Cybercrime: What States Can Do

Maggie Brunner

Program Director, Cybersecurity, Emergency Communications & Technology

Homeland Security & Public Safety Division

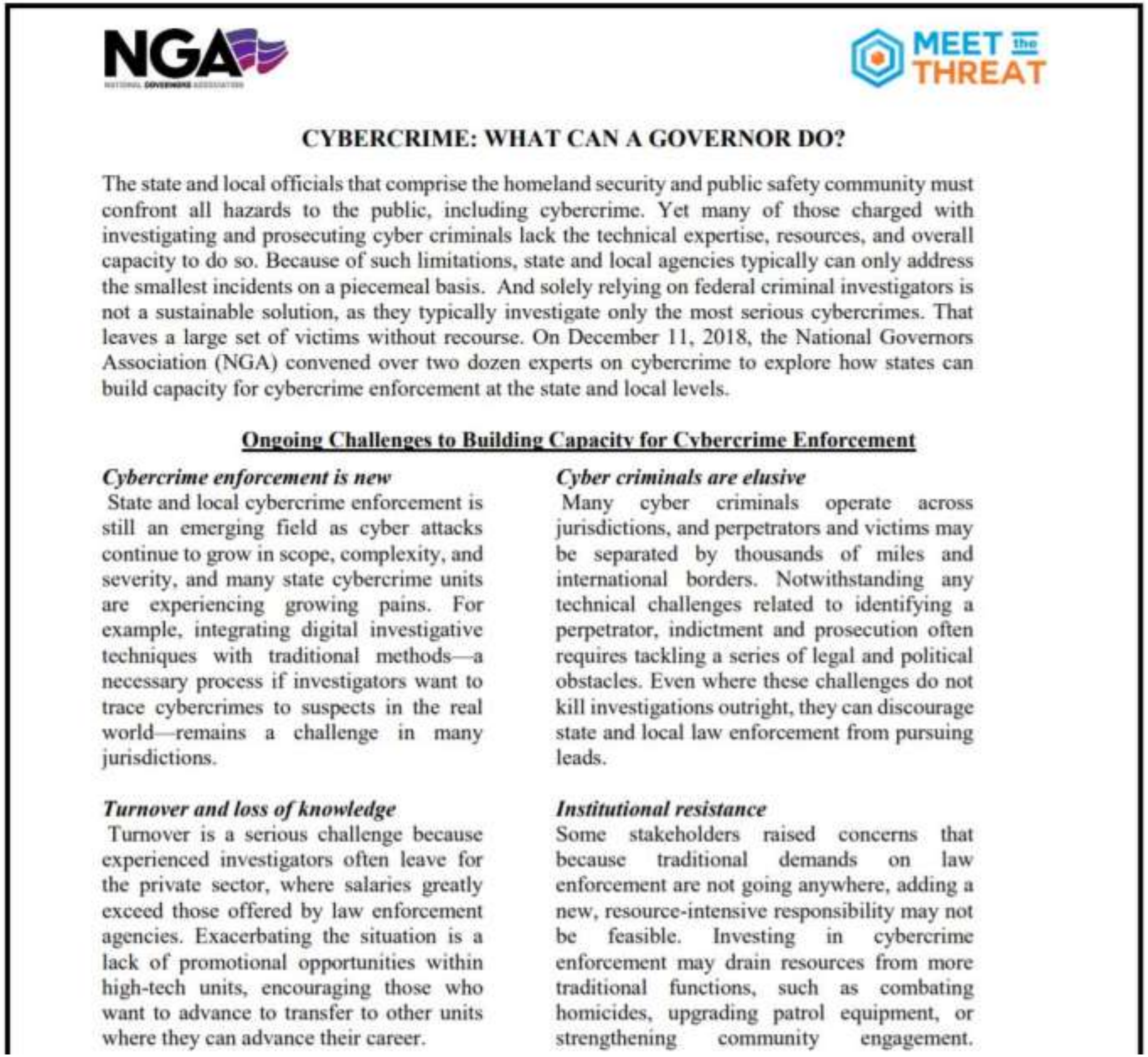
NGA Center for Best Practices

NGA Overview

Nonpartisan, Nonprofit

On-the-Ground Impact

Resource Center for State Cybersecurity



CYBERCRIME: WHAT CAN A GOVERNOR DO?

The state and local officials that comprise the homeland security and public safety community must confront all hazards to the public, including cybercrime. Yet many of those charged with investigating and prosecuting cyber criminals lack the technical expertise, resources, and overall capacity to do so. Because of such limitations, state and local agencies typically can only address the smallest incidents on a piecemeal basis. And solely relying on federal criminal investigators is not a sustainable solution, as they typically investigate only the most serious cybercrimes. That leaves a large set of victims without recourse. On December 11, 2018, the National Governors Association (NGA) convened over two dozen experts on cybercrime to explore how states can build capacity for cybercrime enforcement at the state and local levels.

Ongoing Challenges to Building Capacity for Cybercrime Enforcement

Cybercrime enforcement is new

State and local cybercrime enforcement is still an emerging field as cyber attacks continue to grow in scope, complexity, and severity, and many state cybercrime units are experiencing growing pains. For example, integrating digital investigative techniques with traditional methods—a necessary process if investigators want to trace cybercrimes to suspects in the real world—remains a challenge in many jurisdictions.

Turnover and loss of knowledge

Turnover is a serious challenge because experienced investigators often leave for the private sector, where salaries greatly exceed those offered by law enforcement agencies. Exacerbating the situation is a lack of promotional opportunities within high-tech units, encouraging those who want to advance to transfer to other units where they can advance their career.

Cyber criminals are elusive

Many cyber criminals operate across jurisdictions, and perpetrators and victims may be separated by thousands of miles and international borders. Notwithstanding any technical challenges related to identifying a perpetrator, indictment and prosecution often requires tackling a series of legal and political obstacles. Even where these challenges do not kill investigations outright, they can discourage state and local law enforcement from pursuing leads.

Institutional resistance

Some stakeholders raised concerns that because traditional demands on law enforcement are not going anywhere, adding a new, resource-intensive responsibility may not be feasible. Investing in cybercrime enforcement may drain resources from more traditional functions, such as combating homicides, upgrading patrol equipment, or strengthening community engagement.

Webinar

1. What is Cybercrime and Why is it Important?
2. What are the Challenges Associated with Cybercrime?
3. What can States Do?

What is Cybercrime?

High Tech Crime v. Computer-Enabled Crime

Cost of Cybercrime is Increasing

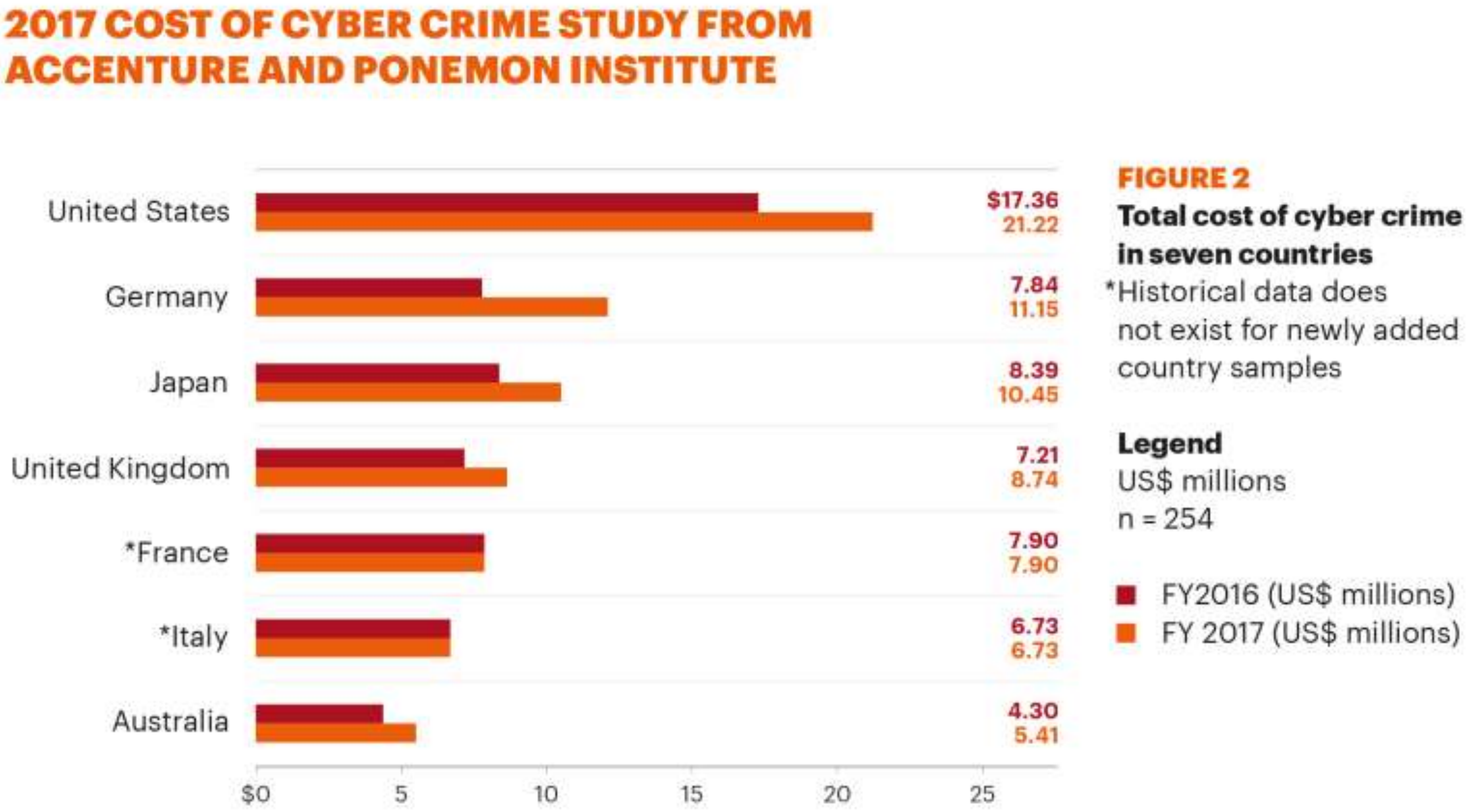

2017 COST OF CYBER CRIME STUDY FROM ACCENTURE AND PONEMON INSTITUTE

FIGURE 2

Total cost of cyber crime in seven countries

*Historical data does not exist for newly added country samples

Legend

US$ millions

n = 254

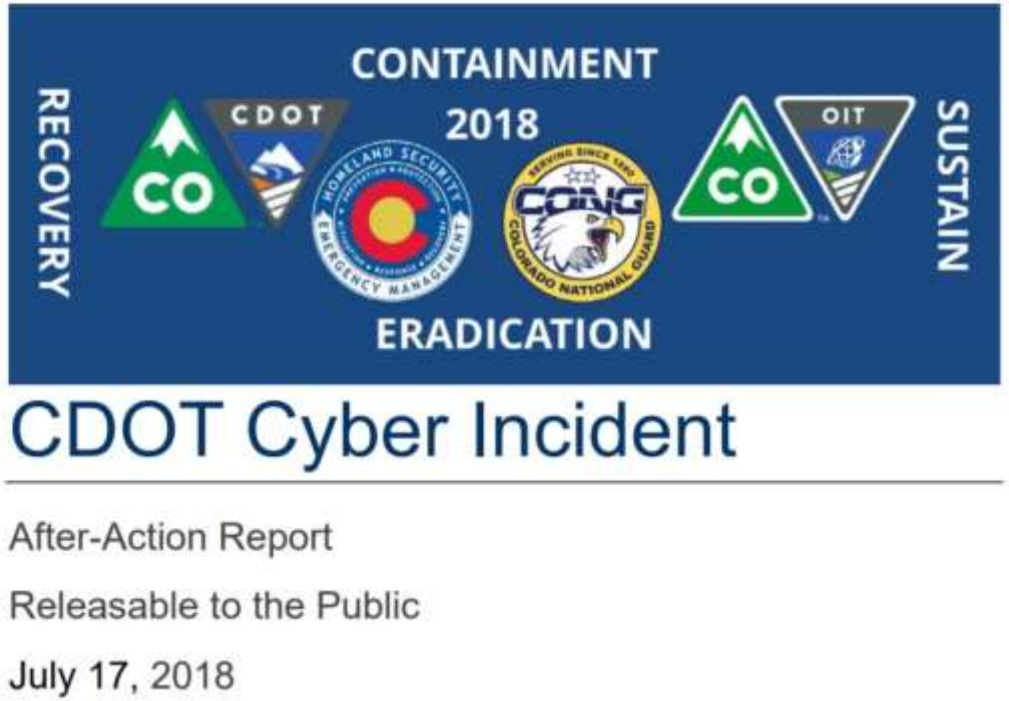
🟥 FY2016 (US$ millions)

🟧 FY 2017 (US$ millions)

Source: Ponemon Institute & Accenture, “The Cost of Cyber Crime Study” (2017)

Severity: Real World Victims

Severity: Critical Infrastructure and Lifeline Services

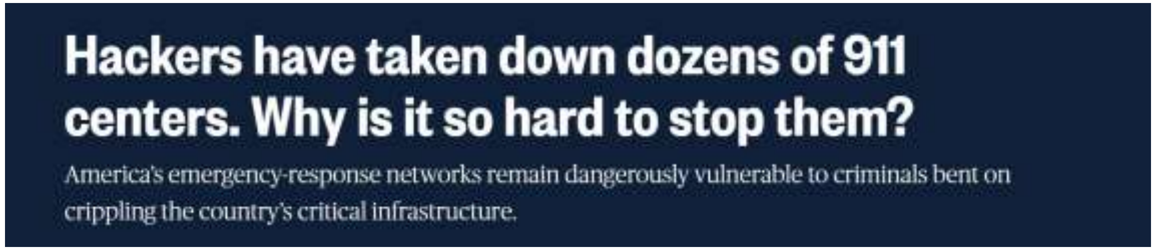


CDOT Cyber Incident

After-Action Report

Releasable to the Public

July 17, 2018



Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?

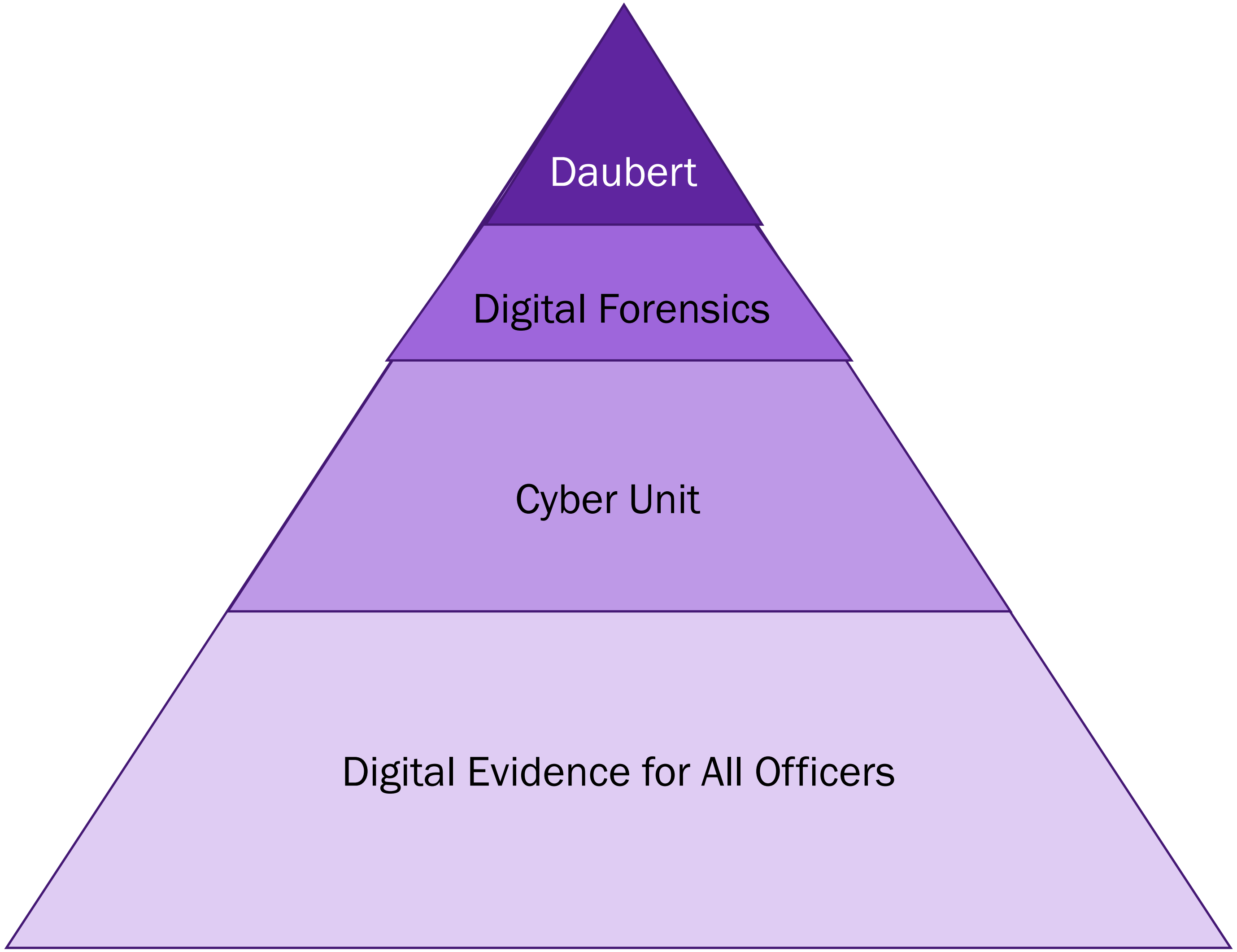
America's emergency-response networks remain dangerously vulnerable to criminals bent on crippling the country's critical infrastructure.

Challenges

CRIME SCENE DO N
CRIME SCENE DO
5
Priorities
NARCOTICS
HOMICIDE

Personnel Considerations

Training



Daubert

Digital Forensics

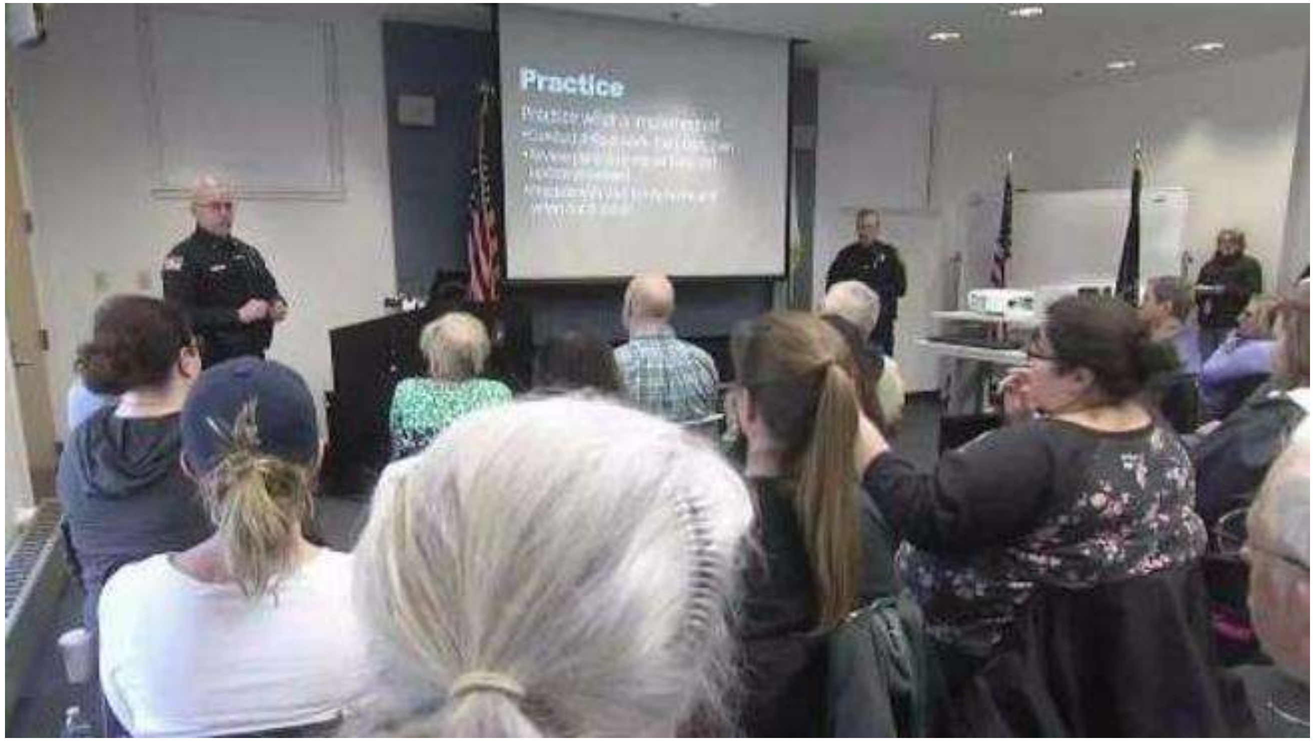
Cyber Unit

Digital Evidence for All Officers

What States Can Do

LAW
LAW
LAW
LAW
LAW
LAW

Educating the Community



Mark Wilson
Julie Rock
FAc

Free Training Resources

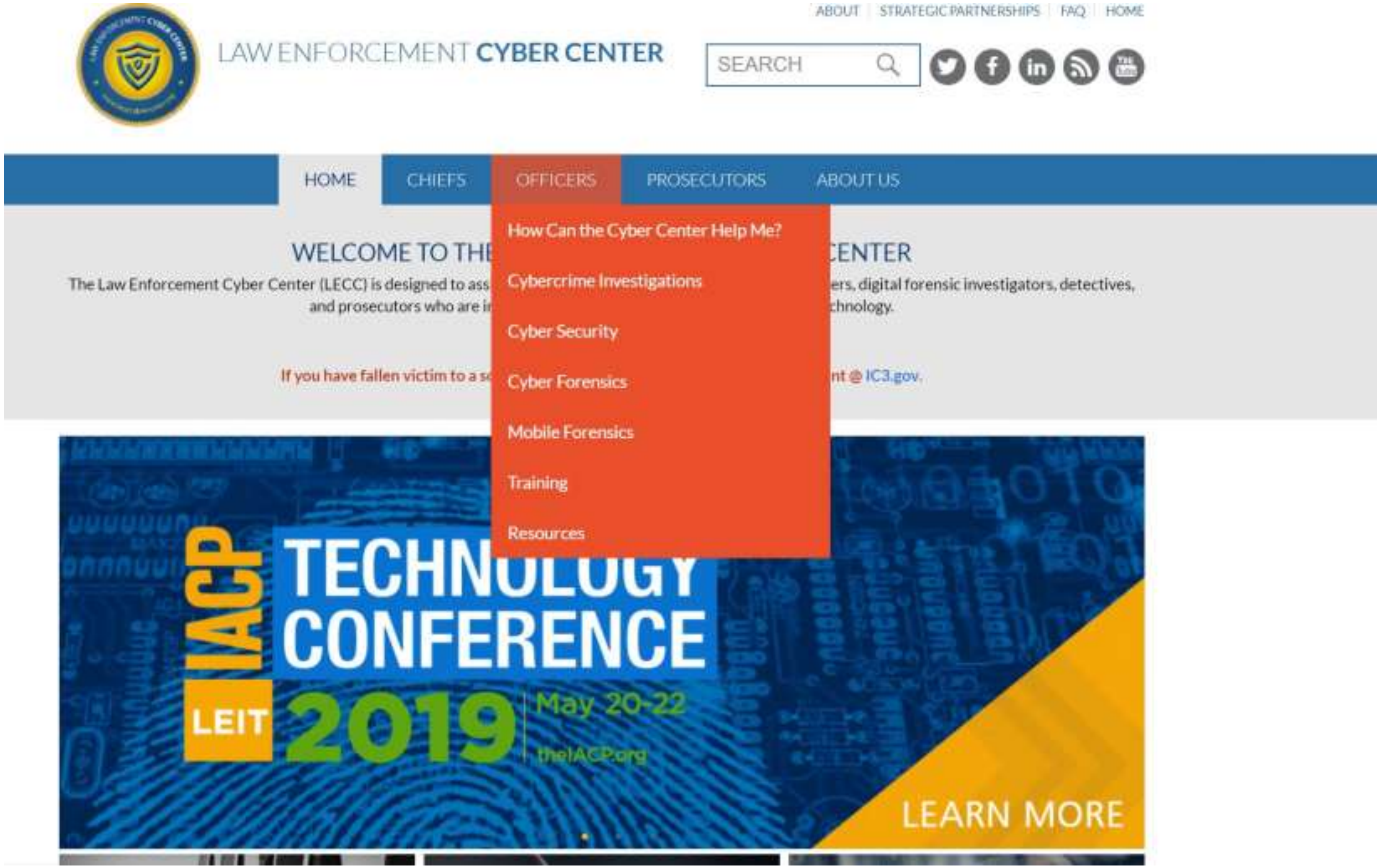
UNITED STATES SECRET SERVICE

NW3C

National White Collar Crime Center

SEARCH

Bureau of Justice Assistance Resources


ABOUT | STRATEGIC PARTNERSHIPS | FAQ | HOME
LAW ENFORCEMENT CYBER CENTER
SEARCH
HOME
CHIEFS
OFFICERS
PROSECUTORS
ABOUT US
How Can the Cyber Center Help Me?
Cybercrime Investigations
Cyber Security
Cyber Forensics
Mobile Forensics
Training
Resources
IACP TECHNOLOGY CONFERENCE
LEIT 2019
May 20-22
theIACP.org
LEARN MORE

WELCOME TO THE … CENTER

The Law Enforcement Cyber Center (LECC) is designed to ass… …ers, digital forensic investigators, detectives, and prosecutors who are i… …chnology.

If you have fallen victim to a s… …nt @ IC3.gov.

www.iacpcybercenter.org

Questions?

NGA

NATIONAL GOVERNORS ASSOCIATION

mbrunner@nga.org

NGA

NATIONAL GOVERNORS ASSOCIATION