THE ELIXIR OF SPORT

FOR CAPACITY BUILDING IN CYBER

WHO WE ARE & HOW THIS BEGAN

- Sports-ISAO: Program Office of Cyber Resilience Institute (CRI)

- CRI: Nonprofit with a mission of building cyber capacity in communities

- ISAO and Pop-up SOC operations began in 2016 to demonstrate a crowdsourced cyber threat and information sharing operation; a key component was an internship of college students
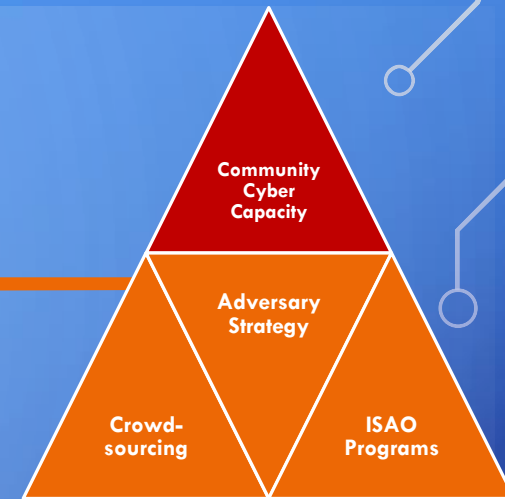
- 2016 → Rio Olympics

- 2017 → IAAF World Championships

- 2018 → Winter Olympics PyeongChang

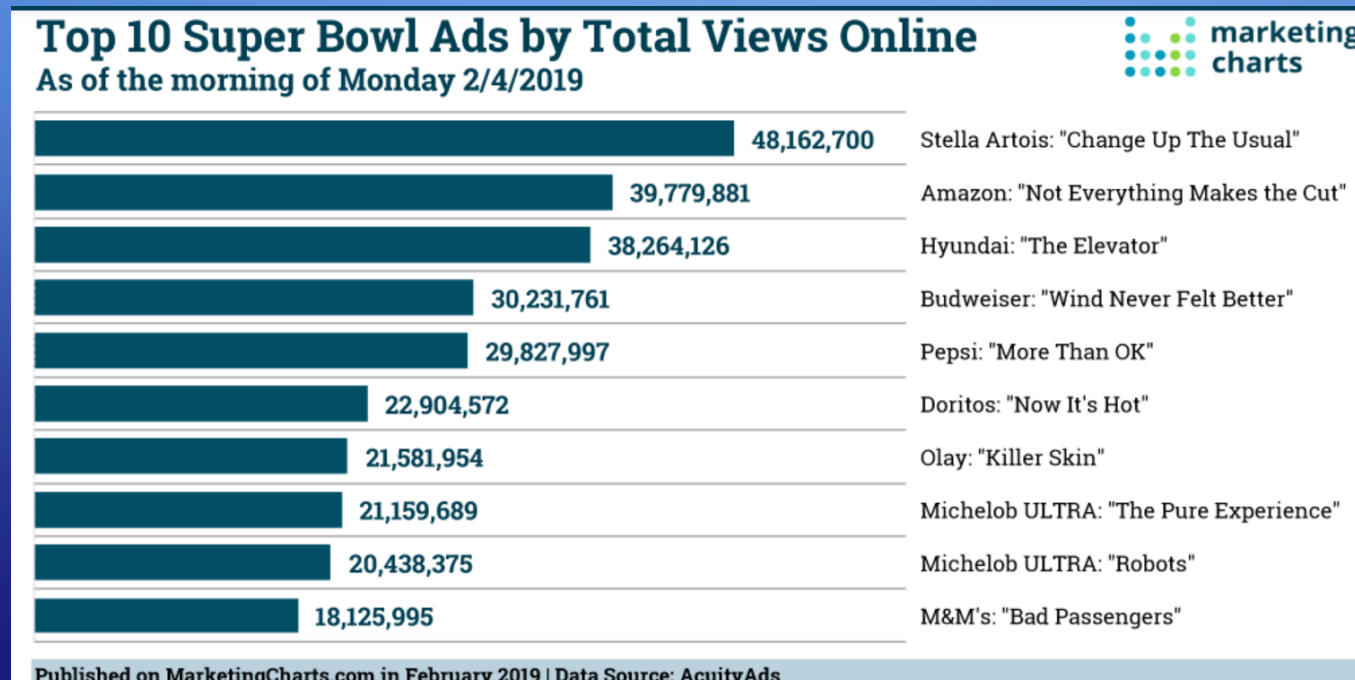- 2018 → World Cup Russia

- 2019 → World Cup France

d-Watch

ANALYSTS FOR THE WORKFORCE – A PATHWAY

THE ELIXIR OF SPORT

- Students from over 40 universities – the **Crowd**Watch

- First college student club at UCCS

- Adversaries: Proving ground for new variants and TTP

Top 10 Super Bowl Ads by Total Views Online
As of the morning of Monday 2/4/2019

Views	Ad
48,162,700	Stella Artois: "Change Up The Usual"
39,779,881	Amazon: "Not Everything Makes the Cut"
38,264,126	Hyundai: "The Elevator"
30,231,761	Budweiser: "Wind Never Felt Better"
29,827,997	Pepsi: "More Than OK"
22,904,572	Doritos: "Now It's Hot"
21,581,954	Olay: "Killer Skin"
21,159,689	Michelob ULTRA: "The Pure Experience"
20,438,375	Michelob ULTRA: "Robots"
18,125,995	M&M's: "Bad Passengers"

Published on MarketingCharts.com in February 2019 | Data Source: AcuityAds

- Total TV ad spend: $1.5B
New spend quadrupled: $548M

- Budweiser: $33.2M

- Amazon: $27.5 million

Community Cyber Capacity
Adversary Strategy
Crowd-sourcing
ISAO Programs

THE ELIXIR OF SPORT
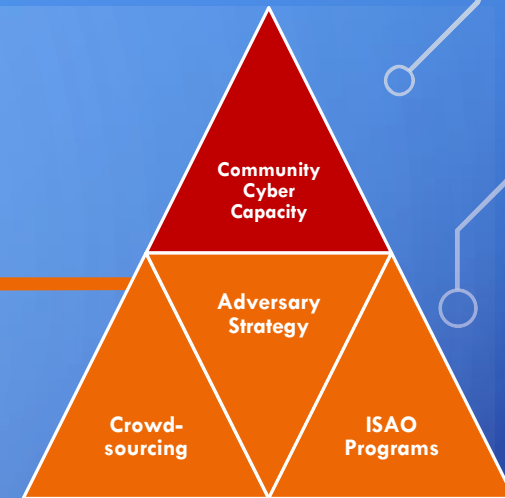
- Magnetism = Demand

- Translation: Workforce

Community Cyber Capacity / Adversary Strategy / Crowd-sourcing / ISAO Programs

US 'CYBERSECURITY' STRATEGY

- 2009 White House '**Cyberspace**' Policy Review

- 2015 DOD **Cyber** Strategy: "The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas."
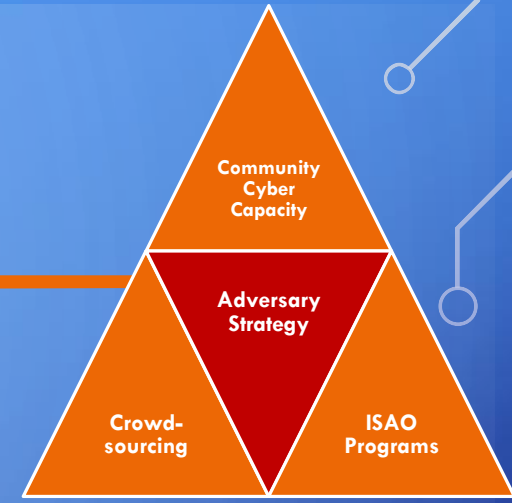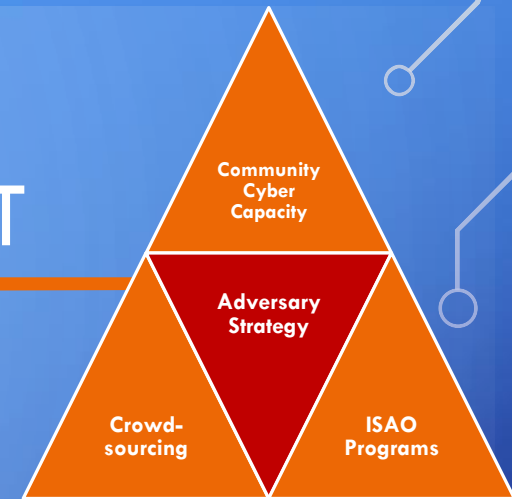
ADVERSARY STRATEGY AND TACTICS

- Mueller Report: "Russia interfered in the 2016 presidential election in sweeping and systematic fashion"

- And China

- And ...

Facebook, Twitter Accuse China of Fueling Hong Kong Disinformation

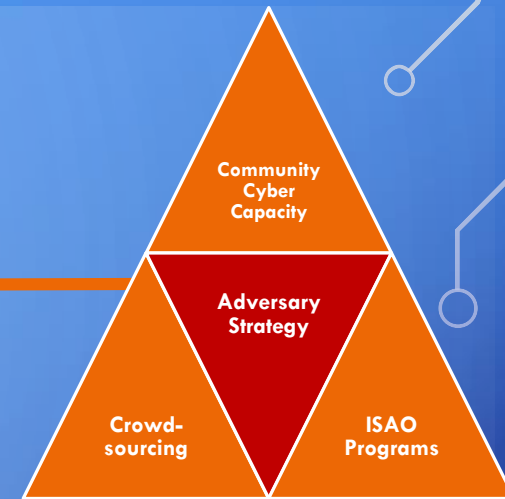# CYBER INTELLIGENCE – A VIEW FROM SPORT

Russian foreign minister: We're banned from Olympics because U.S. 'can't beat us fairly'

By DES BIELER
THE WASHINGTON POST | FEB 12, 2018 | 10:26 AM

INCREASED USE OF CYBER IN STRATEGY

2015 Russian National Security Strategy

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О Стратегии национальной безопасности
Российской Федерации

В соответствии с федеральными законами от 28 декабря 2010 г.
№ 390-ФЗ "О безопасности" и от 28 июня 2014 г. № 172-ФЗ
"О стратегическом планировании в Российской Федерации"
п о с т а н о в л я ю:

"increase the competitiveness and international prestige of the Russian Federation."

Russian view:
U.S. Doctrine and Strategy are anti-Russian

Community Cyber Capacity

Adversary Strategy

Crowd-sourcing

ISAO Programs

RUSSIA

The Foundations of Geopolitics: The Geopolitical Future of Russia
Aleksandr Dugin

"the maximum task is the 'Finlandization' of all of Europe"

The United Kingdom should be cut off from Europe

Ukraine should be annexed by Russia because "Ukraine as a state has no geopolitical meaning"

"Moscow-Tehran axis": Iran is a key ally

CYBER DISINFORMATION AS STATE-ACTOR STRATEGY

The US narrative: Russia must spread Anti-Americanism everywhere: "the main 'scapegoat' will be precisely the U.S."

In the United States:
- Russia should use its special services within the borders of the United States to fuel instability and separatism, for instance, provoke "Afro-American racists".
- Russia should "introduce geopolitical disorder into internal American activity, encouraging all kinds of separatism and ethnic, social and racial conflicts, actively supporting all dissident movements – extremist, racist, and sectarian groups, thus destabilizing internal political processes in the U.S.
- It would also make sense simultaneously to support isolationist tendencies in American politics."

SOCIAL MEDIA TACTICS

Bots: One-third of tweets about Brexit came from just 1% of Brexit-related Twitter Accounts
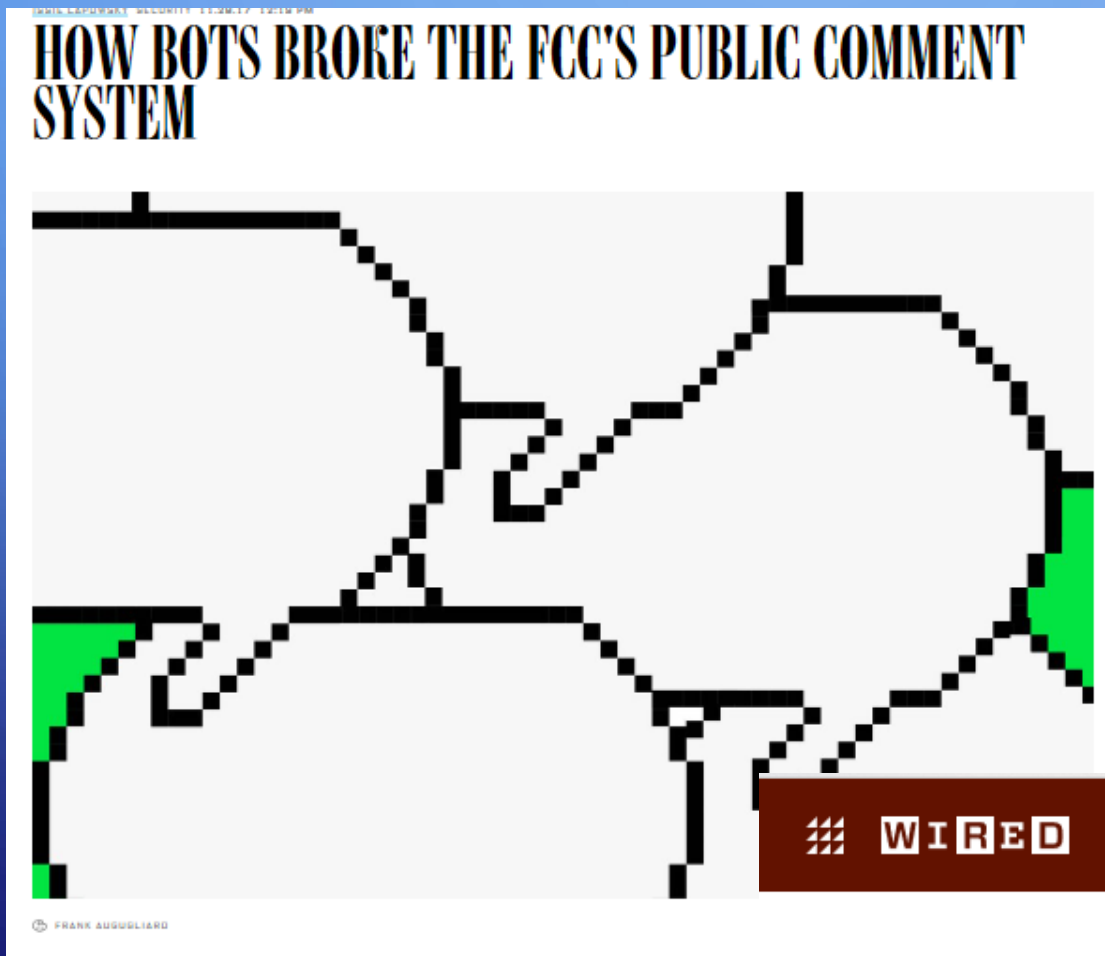
- 54% Leave
- 20% Stay

Study: Russian Twitter bots sent 45k Brexit tweets close to vote

Posted Nov 15, 2017 by *Natasha Lomas* (*@riptari*)

USE OF BOTS

HOW BOTS BROKE THE FCC'S PUBLIC COMMENT SYSTEM

FCC Net Neutrality Vote

Pew Research Center: >Half of comments from duplicate or temporary email addresses

Bots!

A FOCUS ON RUSSIA

Clinton Watts

Russian exploitation of social media

ATTACKING THE PUBLIC-PRIVATE GAP

Russian Internet Research Agency

<u>aka</u>
Troll Farm

St. Petersburg organization

100s of paid Kremlin Backers
having a quota of posts/day

AMPLIFYING THE KREMLIN MESSAGE

www.fancybear.net

U.S. and Canada Sports Officials' Secret Plot Revealed
2016-12-13

Greetings citizens of the world. We are Fancy Bears'.
We keep sharing anti-doping agencies' material with you. The leaked documents reveal that the U.S. and Canada have conspired against the International Olympic Committee before Rio 2016. They tried to further their political interests pretending to fight for clean sport.

Read more

U.S. Anti-Doping Agency Staff Emails
2016-10-06

Jan 26 media reporting: Dutch Intelligence monitored Fancy Bear – identifying the building and Kremlin-tied hackers – WHILE DNC hack was underway!!!

Dutch intelligence reportedly spied on Russian 'Cozy Bear' group linked to DNC hack

Report claims AIVD warned US officials about the threat

Best Evidence Yet: Fancy Bear is Kremlin Run

- hacked cameras and captured video

WHAT DOES IT ALL MEAN?

The cyber landscape has

in just 15 – 20 years

transitioned from web defacement

To identity theft and credit card fraud

To permanent presence hacking for longer term exploitation

To state actor attacks on critical infrastructure that threaten public safety

To a state of asymmetric warfare that includes turning open democracies against one another through propaganda messages and distribution platforms

MAKING MONEY FROM SPORTS ADVERTISING
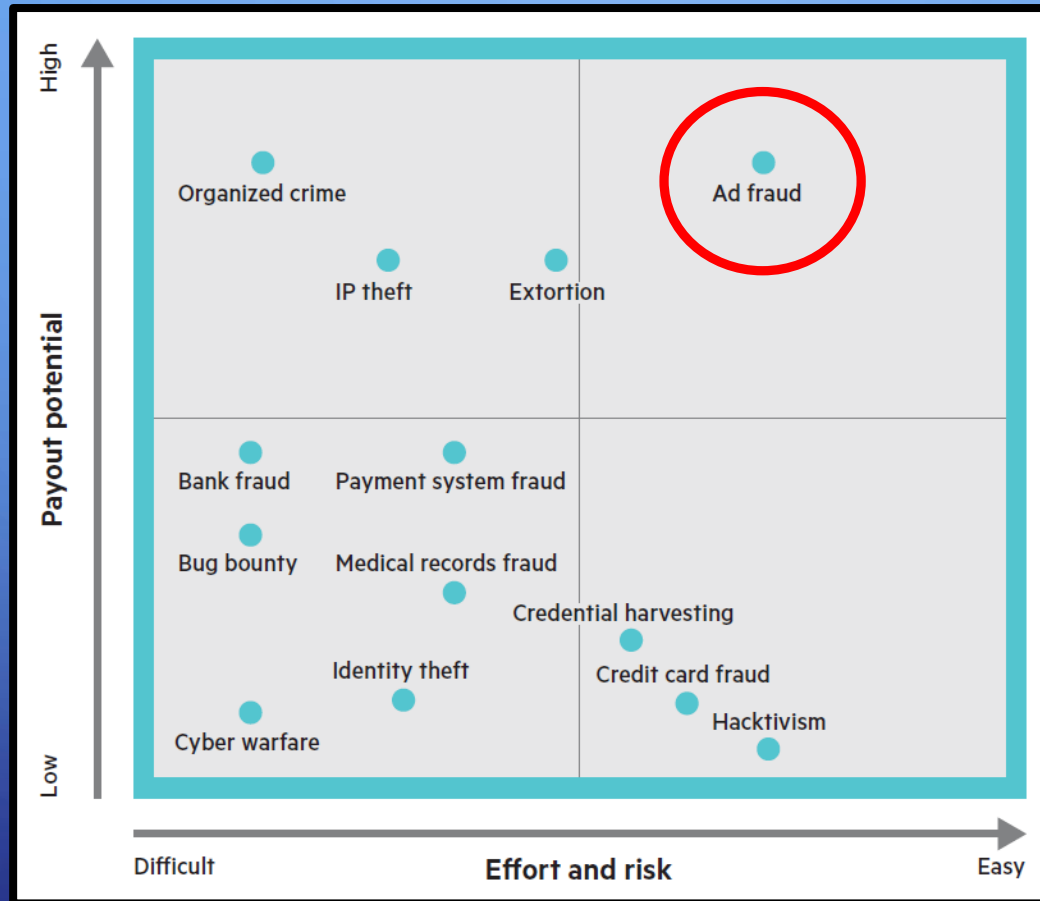
e.g. Methbot

CYBERCRIME ADOPTS SOCIAL MEDIA FOR TTP

CROWDSOURCING CTI

c-Watch Course

A hands-on, pre-apprentice program, conducted online and on-demand, that offers licenses and tools to learners for training in threat intelligence, social media intelligence, analysis, and information sharing operations, leading to a live, experiential collection, analysis and sharing operation – the Sports Capstone.

Our 2019 program for the Woman's World Cup has started: We still have a few more seats. Apply Now!

"We work with a team of analysts to hunt for potential cyber threats and share that information with our U.S. and international partners to reduce the potential for attacks and to increase understanding of hacker profiles and activities"

— C. Kolezynski

"Open communication made it possible for all participants to express their thoughts without reservations. You were made to feel valued. This is an excellent way to train and prepare individuals for the cybersecurity industry. The overall experience of working with such a diverse group as well as the challenging problems made for an enlightening and exhilarating experience."

Community Cyber Capacity / Adversary Strategy / Crowd-sourcing / ISAO Programs

→ The CrowdWatch network
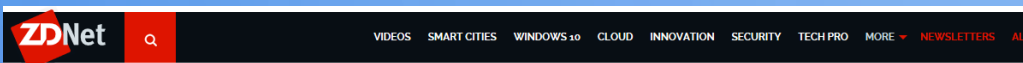
CROWDWATCH USE CASES
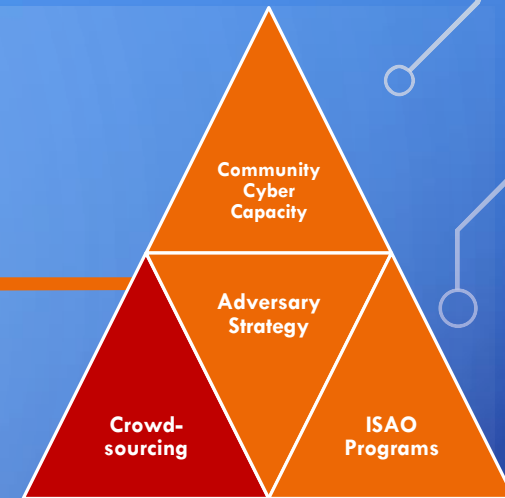
ISAO enabler

Community Workforce Program

Outsourced Analysis

EXPERIENCE REQUIRED

Getting started with a career in cybersecurity

With the ongoing and seemingly never-ending flood of cyberattacks, companies and governments the world over need experienced, skilled professionals to protect, defend, and strike back. But how do you get into the lucrative cybersecurity career? David Gewirtz has some advice.
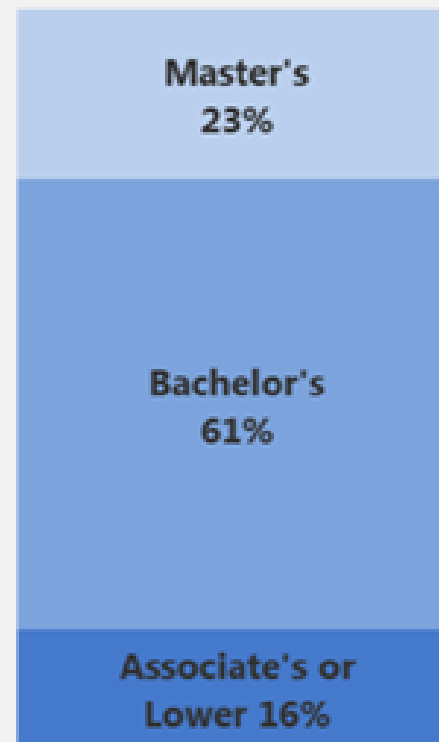
"Cybersecurity (and IT in general) are not the same as computer science. Traditional computer science can be helpful, but it's not the full story."

But there's also all the knowledge needed about how current systems work, which computer science doesn't necessarily prepare you for.
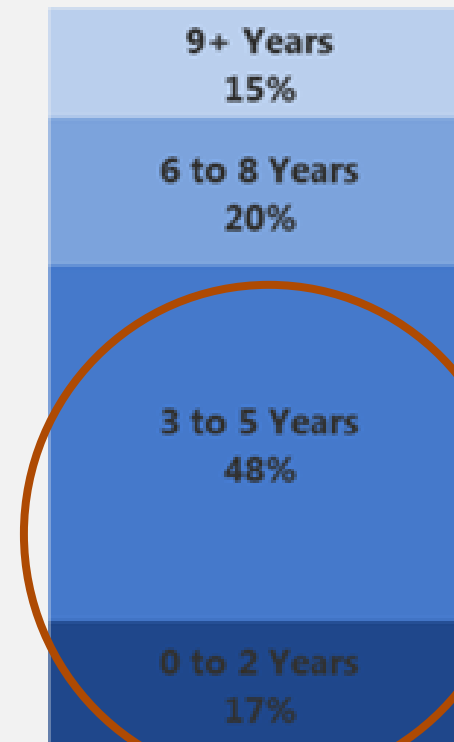
Hiring practice is also all over the map. Generally, cybersecurity jobs (like this one for a U.S. Navy Cyberwarfare engineer) require 4-year college degrees. Many others require experience and industry standard certifications.

Cybersecurity Postings

Requested Education Level	Minimum Experience
Master's 23%	9+ Years 15%
	6 to 8 Years 20%
Bachelor's 61%	3 to 5 Years 48%
Associate's or Lower 16%	0 to 2 Years 17%

SOURCE: BURNING GLASS TECHNOLOGIES

# C-Watch: FOUNDATIONAL KNOWLEDGE + SKILLS

KEY SKILLS & KNOWLEDGE

- ISAOs and national efforts

- Legal & Policy issues in cyber threat intelligence

- Social media intelligence

- Automated cyber threat exchange – STIX/TAXII

- SOC Operations & Collection Management

- Actionable intelligence

- Report Writing

THE HUNT COLLECT ▶ THE FUSION ANALYZE ▶ THE USE CASE REPORT
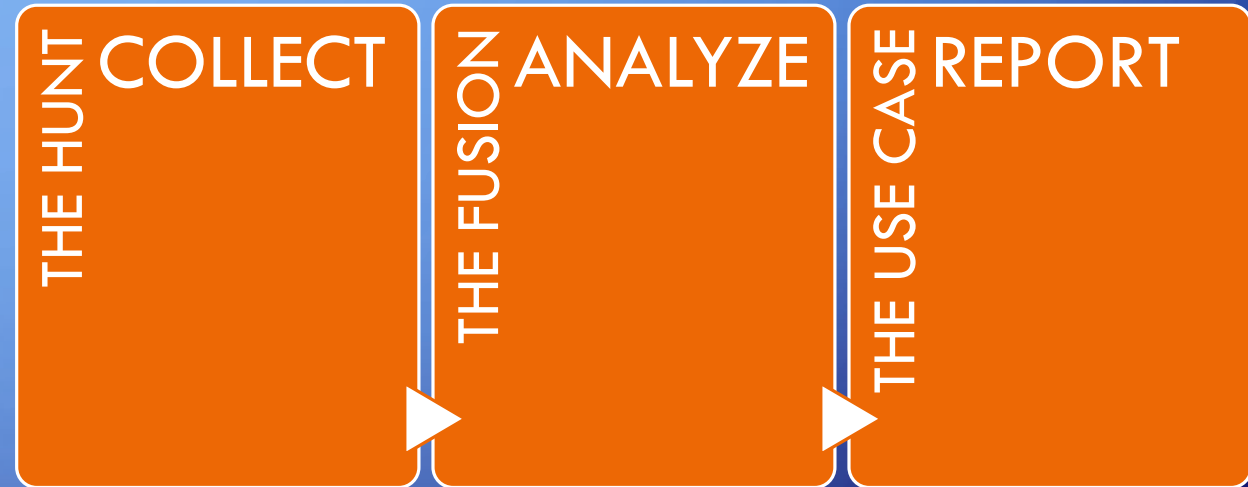
THE EXPERIENTIAL LEARNING COMPONENT

- Three Tracks

- Interdisciplinary Teams

- Mentor Oversight

- Capstone: Major Sport Event
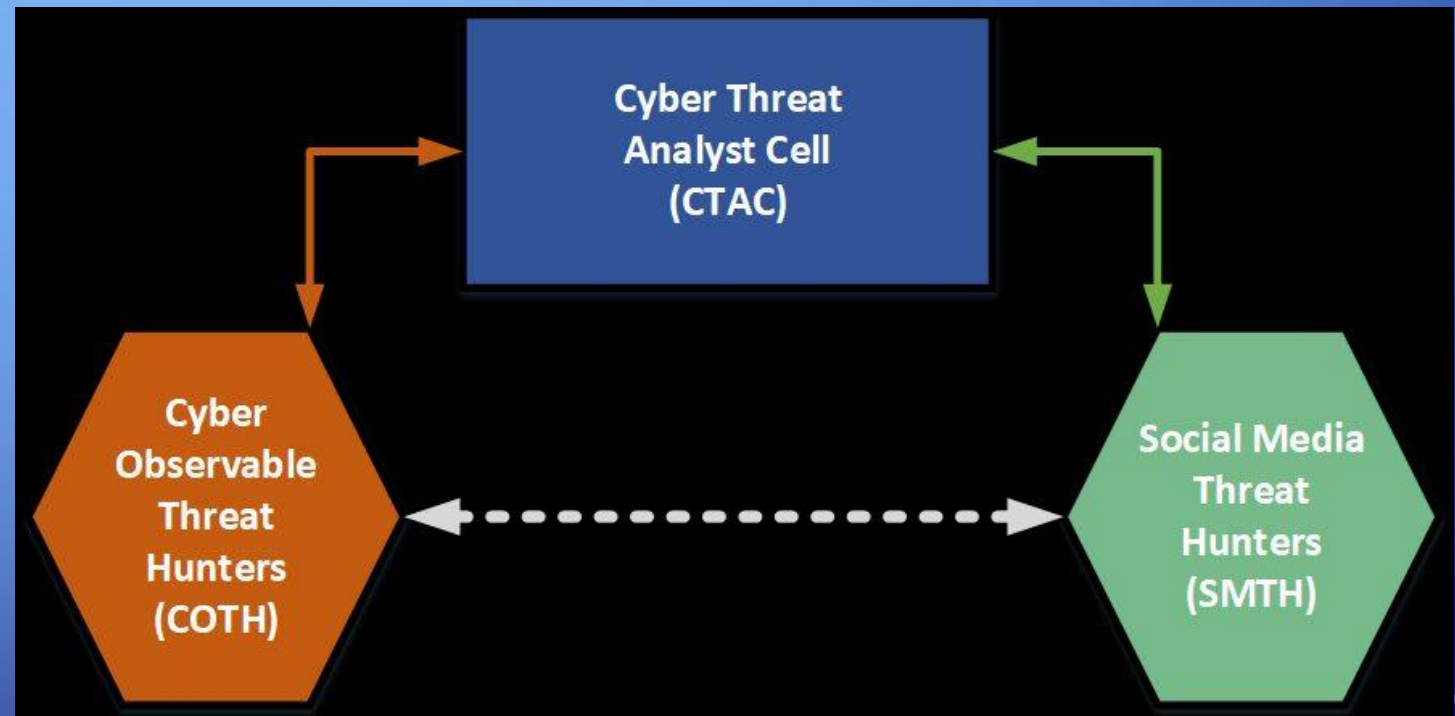
ACHIEVING THE ISAO MISSION

THE CHASM BETWEEN CYBER POLICY ... AND REALITY

THE GAP: A BUSINESS MODEL TO MAKE POLICY HAPPEN

the WHITE HOUSE

NATIONAL POLICY

Share information ... in as close to real time as possible.

* Executive Order 13691

THE GAP

c-Market FILLS THE GAP

We are 100% volunteers.**

** Quoted from a Community Cyber Program in a major US city

The New York Times

U.S.

A Cyberattack Hobbles Atlanta, and Security Experts Shudder

By ALAN BLINDER and NICOLE PERLROTH MARCH 27, 2018

THE WALL STREET JOURNAL.

Subscribe Now
$1 FOR 2 MONT

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine Search

TECH

Facebook Controversy: What to Know About Cambridge Analytica and Your Data

Facebook Inc.'s crisis centers on the company's most precious asset: the personal data of nearly two billion people
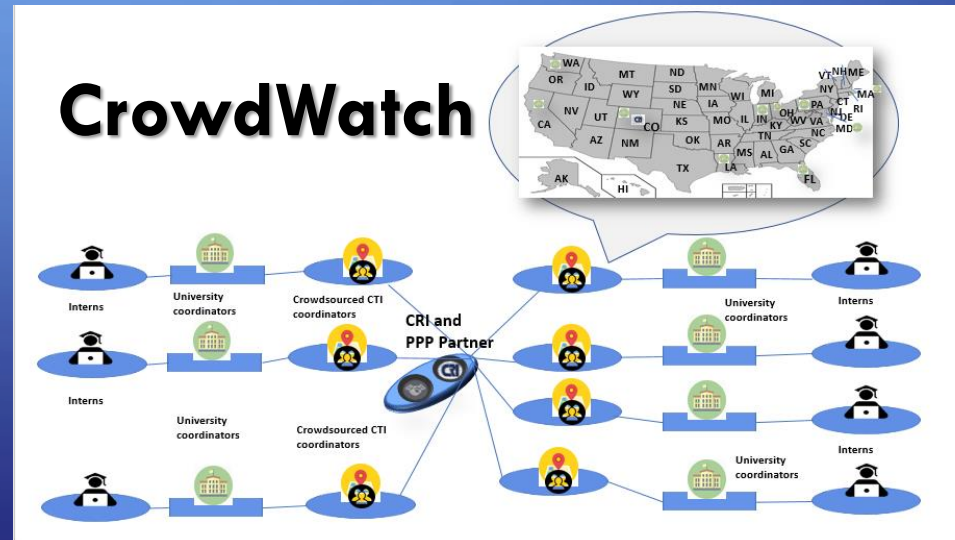
ISAOs are Part of the Solution

CrowdWatch enables ISAO Formation

JOBS, RESEARCH, AND STAFF AUGMENTATION

- PLACEMENT: 2016-19 INTERNS HIRED BY FIREEYE, USIC, SYMANTEC, BLUECOAT, FORENSICS COMPANY IN OHIO, ETC.

- OUTSOURCED RESEARCH AND STAFF AUGMENTATION TALKS: STATE, SPORT GROUPS, DHS

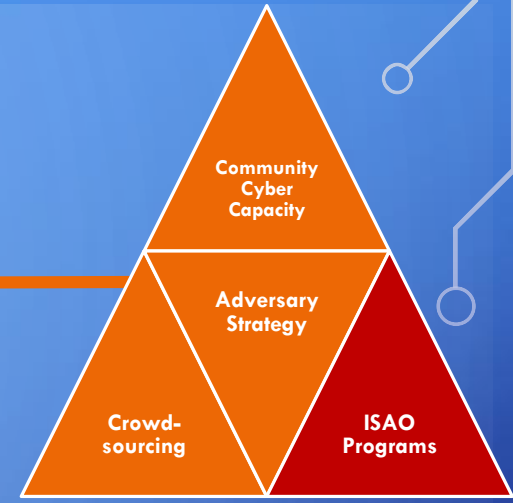- HSIN SPORTS-ISAO COMMUNITY OF INTEREST

- GRIDEX 2019

CrowdWatch

PRIVATE-PUBLIC PARTNERSHIP

"PARTNERSHIP" – WHAT IT MEANS

TOKYO OLYMPICS

C-WATCH ENROLLMENT 2020

STATE DEPARTMENT TIER 1 RESPONSE

EMBASSY REPORTING/FBI CYWATCH/DHS NCCIC

POST-SCRIPT

CALL TO ACTION

- Grassroots petition for Community Cyber Capacity Building

- 20+ signatories so far

- Specific Outcome: to add "Community Cyber Capacity" to the DHS National Critical Function List of the National Risk Management Center

QUESTIONS

www.cyberresilienceinstitute.org

www.sports-isao.org

www.c-market.us

Doug.depeppe@cyberresilienceinstitute.org