Hunt, Bourne and Ryan are Amateurs: 

*Using CTI to Save the World*

4OCT2023
Oregon Cyber Resilience Summit
MATT SINGLETON
Executive Strategist

- **25+ years:** Innovating at the intersection of security, education & digital transformation
- **State Government:** Former Chief Information Security Officer for the State of Oklahoma; Chief Operations Officer for the state’s IT division; State Chief Information Officer for Education
- **Higher Education:** Developed cybersecurity strategy and program for the University of Oklahoma system; Led innovation arm of OU IT; Professor of Cybersecurity
- **Education:** M.P.S. - Applied Intelligence, specializing in Cyber Intel, Homeland Security & Counterterrorism from Georgetown University; B.A. - Administrative Leadership from the University Of Oklahoma
- **Thought Leadership:** Momentum, National Association of State Technology Directors; Hunt, Bourne and Ryan are Amateurs, Threatday
AGENDA

- Art of Intelligence
- Cyber Threat Intelligence
- Pre/Post-Pandemic Dynamics
- CTI Application
“There are known knowns. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don't know. But there are also unknown unknowns. There are things we do not know we don't know.”

– Secretary of Defense Donald Rumsfeld, 12 February 2002
### Rumsfeld’s Quote

<table>
<thead>
<tr>
<th>There are known knowns</th>
<th>Al-Qaeda Example</th>
<th>Violent Crime Example</th>
<th>Cybersecurity Example</th>
<th>Intelligence Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are known unknowns</td>
<td>We know that al-Qaeda’s intent is to commit more terrorist attacks against the U.S. and U.S. interests.</td>
<td>We know there is an increase in violent crime using guns within a community.</td>
<td>We know MS-NRPC has a critical vulnerability that could allow the compromise of all AD.</td>
<td>The information we know must be consistently monitored and verified (i.e., “standing requirements”) to determine any changes in the status of the information we know.</td>
</tr>
<tr>
<td>There are unknown unknowns</td>
<td>We know that al-Qaeda has plans for future terrorist attacks, but the timing, method, and locations are unknown.</td>
<td>We know there is an increase in black market guns, but it is unknown who the supplier is, where the guns come from, or how the transactions are made.</td>
<td>We know other nations will try to influence US elections, but all strategies/tactics not yet known.</td>
<td>We know that we have intelligence gaps. Intelligence requirements, sources, and methods must be defined so that we may learn the currently unknown information.</td>
</tr>
<tr>
<td></td>
<td>If al-Qaeda has developed new alliances or new methods to commit attacks, these are unknown to us.</td>
<td>There are factors driving the increase in violence beyond the availability of guns; however, these other factors are unknown to us at the time.</td>
<td>Fraudsters will exploit eligibility programs during the pandemic; however, their targets and priorities are unknown to us.</td>
<td>Information must be collected from all sources and analyzed in an attempt to identify new threat information.</td>
</tr>
</tbody>
</table>
What is Threat Intel?

Gartner defines threat intelligence as “evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets.”

Internal Threat Intelligence – What we have:

- Discovered,
- Experienced, or
- Developed.

External Threat Intelligence - What we get from external data sources:

- Subscription feeds,
- Proprietary reports,
- In-depth analysis on threat actors, their tactics, techniques and procedures (TTP), and
- Often industry-specific.
Does Cyber Really Matter?

Cyber Meets Physical:
- Doxing
- Internet of Things (IoT)
- Smart Vehicles
- Social Media
- Security/Safety Systems
- Medical Systems

https://www.securitymagazine.com/articles/92518-the-need-for-cybersecurity-and-physical-security-convergence
Florida water treatment facility hack used a dormant remote access software, sheriff says

By Alex Marguerite, Eric Levenson and Amie Tee, CNN

Updated 5:33 PM ET, Wed February 10, 2021

Remote work leads to growing concerns over cybersecurity 02:24

(CNN) — A hacker who last week tried to poison a Florida city’s water supply used a remote access software platform that had been dormant for months, Pinellas County Sheriff Bob Gualtieri told CNN on Tuesday.

The cyber intruder got into Okanagan’s water treatment system twice on Friday — at 8 a.m. and 1:30 p.m. — through a dormant software called TeamViewer. The software hadn’t been used in about six months but was still on the system.

"How they got in, whether it was through a password or through something else, I can’t tell you that," said Gualtieri.


The New York Times

Cyber Attack Suspected in German Woman’s Death

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital’s computers. It could be the first fatality from a ransomware attack.

By Melissa Eddy and Nicole Perlroth

BERLIN — The first known death from a cyberattack was reported Thursday after cybercriminals hit a hospital in Düsseldorf, Germany, with so-called ransomware, in which hackers encrypt data and hold it hostage until the victim pays a ransom.

Pre-Pandemic

Hearing reset for Oklahoma woman in horse theft and animal cruelty case

BY JIM WILLIAMSON, AP
Published: Fri, March 5, 2016 12:05 AM
TEXARKANA, Ark. — A Prentice County, Okla., District Court
five horses.

TULSAWORLD
Timeline: The shooting of Terence Crutcher

Sept. 19, 2016: Police release video of shooting

The video in Nathaniel Rodriguez’s voice peaks as emergency workers load her husband onto a stretcher in the Warren Theatre parking lot.

“Pepsi! Is he OK? He doesn’t move?”

“They’ve got him and they’re going to take care of him,” an officer responds.

“She doesn’t move! You killed him! You killed him!”

Five law enforcement officers pinned Nathaniel Rodriguez, 44, to the ground and handcuffed him.

Cellphone video in fatal Moore, OK, Warren Theatre incident is made public

https://time.com/3951529/oklahoma-hoodie-ban/

Oklahoma could join a list of states where it is illegal to wear a hoodie in public, if a state senator’s proposed bill goes through.

Former Norman City Councilwoman believes she was intended target of attack

Post-Pandemic

Oklahoma County Commissioners are voting to restrict free speech TOMORROW MORNING 8/12 at 9AM. Check the resolution and areas they are restricting here: oklahomacounty.legistar.com/View.ashx?M=F&... They are attempting to prevent the protests at the courthouse and Jail, particularly at the courthouse.

Blumert 405.713.1501
Carrie.Blumert@oklahomacounty.org

Maughan: 405.713.1502
Brian@oklahomacounty.org

Calvey: 405.713.1503
Kevin.calvey@oklahomacounty.org

Contact the ok county commission relentlessly. There is no item of any comment. If there is no public input, there should be a vote. Raise hell @OkCountyMaughan @kevin.calvey

---

Frozen Cloud
November 17 at 15:38 PM

Please please bring everyone you know who supports and remember to give them credits and release those trying to do the right things!!

---

OCCUPY FOR PRISONERS

---

Riskline
@Riskline

UNITED STATES OF AMERICA: Protest against COVID-19 restrictions planned in Oklahoma City on 23 November | riskline.com

---

Midnight Rider @Qanon76 - 1h
If you're going to Washington D.C. to be a part of history on January 6th, comment below and share what state you'll be representing. Together We Win!!

---

Peaced Off Patriot @QonTwo
Repying to @Qanon76
Oklahoma will be there in force

---

CROWDSTRIKE
What is CTI Used For?

Do you utilize CTI for the following?

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat detection</td>
<td>88.5%</td>
</tr>
<tr>
<td>Threat prevention</td>
<td>76.8%</td>
</tr>
<tr>
<td>Threat response</td>
<td>71.7%</td>
</tr>
<tr>
<td>Threat mitigation</td>
<td>59.4%</td>
</tr>
<tr>
<td>Other</td>
<td>1.9%</td>
</tr>
</tbody>
</table>

What was “Other” in OK?

- Election Security
- Fraud
  - Unemployment Insurance
- Public Health/Safety
- OK-ISAC
  - Private Sector
  - State Agencies
  - Other States
  - K-12
  - Higher Ed
  - Municipalities
  - OK Information Fusion Center
  - Federal Agencies
What Could “Other” Be?

- More Fraud:
  - Temporary Assistance for Needy Families (TANF)
  - Supplemental Nutrition Assistance Program (SNAP)
  - Special Supplemental Nutrition Program for Women, Infants and Children (WIC)
  - Workers Compensation
- Sentiment
- Counterintelligence
- Counterterrorism