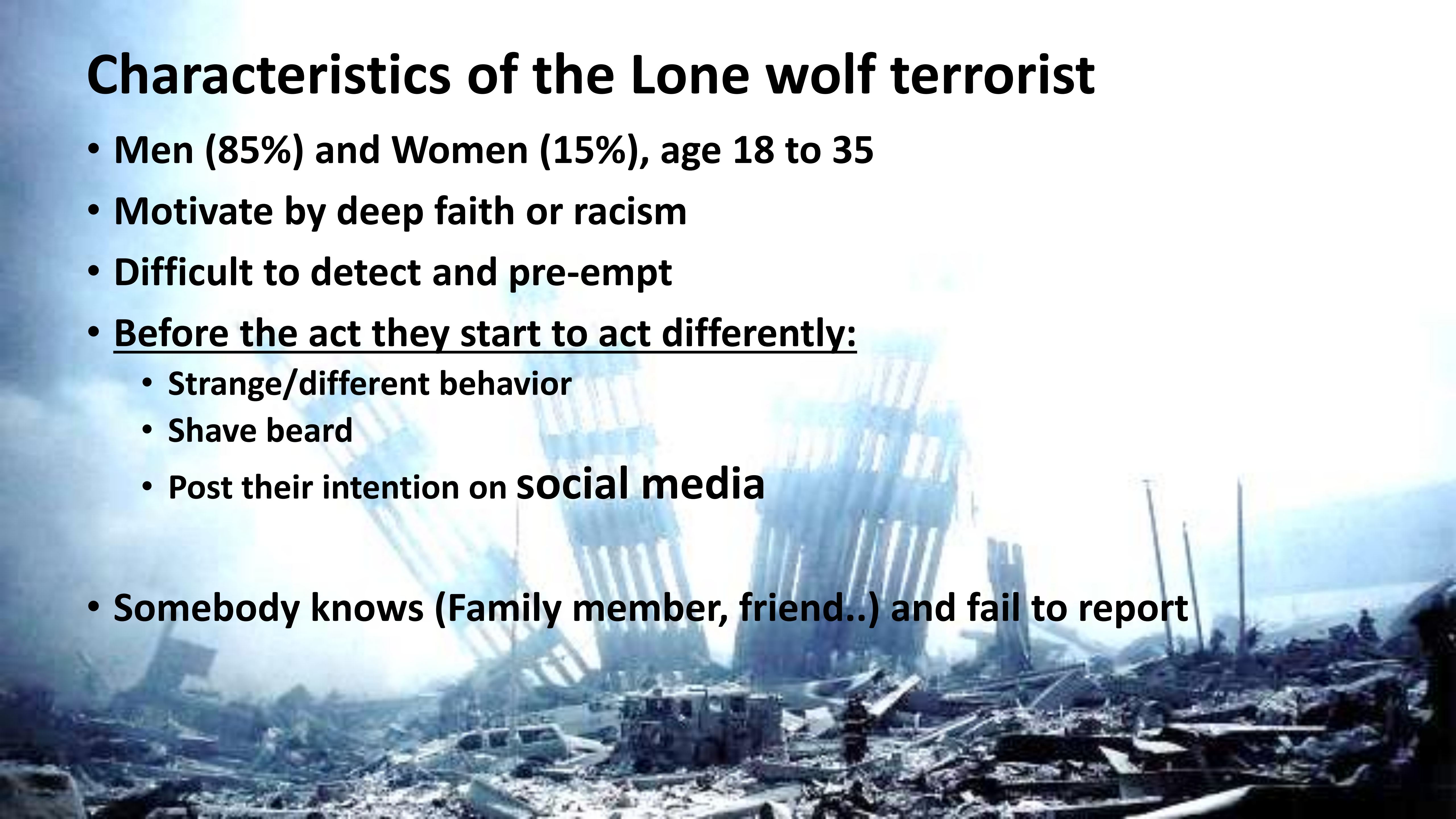
How social media changed terrorism.

By ISAAC CHOTINER

JUNE 13, 2016 • 12:28 AM

Omar Mateen.

Reuters handout



Characteristics of the Lone wolf terrorist

- Men (85%) and Women (15%), age 18 to 35
- Motivate by deep faith or racism
- Difficult to detect and pre-empt
- Before the act they start to act differently:
  - Strange/different behavior
  - Shave beard
  - Post their intention on social media
- Somebody knows (Family member, friend..) and fail to report

Motivation

- Group pressure
- Radical belief/religious
- Revenge
- Family rejection
- Social rejection and loneliness
- Been mocked by other
- Feeling they not able to preform religious ceremonies

CYBER
ATTACKS
AHEAD

World of cyber

The art of networks

What is Cyber Warfare?

Cyber warfare – The struggle for data

Control, exploit and defend data, information and information systems

Different types of adversaries

Insiders

Amateurs

Anarchists

Criminals

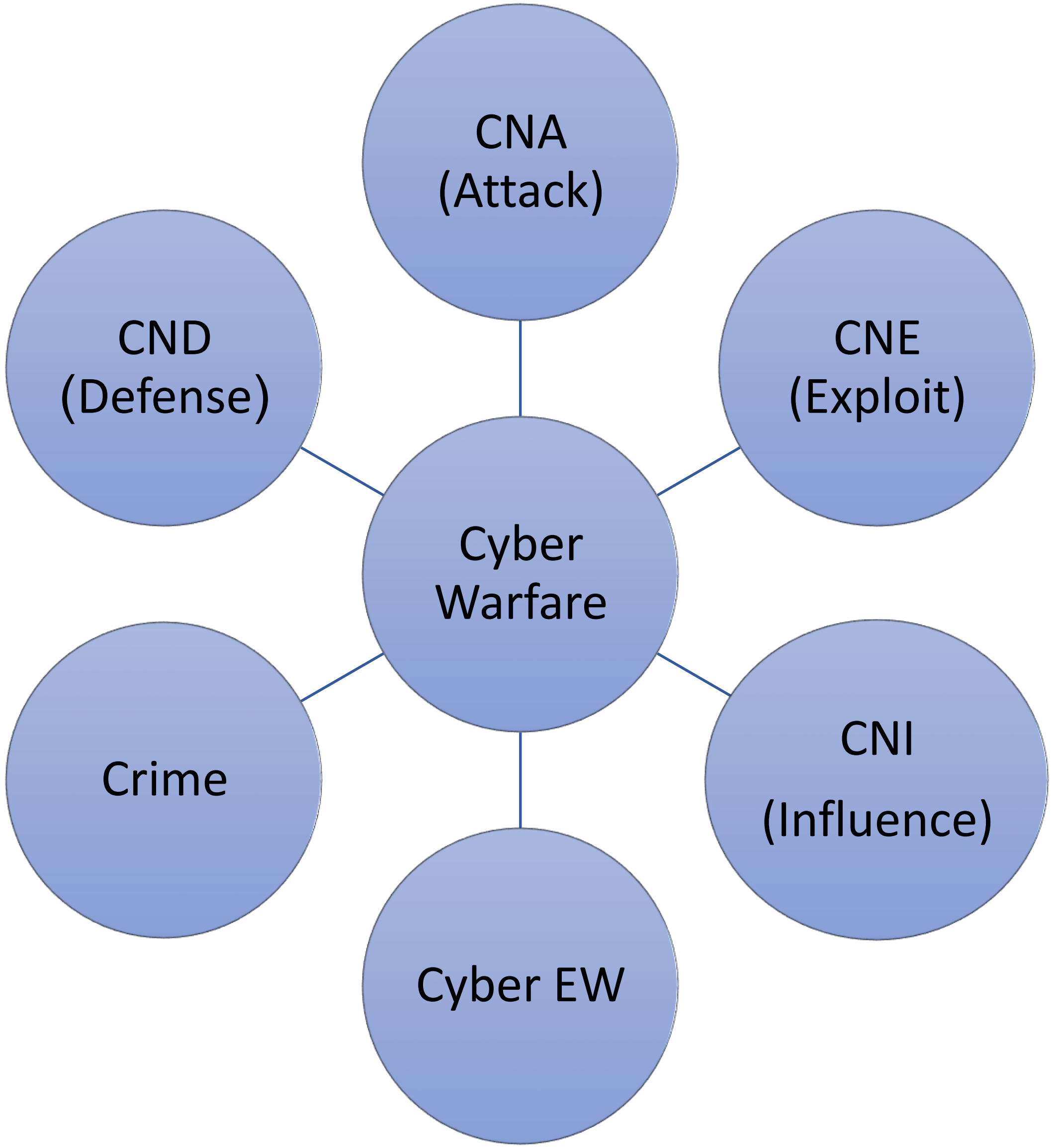
Terror organizations

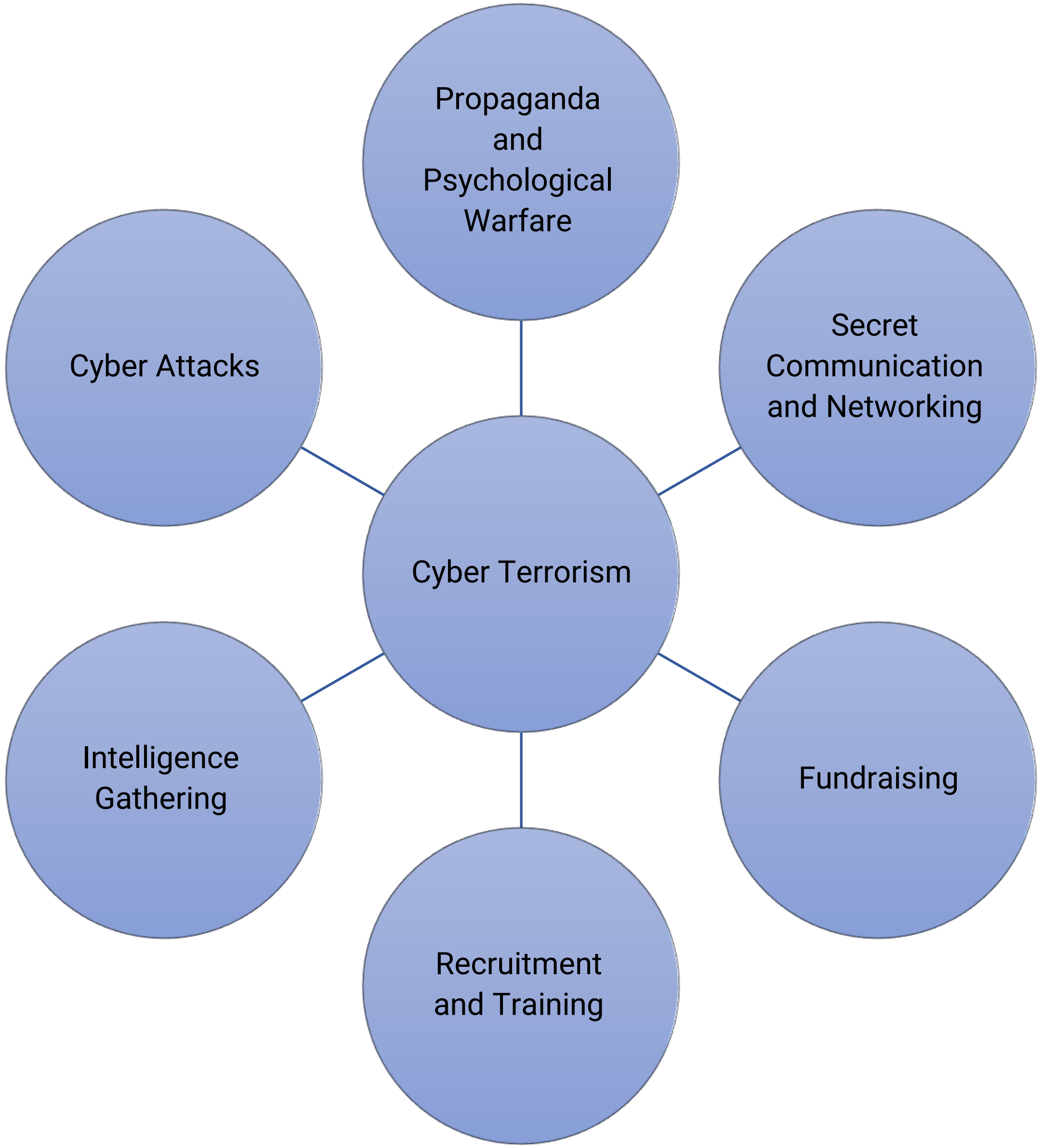
States

And different types of weapons

To cheap (even free), easy to get, for everyone and pretty easy to use…

Cyber Warfare





Cyber Terrorism

Propaganda and Psychological Warfare

Secret Communication and Networking

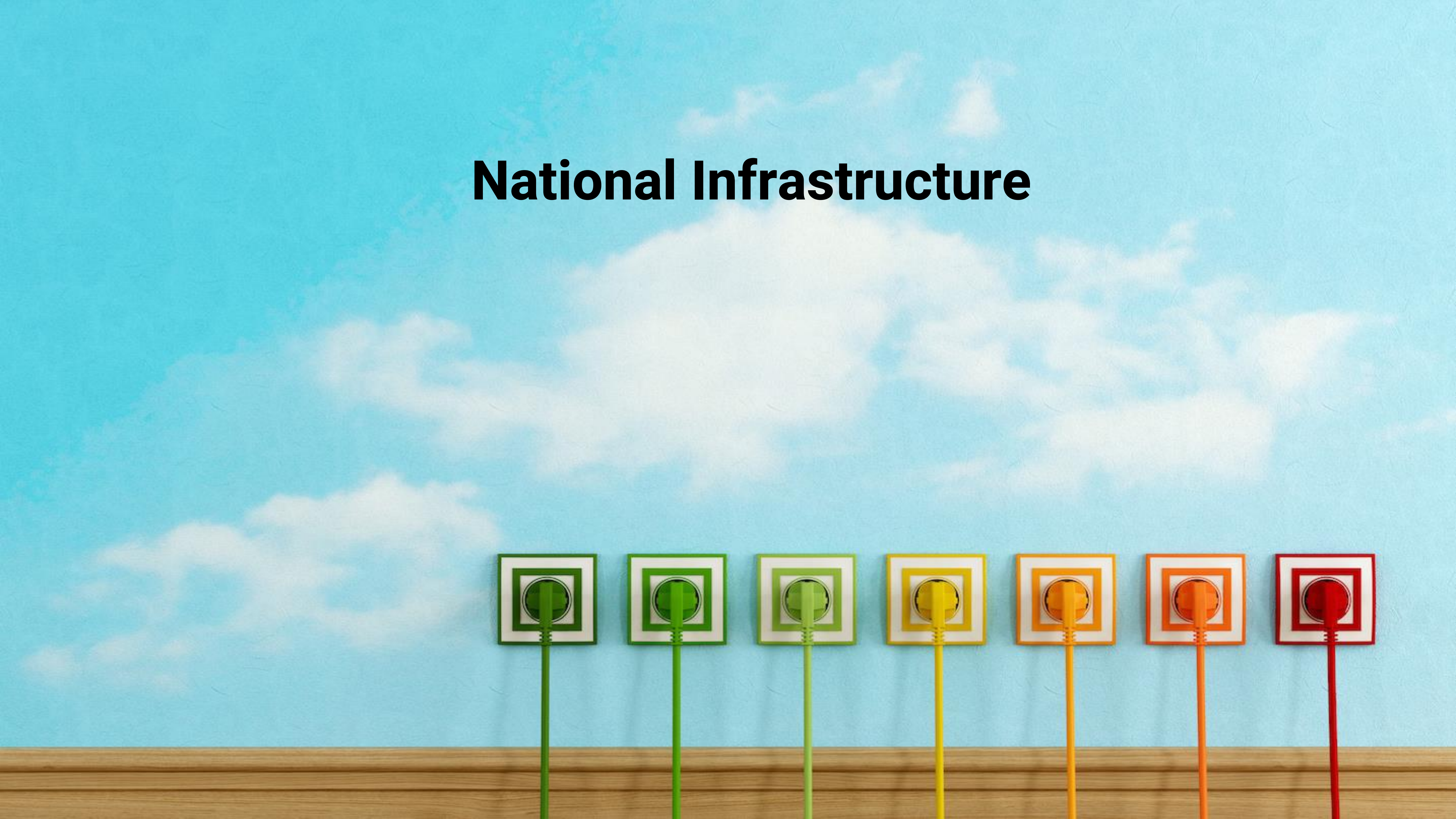
Fundraising

Recruitment and Training

Intelligence Gathering

Cyber Attacks

National Infrastructure



Cyber attacks are shutting down countries, cities and companies.

Threats to critical infrastructure from Russia and China

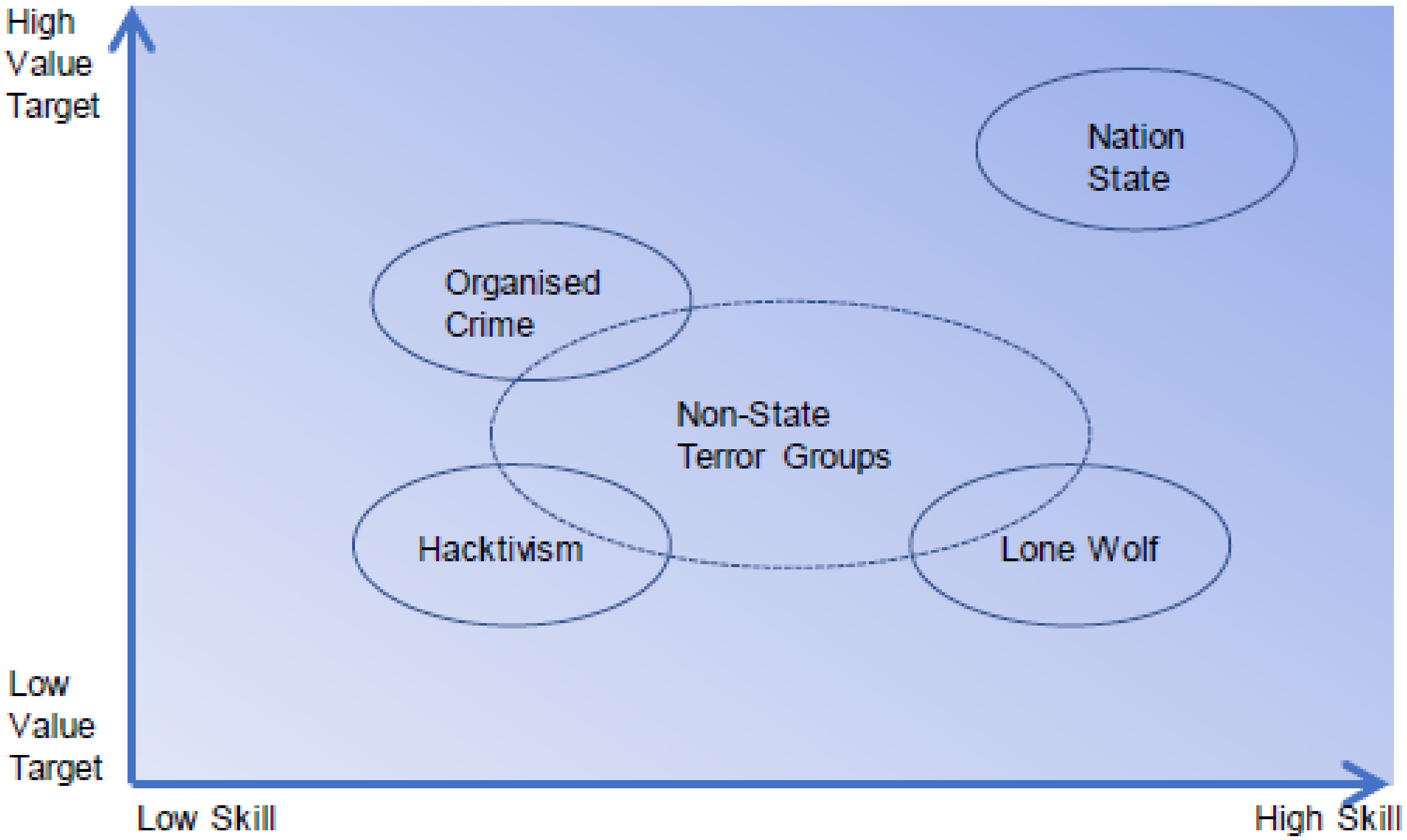
OneTrust
Privacy Management Software
HOW THE WORLD MANAGES THIRD-PARTY VENDOR RISK
A Centralized Security & Privacy Risk Management Platform
Start Free Trial

In January 2019 testimony in front of the Senate Select Committee on Intelligence, key U.S. intelligence officials – including CIA Director Gina Haspel, Director of National Intelligence Dan Coats, and FBI Director Christopher Wray – outlined the various types of cyber threats that China and Russia pose to the United States, both at home and abroad. They highlighted three key areas where the two strategic rivals pose the biggest threats to national security: cyber attacks against critical infrastructure, online influence and misinformation campaigns on social media designed to destabilize American democratic institutions, and direct interference in U.S. elections (including the upcoming 2020 presidential election).

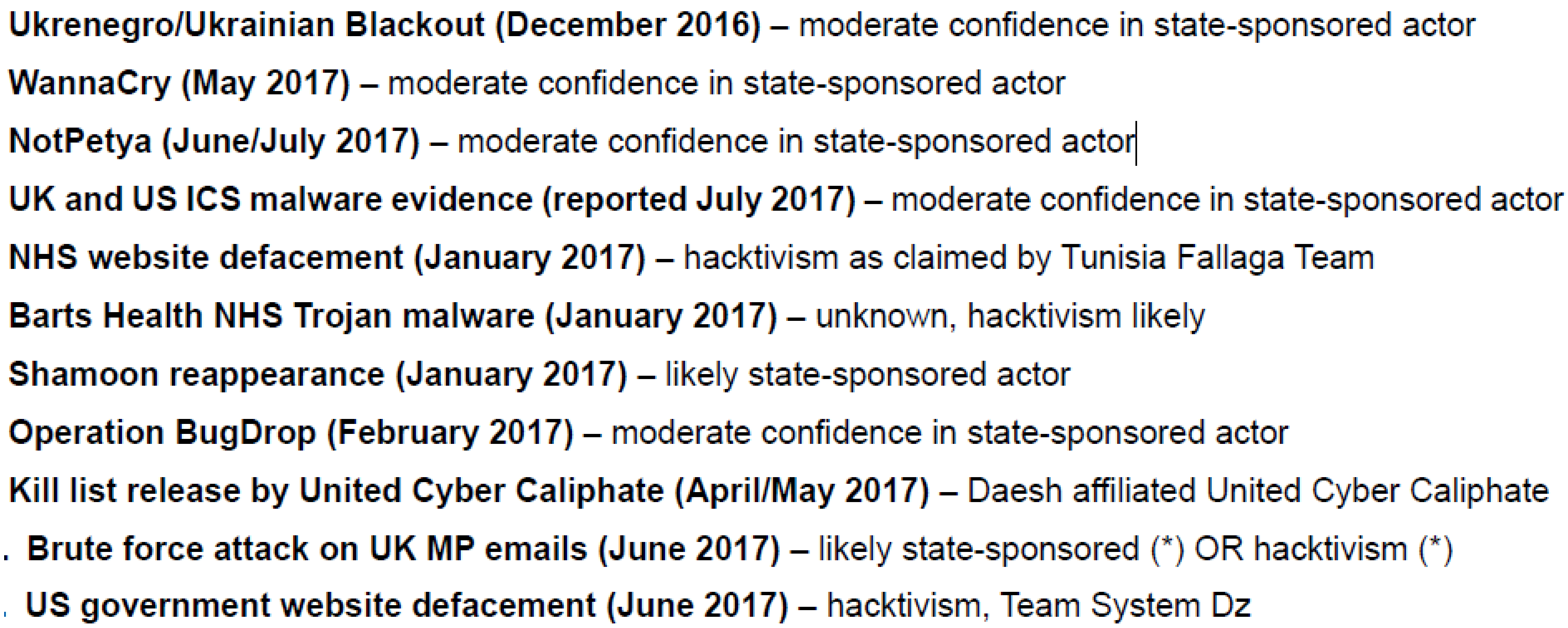
Who are the cyber-Terrorist?

- States
- Terror organizations
- Activist -> Hacktivist
- Lone Wolf

Threat Intelligence Model of Cyber Capabilities



Few Examples…



Ukrenegro/Ukrainian Blackout (December 2016) – moderate confidence in state-sponsored actor

WannaCry (May 2017) – moderate confidence in state-sponsored actor

NotPetya (June/July 2017) – moderate confidence in state-sponsored actor

UK and US ICS malware evidence (reported July 2017) – moderate confidence in state-sponsored actor

NHS website defacement (January 2017) – hacktivism as claimed by Tunisia Fallaga Team

Barts Health NHS Trojan malware (January 2017) – unknown, hacktivism likely

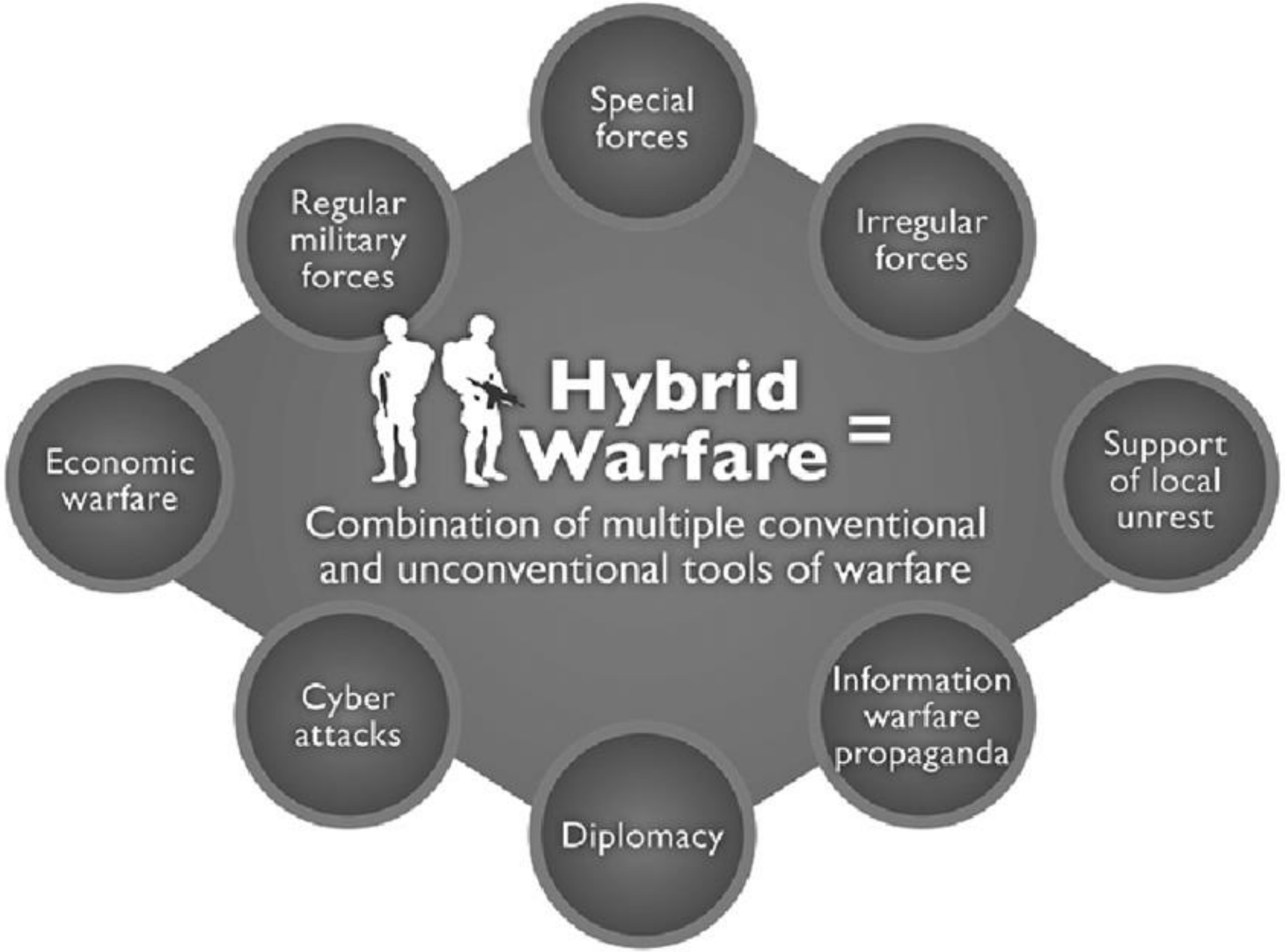
Shamoon reappearance (January 2017) – likely state-sponsored actor

Operation BugDrop (February 2017) – moderate confidence in state-sponsored actor

Kill list release by United Cyber Caliphate (April/May 2017) – Daesh affiliated United Cyber Caliphate

- **Brute force attack on UK MP emails (June 2017)** – likely state-sponsored (*) OR hacktivism (*)
- **US government website defacement (June 2017)** – hacktivism, Team System Dz

WELCOME!



Hybrid Warfare =

Combination of multiple conventional and unconventional tools of warfare

- Special forces
- Irregular forces
- Support of local unrest
- Information warfare propaganda
- Diplomacy
- Cyber attacks
- Economic warfare
- Regular military forces

O7 CDR (ret.) Dr. Eyal Pinko
eyalpinko@gmail.com

Questions?

Thank you!

O7 CDR (ret.) Dr. Eyal Pinko
eyalpinko@gmail.com