Civil Cyber Defense: Use Your Resources to Defend Nonprofits as they Combat Human Trafficking and Subvert Authoritarian Regimes

Tiffany Strauchs Rad, U.C. Berkeley

Austin Shamlin, Traverse Project

Defcon, August 11, 2023

Introductions

- **Tiffany Strauchs Rad** (BS, MA, MBA, JD): presented cybersecurity research – both technical and legal topics -- at many security conferences such as Black Hat USA, Black Hat Abu Dhabi, Defcon (17, 18, 19).
- My independent security research was listed as "Top 10 White Hat Hacks" by Bloomberg, and my critical infrastructure research was featured on the USA network series, “Mr. Robot.”
- I am a car hacker and do transportation infrastructure security consulting.
- I am an Adjunct instructor at the University of Maine and U.C. Berkeley teaching classes such as the "Citizen Clinic."

- **Austin Shamlin**: CEO and founder of Traverse Project, a nonprofit founded in 2023 to combat human trafficking networks.
- Served in the law enforcement and security industry for over 20 years, most recently serving as director of operations with an anti-human trafficking nonprofit under the Tim Tebow Foundation.
- I am professionally recognized geopolitical security subject matter expert on Haiti and has previously served as a special advisor to the Haitian Minister of Justice.
- Prior to Traverse Project, I served as a police executive with the D.C. government. Prior to that, I worked as a government contractor in Somalia, Afghanistan, Iraq, and Haiti.

What is Civil Cyber Defense?

- Definition of Civil Society: A community of citizens linked by common interests and collective activity.

- Definition of Cyber Defense: A coordinated act of resistance that guards information, systems, and networks from cyber attacks by implementing protective procedures.

Basic Operations of a High-Risk Clinic

- Citizen Clinic takes one “High Risk” cyber security consult client a semester and one “Low Risk”: assess students’ “risk appetite.”
- One client will be domestic and the other will either be international or have operations overseas.
- The first 6 weeks of the semester is academic work/technical training and the second 6 weeks the student-led teams meet weekly with clients.

Basic Operations of a High-Risk Clinic

- High-security Procedures: Use required tools and security protocols (such as no images, use VPNs, use aliases) or you cannot communicate with the client and might be asked to leave the class. Never put your work on your personal devices and final client work products are not stored on university servers.

- Strict NDAs: You cannot discuss the identity or work done for the client with family and students outside of the class – not even with other faculty at Berkeley apart from a few named instructors and directors.

How “High” is a “High Risk” Cybersecurity Clinic?

We discovered that one of our nonprofit clients had Pegasus (Spyware) two weeks before the end of the semester.

Lawsuit against NSO Group filed by the Knight First Amendment Institute at Columbia University: https://knightcolumbia.org/content/el-faro-journalists-knight-institute-sue-nso-group-over-spyware

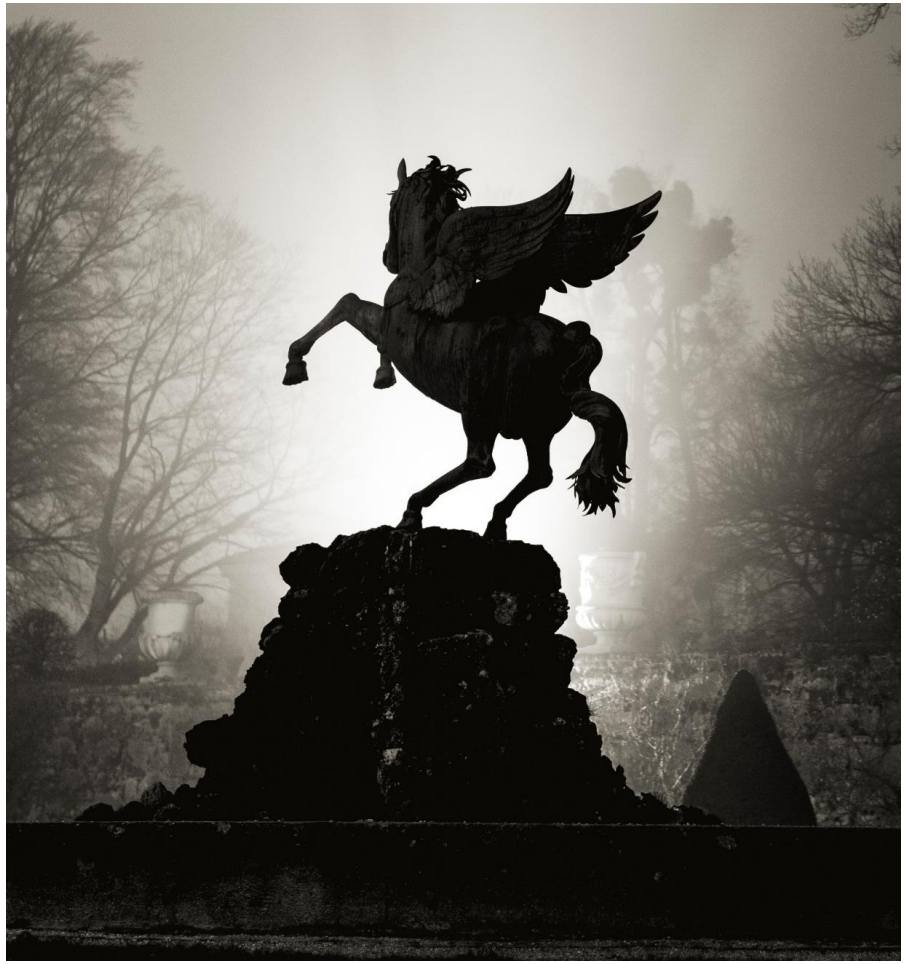


Photo by Hans-Peter Traunig on Unsplash

More than just cybersecurity undergraduate and graduate students…

- Computer Science
- Law
- Policy
- Data Analytics/Information Systems
- Business Administration
- Journalism

If you run a clinic, you do it all. In addition to cybersecurity training and consulting, don't forget…

- Privacy and Security: Maintaining aliases of "employees": no names, no images
- Creation of legal documents (NDAs, IP protection)
- Compliance: PCI-DSS,GDPR,HIPPA, California Consumer Privacy Act, etc.
- Human Relations: "hiring" and "firing"
- Marketing: Finding new clients, maintaining communications with old clients, observing current "employee" and client relations
- Information Technology support
- Language Translation
- Scoping Projects and Project Management/Managing Client Expectations
- Criminal Law: preserving evidence, "no hacking," Dark Web
- Psychological Well-Being of "employees"
- Insurance
- Review/Editing/Grading of final work products

Some Free (or almost free) Tools We Use

VPN:

https://www.expressvpn.com/

but check for leakage with https://www.dnsleaktest.com/

GhostPRTCL (self destructing remote access): https://www.ischool.berkeley.edu/projects/2021/ghostprtcl-ephemeral-remote-access-solution

https://leavenotrace.cloud/

Blocking Trackers:

https://panopticlick.eff.org/

https://privacybadger.org

Browsing:

Brave https://Brave.com

Tor: https://www.torproject.org

Tor for Cell Phones: https://guardianproject.info/apps/org.torproject.android/

Texting and Cell Phones:

https://signal.org/

Pastebin Search Tools:

https://pastebin.ga

https://redhunlabs.com/online-ide-search

Information Collection:

Maltego (free and paid versions): https://maltego.com

General field lookups (phone number, addresses, usernames). This is an OSINT resource guide by Michael Bazzell: https://inteltechniques.com/tools/index.html

Google Searches (search for Google exposed info)

https://www.exploit-db.com/google-hacking-database

Social Media:

https://yandex.com

https://instaloader.github.io/

https://github.com/Datalux/osintgram

https://github.com/JustAnotherArchivist/snscrape

Google Image search

Breach Info:

https://haveibeenpwned.com/

File Meta Data (photo geolocation, file author)

Exiftool https://exiftool.org

Public Asset Lookups (cameras, ICS, IOT devices…almost anything accidently put on the Internet)

Shodan https://www.shodan.io/dashboard (free and paid, free with an .edu email)

Website/IP:

Nmap: https://nmap.org

Cyber Threat Intel: Abuse.ch https://abuse.ch

DNS https://dnsdumpster.com

Citizen Clinic's Civil Cyber Defense Clients

- Refugee organization in Eurasia documenting war crimes and assisting displaced citizens
- Refugee organization providing health care to migrants in tent cities in Greece and documenting their migration stories and strife with nationalism in Europe.
- Two organizations promoting free speech and fighting disinformation created by authoritarian governments that are publishing false content to discredit and destabilize democratic governments.
- Central American organization assisting migrants fleeing organized crime and political unrest.
- American lawyers working out of tents in Mexican border towns taking "business" from human traffickers by encouraging legal migration processes.



Citizen Clinic's Civil Cyber Defense Clients

- Organization supporting lawyers prosecuting war criminals.
- Organization facing criminal prosecution of its directors because they promote democracy while under the surveillance of an authoritarian regime.
- Organization assisting indigenous people around the world in defending their land rights versus cartels or "eco-warriors" encroaching upon their land.
- Organization supporting an indigenous community in Asia who are trying to maintain their fishing territory challenging the Chinese government while they to bring food to their community.



Photo by Katie Moum on Unsplash

You will see and learn about difficult topics.

You will see immediate changes being made to secure your clients.

As the public face of your clinic, you might become the target of sophisticated adversaries with significant funding.

You will need to be as brave as your clients.

…and you’re going to love it

Want to start a Cybersecurity Clinic at your university?

Perfect timing! Google created a generous grant in June 2023 and may fund up to $1 million for new cybersecurity clinics.

> “Google, in collaboration with the Consortium of Cybersecurity Clinics, will support selected colleges, universities, and community colleges with up to $1M each to increase access and opportunities for students interested in pursuing careers in cybersecurity. In addition, recipients can access the Google Cybersecurity Certificate, Google Titan security keys, and student mentorship opportunities from Google.”

https://cyberclinics.withgoogle.com/

Current Cybersecurity Clinics in the U.S.



https://cybersecurityclinics.org/

Where to get started:

The Consortium of Cybersecurity Clinics
https://cybersecurityclinics.org/

Are you a university and want to start a clinic?

Contact Citizen Clinic:
https://forms.gle/W2H63E1EMDUDys7h8

or Trad@Berkeley.edu





Countering the human trafficking threat through data intelligence

OUR MISSION

To Identify, Map, and Disrupt transnational human trafficking networks with a nexus to the United States

OUR PARTNERS



























HUMAN TRAFFICKING IS THE FASTEST GROWING GLOBAL CRIME

HOW BIG OF AN ISSUE IS HUMAN TRAFFICKING?



GENERATES $150 BILLION/ANNUALLY

28 MILLION VICTIMS

29% MEN



71% WOMEN



1/4 CHILDREN



12 % GROWTH SINCE 2016



*International Labour Organization, Walk Free and the International Organization for Migration report 50 million people in slavery (2021). 28 million in forced labor and 22 million in forced marriages.

OUR STRATEGY

Identify

We use data to uncover patterns and trends to identify human trafficking networks and how they operate

Map

Once we have identified a network, we begin mapping the spiderweb of people, locations, and victims associated with that network

Disrupt

Once the network is mapped, we work with aw enforcement partners to develop a targeted strategy to disrupt their operations.

OUR METRICS

PRIMARY METRICS

- HT Networks Mapped
- Target Packages
- Evidence Packages

SECONDARY METRICS

- Victims Identified + Rescued
- Arrests and Prosecutions

PROJECTS

Operation WESTKEG

In April, Traverse started Op WESTKEG, which is focused on networks operating in Texas. We are currently mapping targets in major cities with a nexus to other U.S. cities and abroad. Once we identify target networks, our team will work with Texas state law enforcement to create a disruption strategy.

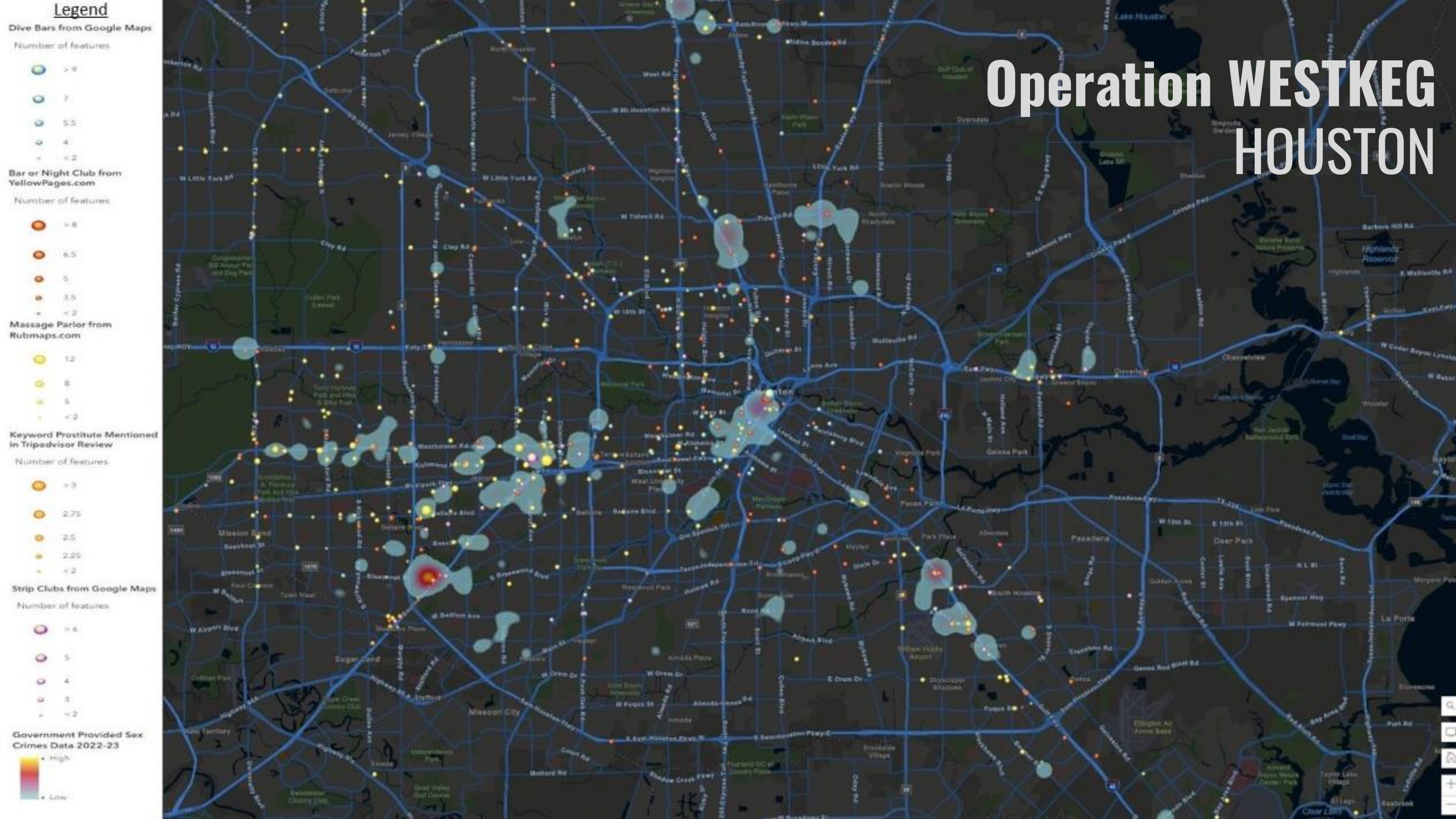
- Data collection and analysis
- HT network mapping

Project KEY

Sextortion is one of the fastest growing crises among teenagers in the U.S. Since 2022, there have been over 7,000 sextortion reports and claimed the lives of over a dozen victims to suicide. Traverse has created an awareness campaign that has already reached over 200,000 children ages 13-17.

- Reach 2M teenagers in 2023
- Push out to all major platforms

Operation WESTKEG
HOUSTON



Want to start a clinic? Want to help clinics and high-risk nonprofits?



Picture by Hanna Zhyhar on Unsplash

Contact us at Citizen Clinic: https://forms.gle/J2FWXf9MMzMeqbaB7

or Trad@Berkeley.edu

Contact us at Traverse Project: Austin.Shamlin@traverseproject.org

https://traverseproject.org/