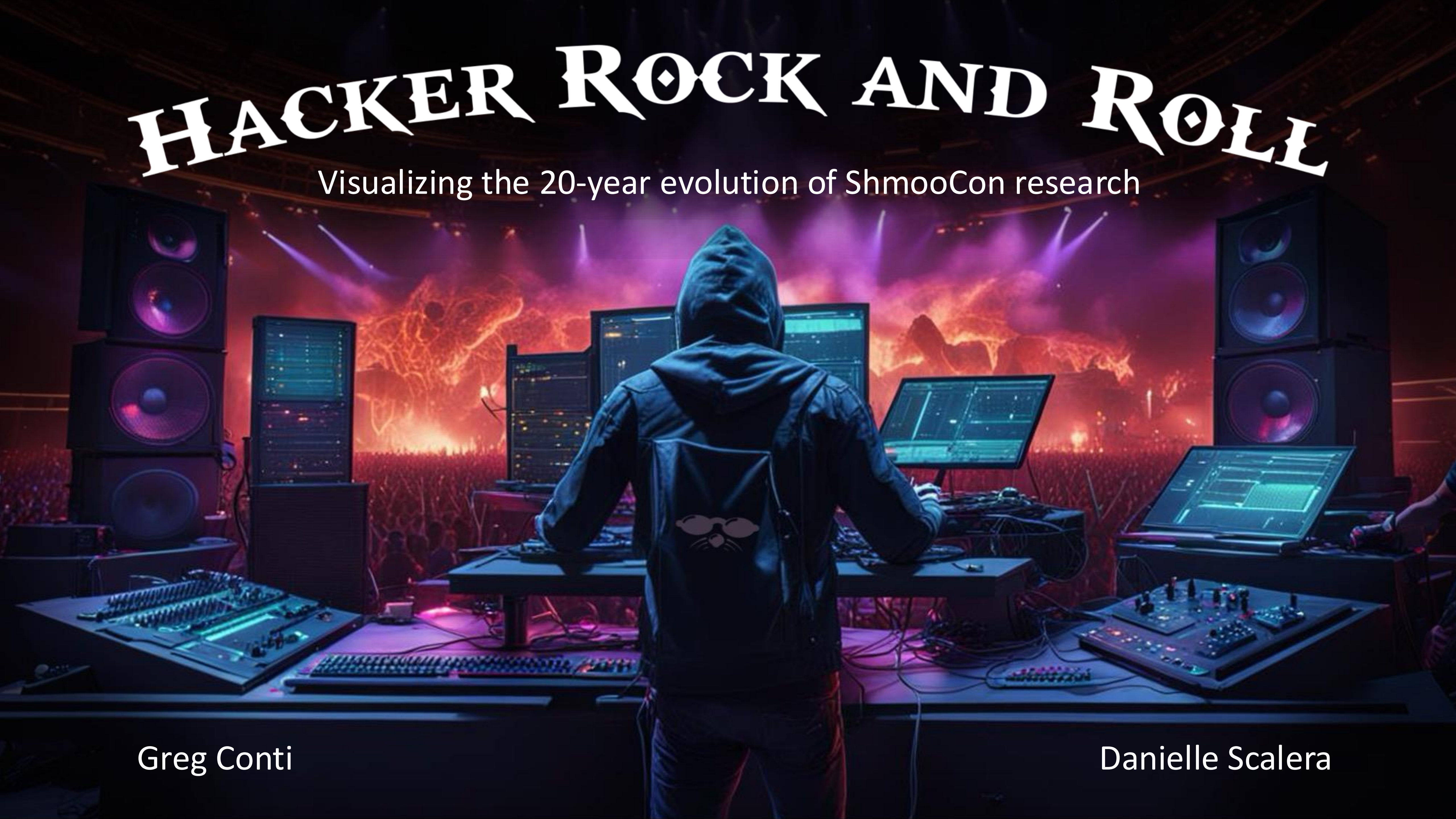
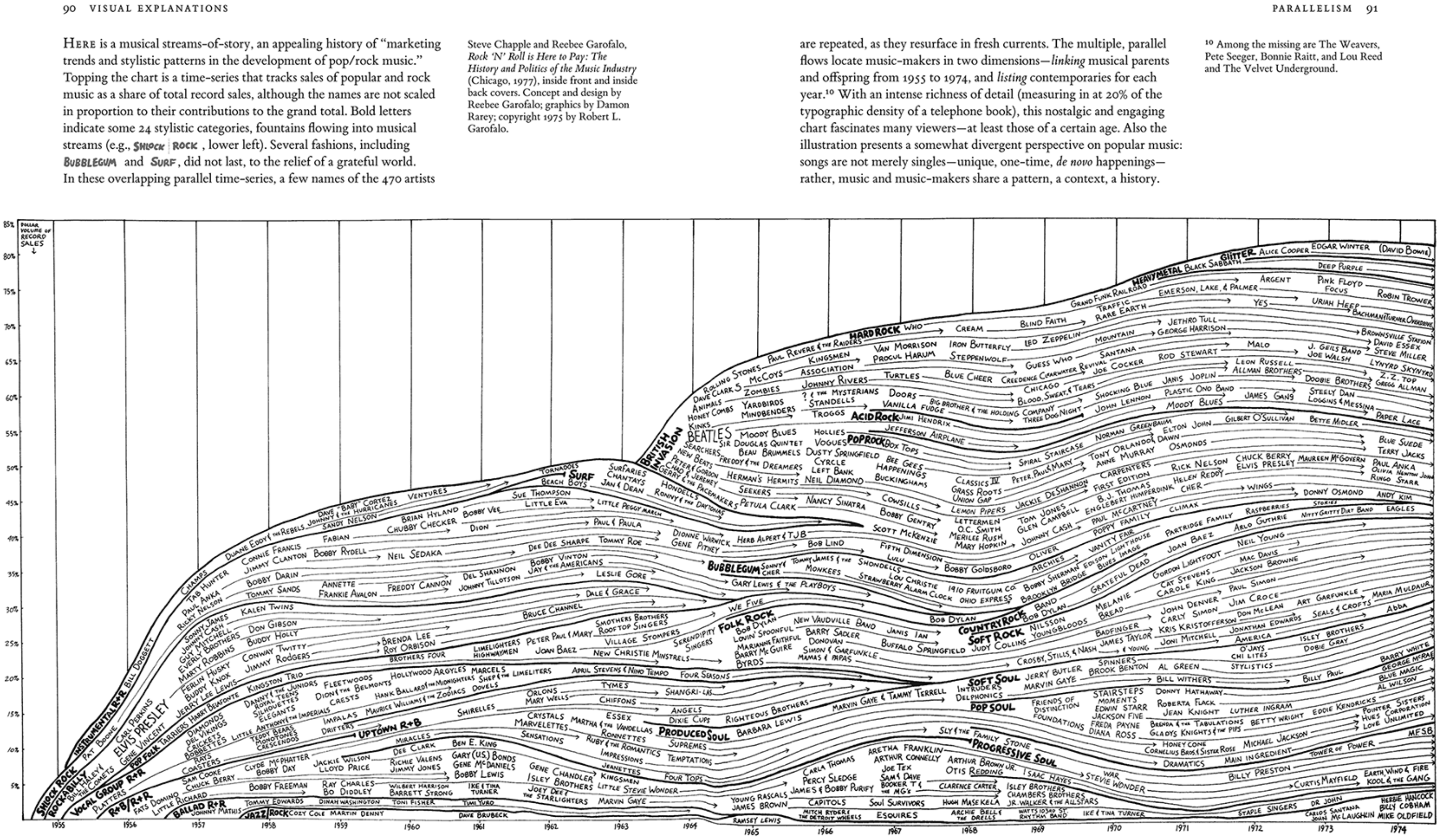


HACKER ROCK AND ROLL

Visualizing the 20-year evolution of ShmooCon research

Greg Conti

Danielle Scalera



90 VISUAL EXPLANATIONS

PARALLELISM 91

HERE is a musical streams-of-story, an appealing history of "marketing trends and stylistic patterns in the development of pop/rock music." Topping the chart is a time-series that tracks sales of popular and rock music as a share of total record sales, although the names are not scaled in proportion to their contributions to the grand total. Bold letters indicate some 24 stylistic categories, fountains flowing into musical streams (e.g., **SHLOCK ROCK**, lower left). Several fashions, including **BUBBLEGUM** and **SURF**, did not last, to the relief of a grateful world. In these overlapping parallel time-series, a few names of the 470 artists are repeated, as they resurface in fresh currents. The multiple, parallel flows locate music-makers in two dimensions—*linking* musical parents and offspring from 1955 to 1974, and *listing* contemporaries for each year.[10] With an intense richness of detail (measuring in at 20% of the typographic density of a telephone book), this nostalgic and engaging chart fascinates many viewers—at least those of a certain age. Also the illustration presents a somewhat divergent perspective on popular music: songs are not merely singles—unique, one-time, *de novo* happenings—rather, music and music-makers share a pattern, a context, a history.

Steve Chapple and Reebee Garofalo, *Rock 'N' Roll is Here to Pay: The History and Politics of the Music Industry* (Chicago, 1977), inside front and inside back covers. Concept and design by Reebee Garofalo; graphics by Damon Rarey; copyright 1975 by Robert L. Garofalo.

[10] Among the missing are The Weavers, Pete Seeger, Bonnie Raitt, and Lou Reed and The Velvet Underground.

https://reebee.net/rock-genealogy

https://www.edwardtufte.com/bboard/q-and-a-fetch-msg?msg_id=0002N4

whoami

Greg Conti

- Former West Point CS faculty
- Former NSA and US Cyber Command
- Frequent ShmooCon participant since ShmooCon 3
- Black Hat and Defcon trainer
- Principal at Kopidion

Danielle Scalera

- Pursuing a Master's in Cybersecurity at NJIT
- BS in Cybersecurity, Marist College
- Security researcher at Kopidion
- SummerCon '24 volunteer
- '22 Black Hat Training Assistant
- First time speaker ☺

KOPIDION™

The views in this talk are those of the speaker and do not reflect the policy or position of our current or former employers.

Dupont Circle, c.2005

How has ShmooCon research has evolved over time?

The opportunity

Over the last 20 years, ShmooCon has produced a wealth of innovative, high-impact and inspirational work.

The challenge

All that great work is not in an easily-analyzable format. We're missing out!

Our mission

Put all that data into a format that can be easily analyzed, share some results to inspire others and celebrate ShmooCon!

Dupont Circle, c.2050

Why do this?

- Understand how the hacker community innovates
- Find inspiration and new areas to explore
- Appreciate the magnitude of what has been achieved at ShmooCon

So what?

- Reduce plagiarism
- Amplify impact
- Increase appreciation for hacker community

Who cares?

- Hackers
- Non hackers
- The future

How are topics selected for ShmooCon?

Every conference is different, but here are some general guidelines

“Fast and Furious” Presentations meant to entertain, educate, and allow you to drive your point home quickly

“One Track Mind” Plenary presentations of broad technical interest

“Build It” Presentations about creating inventive software and hardware solutions

“Belay It:” Presentations about cutting edge defensive solutions to current problems

“Bring It On” Presentations with an open mind to technology and security related topics

Presentations related to these subjects are often considered appropriate:

- Technological evolution
- Breaches
- Threat actor activities
- Current events
- Cultural trends
- Review committee composition
- Cost and funding of research
- CFP language
- Infosec marketplace

Timeline: 2004 - 2014

Facebook created
Google went public

2004

2005

ShmooCon founded
and YouTube created

AWS launched

2006

2007

First iPhone, Netflix
video streaming,
Estonia cyber attacks

Bitcoin invented

2008

2009

Operation Aurora,
4G/LTE

First iPad, U.S. Cyber
Command, Snowmaggedon,
NASDAQ penetrated,
Stuxnet

2010

2011

Amazon Fire tablet,
DARPAs Cyber Fast
Track

Edward Snowden
Target hack, Mandiant
APT 1 report

2013

2014

Google Cardboard,
Tesla autopilot, OPM
hack, Sony Pictures
hack

Special thanks to Jack Daniel for permission to use the 2010 Snowmageddon photo

Timeline: 2015 – present

2015

Windows 10, Amazon Alexa & Echo, DNC hack, CSI: Cyber

2016

AlphaGo, Oculus Rift and Pokemon Go

2019

CRISPR-Based Diagnosis, foldable devices

2020

mRNA Vaccines, 5G networks, Google and IBM make advances toward practical quantum computing,COVID-19 lockdown :(

2021

No ShmooCon, Colonial Pipeline

Colonial Pipeline Company

2022

NEURALINK

~~August 29, 1997~~
November 30th 2022, Chat GPT 3 released for public use, Log4j, Neuralink, Ukraine Invasion

2023

ChatGPT 4 released March 14th 2023

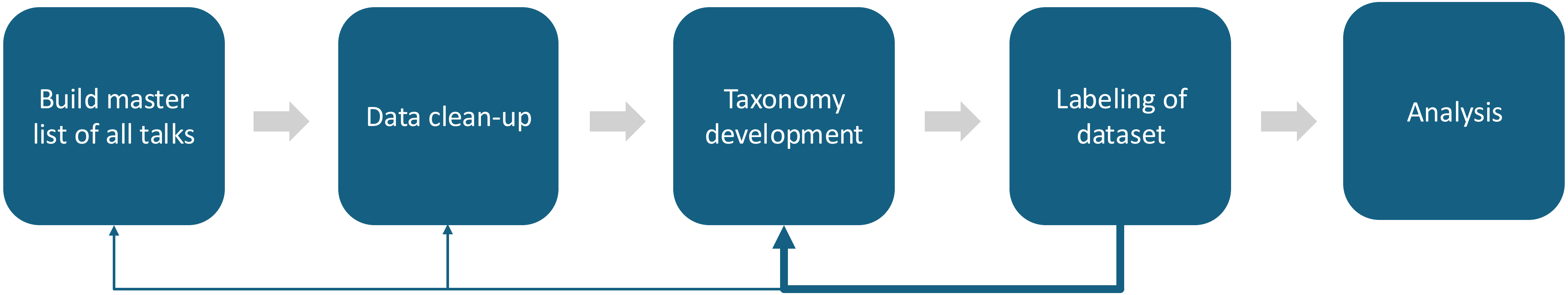
ChatGPT

2024

Apple Vision Pro released, SpaceX caught Falcon 9 booster, Midnight Blizzard, US telecom hack

2025

Last ShmooCon



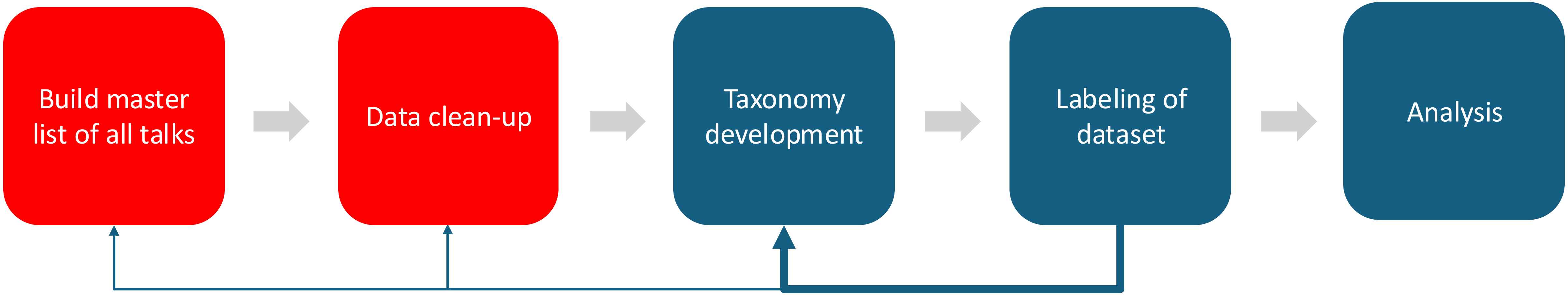
Build master list of all talks

Data clean-up

Taxonomy development

Labeling of dataset

Analysis



Build master list of all talks

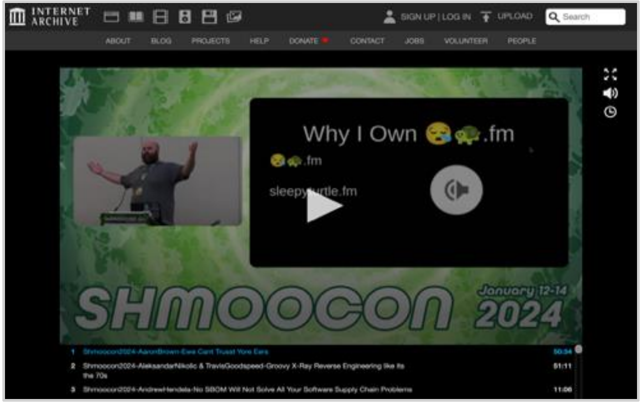
Data clean-up

Taxonomy development

Labeling of dataset

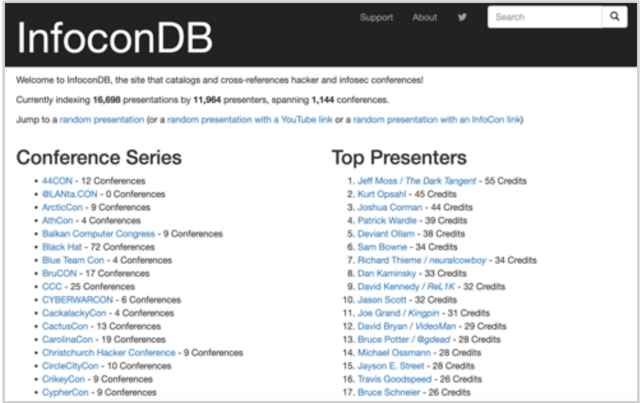
Analysis

Data sources



1 Shmoocon2024-AaronBrown-Ewe Cant Truust Yore Ears 50:34
2 Shmoocon2024-AleksandarNikolic & TravisGoodspeed-Groovy X-Ray Reverse Engineering like its the 70s 51:11
3 Shmoocon2024-AndrewHendela-No SBOM Will Not Solve All Your Software Supply Chain Problems 11:06

archive.org



Welcome to InfoconDB, the site that catalogs and cross-references hacker and infosec conferences!

Currently indexing **16,698** presentations by **11,964** presenters, spanning **1,144** conferences.

Jump to a random presentation (or a random presentation with a YouTube link or a random presentation with an InfoCon link)

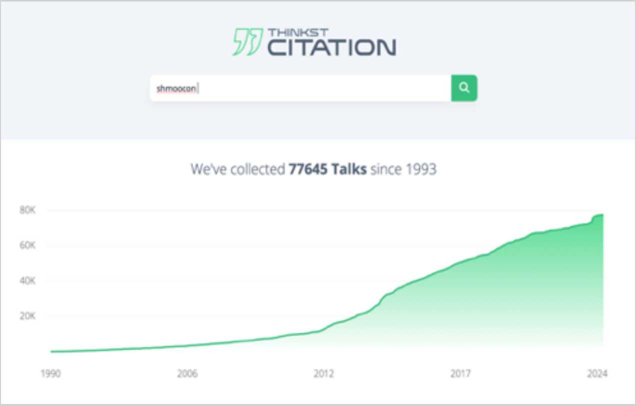
Conference Series

- 44CON - 12 Conferences
- @LANta.CON - 0 Conferences
- ArcticCon - 9 Conferences
- AthCon - 4 Conferences
- Balkan Computer Congress - 9 Conferences
- Black Hat - 72 Conferences
- Blue Team Con - 4 Conferences
- BruCON - 17 Conferences
- CCC - 25 Conferences
- CYBERWARCON - 6 Conferences
- CackalackyCon - 4 Conferences
- CactusCon - 13 Conferences
- CarolinaCon - 19 Conferences
- Christchurch Hacker Conference - 9 Conferences
- CircleCityCon - 10 Conferences
- CrikeyCon - 9 Conferences
- CypherCon - 9 Conferences

Top Presenters

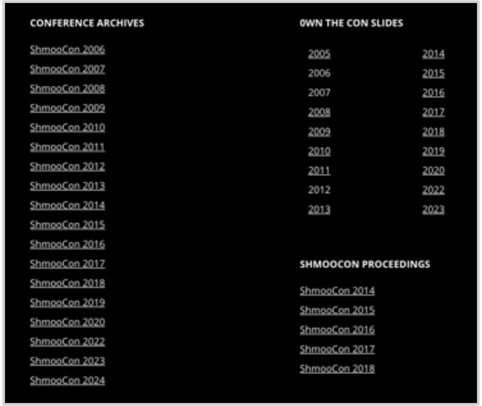
1. Jeff Moss / *The Dark Tangent* - 55 Credits
2. Kurt Opsahl - 45 Credits
3. Joshua Corman - 44 Credits
4. Patrick Wardle - 39 Credits
5. Deviant Ollam - 38 Credits
6. Sam Bowne - 34 Credits
7. Richard Thieme / *neuralcowboy* - 34 Credits
8. Dan Kaminsky - 33 Credits
9. David Kennedy / *ReL1K* - 32 Credits
10. Jason Scott - 32 Credits
11. Joe Grand / *Kingpin* - 31 Credits
12. David Bryan / *VideoMan* - 29 Credits
13. Bruce Potter / *@gdead* - 28 Credits
14. Michael Ossmann - 28 Credits
15. Jayson E. Street - 28 Credits
16. Travis Goodspeed - 26 Credits
17. Bruce Schneier - 26 Credits

infocondb.org



We've collected **77645 Talks** since 1993

citation.thinkst.com



CONFERENCE ARCHIVES

- ShmooCon 2006
- ShmooCon 2007
- ShmooCon 2008
- ShmooCon 2009
- ShmooCon 2010
- ShmooCon 2011
- ShmooCon 2012
- ShmooCon 2013
- ShmooCon 2014
- ShmooCon 2015
- ShmooCon 2016
- ShmooCon 2017
- ShmooCon 2018
- ShmooCon 2019
- ShmooCon 2020
- ShmooCon 2022
- ShmooCon 2023
- ShmooCon 2024

0WN THE CON SLIDES

2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2022
2023

SHMOOCON PROCEEDINGS

- ShmooCon 2014
- ShmooCon 2015
- ShmooCon 2016
- ShmooCon 2017
- ShmooCon 2018

shmoocon.org

InfoCon
Home | FAQ | Supporters | RSS Feeds | .onion | Forums | Mastodon
InfoCon.org
Hacking Conference Archive
Type to search...

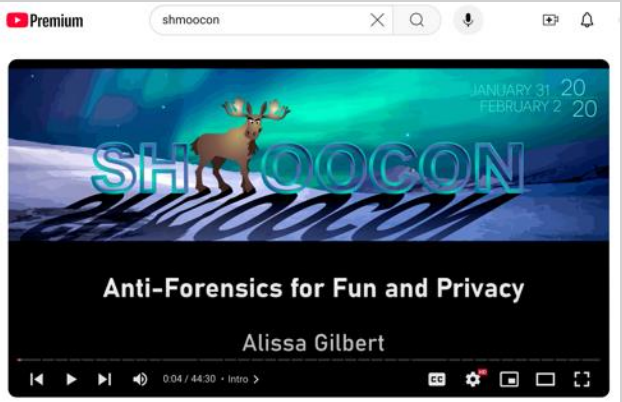
Conventions Collection

Description of things to be said about the content which is noted above in the header.

/cons/

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
0xcon/	-	2024 Jul 26 07:39
2600/	-	2024 Jul 26 07:43
44CON/	-	2024 Jul 26 05:08
8dot8/	-	2024 Sep 18 10:15

infocon.org



YouTube

Photography is not allowed at ShmooCon without permission of everyone in frame. I blurred out the crowd from this anonymous photo submission of my talk (thank you, BTW!) to get around that rule. By my incredibly humble estimation, there were approximately 7500 attendees at my talk.

Blogs & articles

Error reduction

What we found

- Lots of hard work by volunteers
- Gaps and variations in the archive sites
- Cancellations and replacement speakers
- Videos not recorded or posted
- Typos, varying abbreviations and transcriptions
- “Everything”

Our approach

- Triangulation
- Iterative review

What did we find (continued)?

Long titles (SC17)

HACK THE, er… HEMISPHERE! How we (legally) broadcasted hacker content to all of North America (and beyond) using an end-of-life geosynchronous satellite

Edgy titles (SC13)

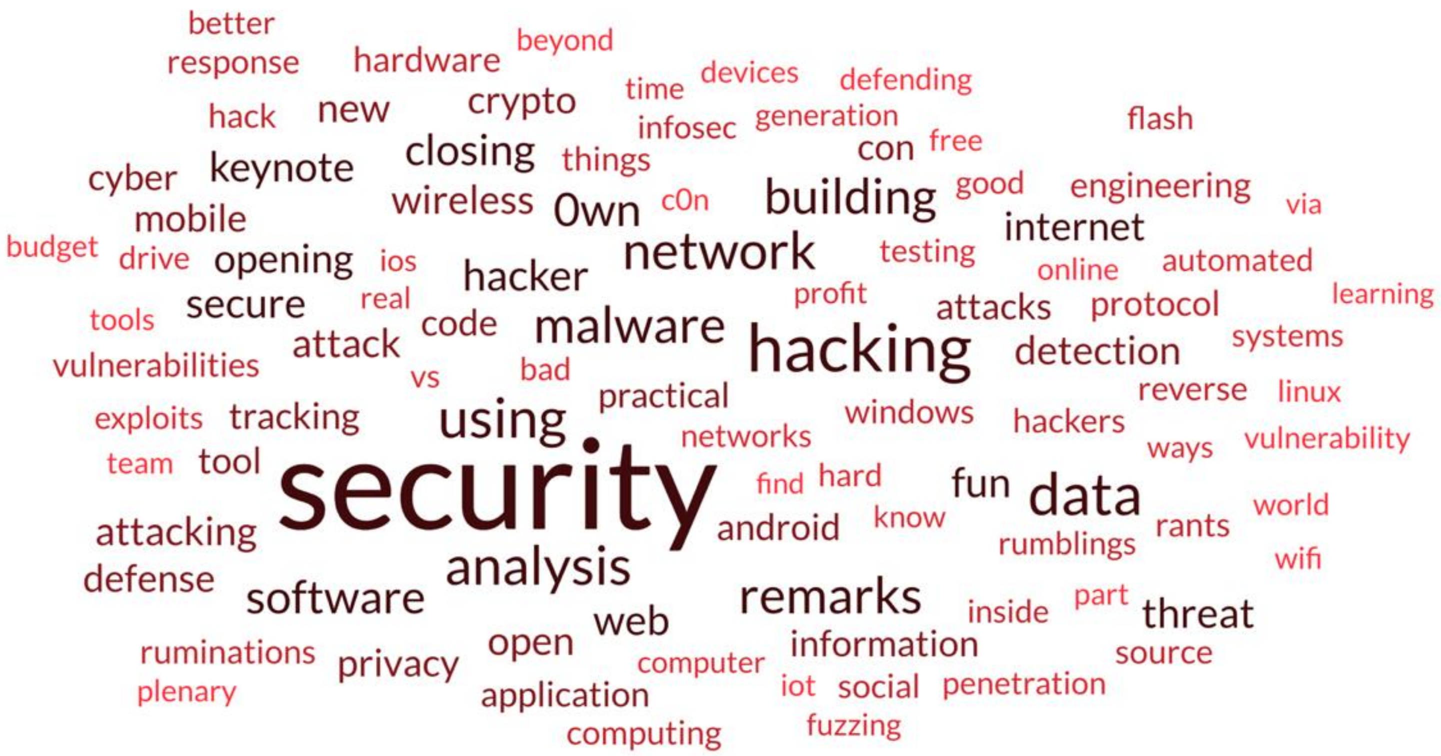
Can a Drunk Person Authenticate Using Brainwaves? #NotAlcoholicsJustResearchers

Hard to discern titles (SC7)

Defending against Targeted attacks, using Duck tape, Popsicle Sticks and Legos

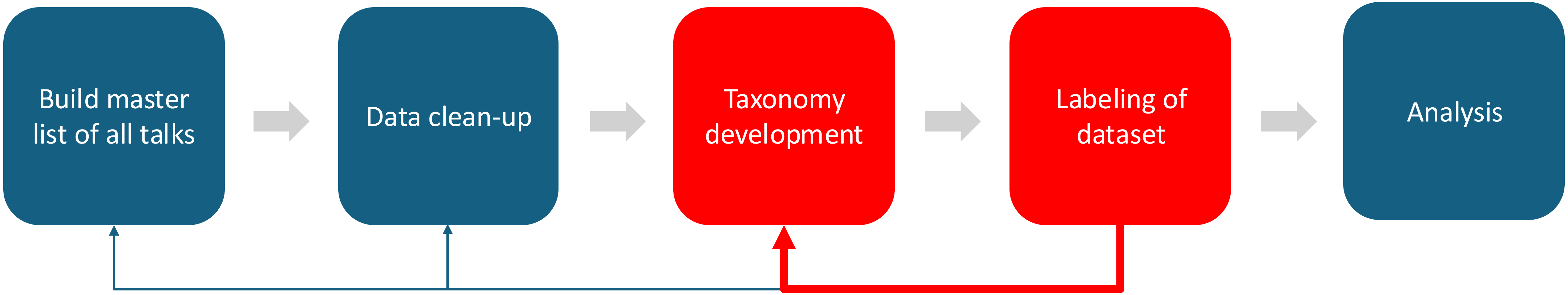
Bruce Potter stand-up (SC1, SC2, SC3, SC4, SC5, SC6, SC7, SC8, SC9, SC10, SC11, SC12, SC13, SC14, SC15, SC16, SC17, SC18, SC19, SC20)

Talk titles over the years



Most frequent words in ShmooCon talk titles

- Collected **2005-2025**
- Except 2021 (Covid)
- **801** talks in dataset
- All plenary and primary track talk title and year
- From *A Blackhat's Tool Chest* to *Zoom 0-Day: How Not to Handle a Vulnerability Report*
- Future: add Firetalks and speakers



Build master list of all talks

Data clean-up

Taxonomy development

Labeling of dataset

Analysis

Creating a strawman taxonomy

Art and science

- It’s a bit of both

Emergent vs comprehensive approach

- The directions taken and why

Goals

- 100% coverage of ShmooCon talks
- Each talk should have a single logical home
- Extensible
- Serve as starting point for refinement and formal validation

Taxonomy – ideation and related work

Hacker and InfoSec

Black Hat Briefings tracks, InfoSec certification categories, conference CFPs, existing metadata (keywords), *The Best of 2600* index

Professional societies

IEEE Taxonomy, ACM Computing Classification System, CISSP Domains

Military

Frameworks (intelligence (1,2), electronic warfare, effects based operations, etc.)

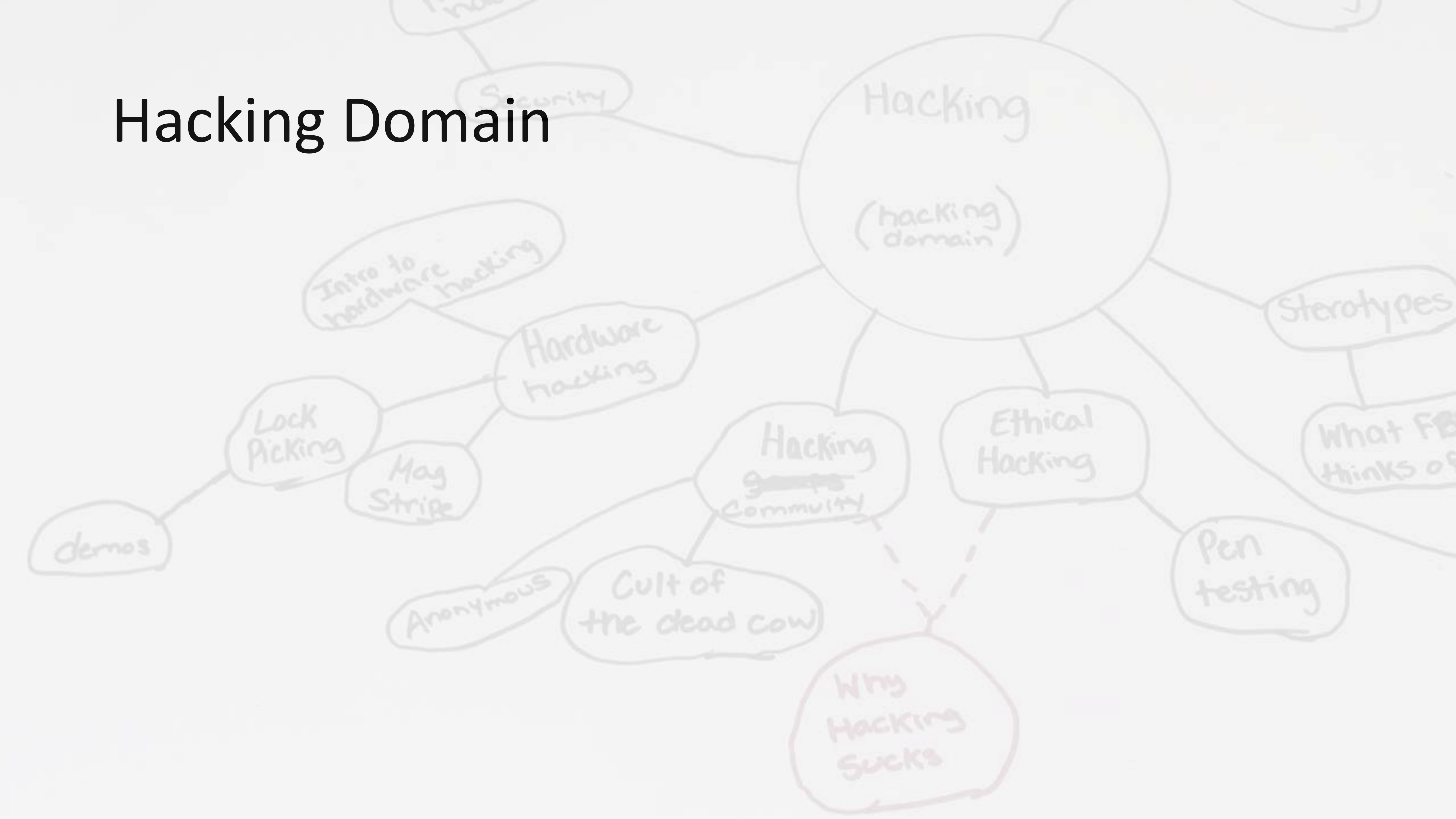
Industry, government, and non-profits

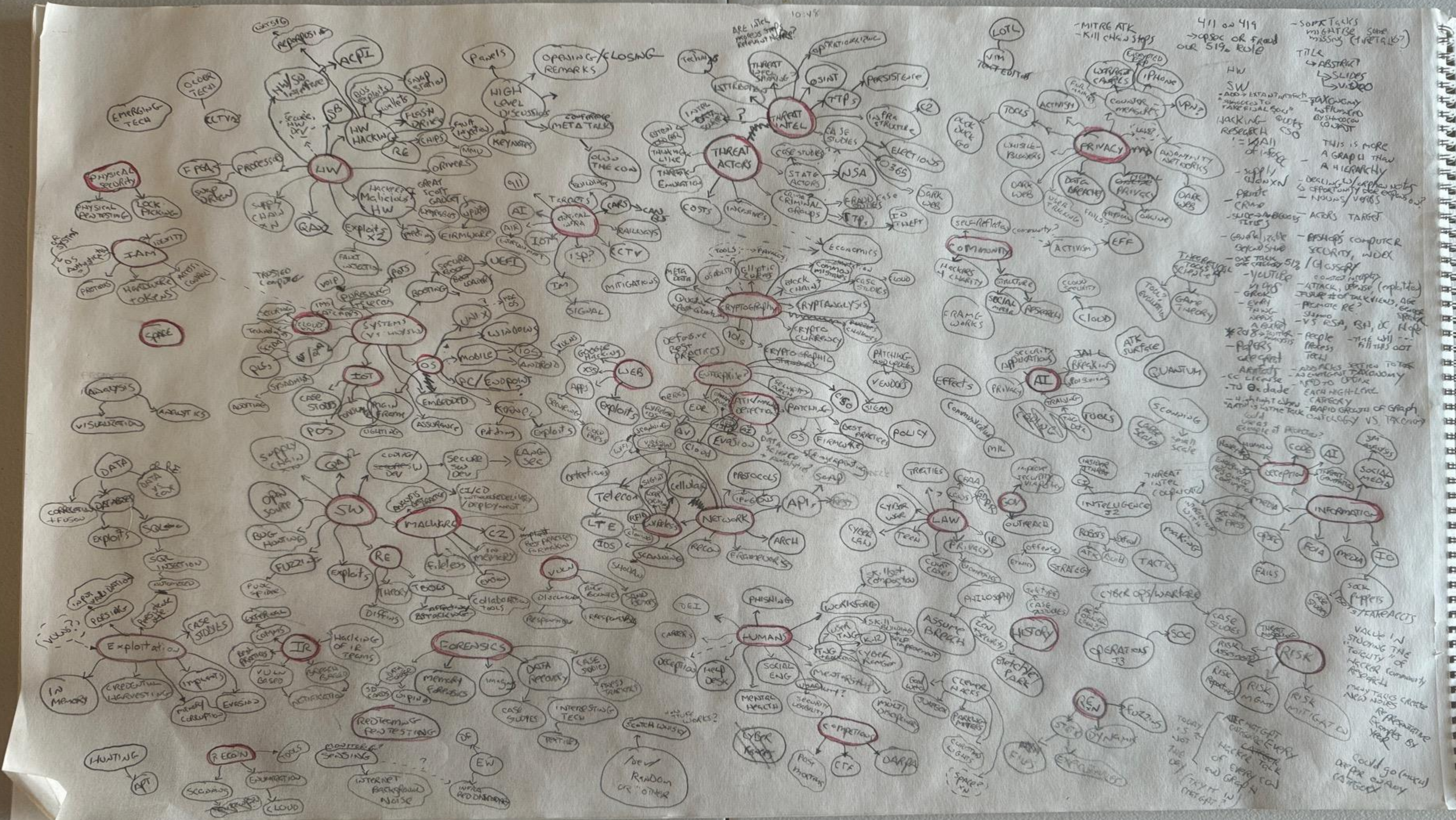
MITRE ATT&CK, DISARM Framework (IO), SPARTA Framework (Space), LM Kill Chain, European Commission Cybersecurity Taxonomy

Academia

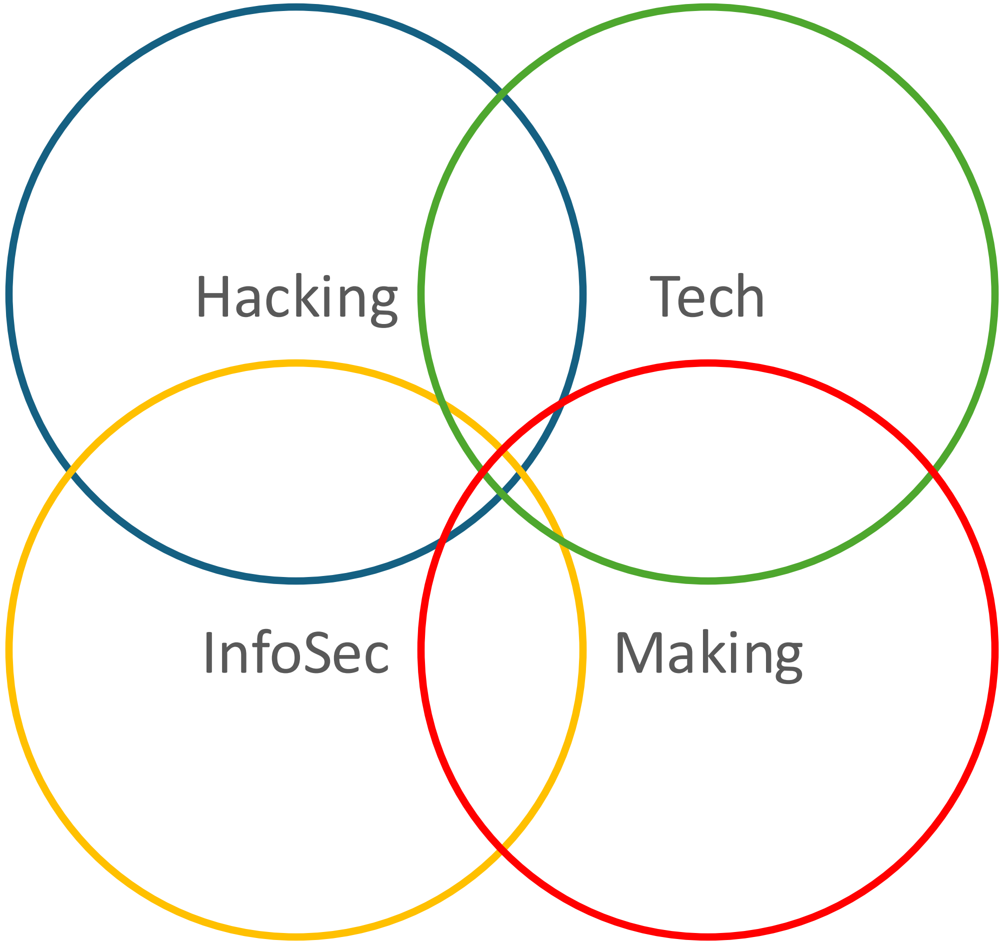
Textbook indices and glossaries, "Hacker taxonomy" publications, academic disciplines (law, philosophy, math, CS, EE, CSE, …)

Hacking Domain



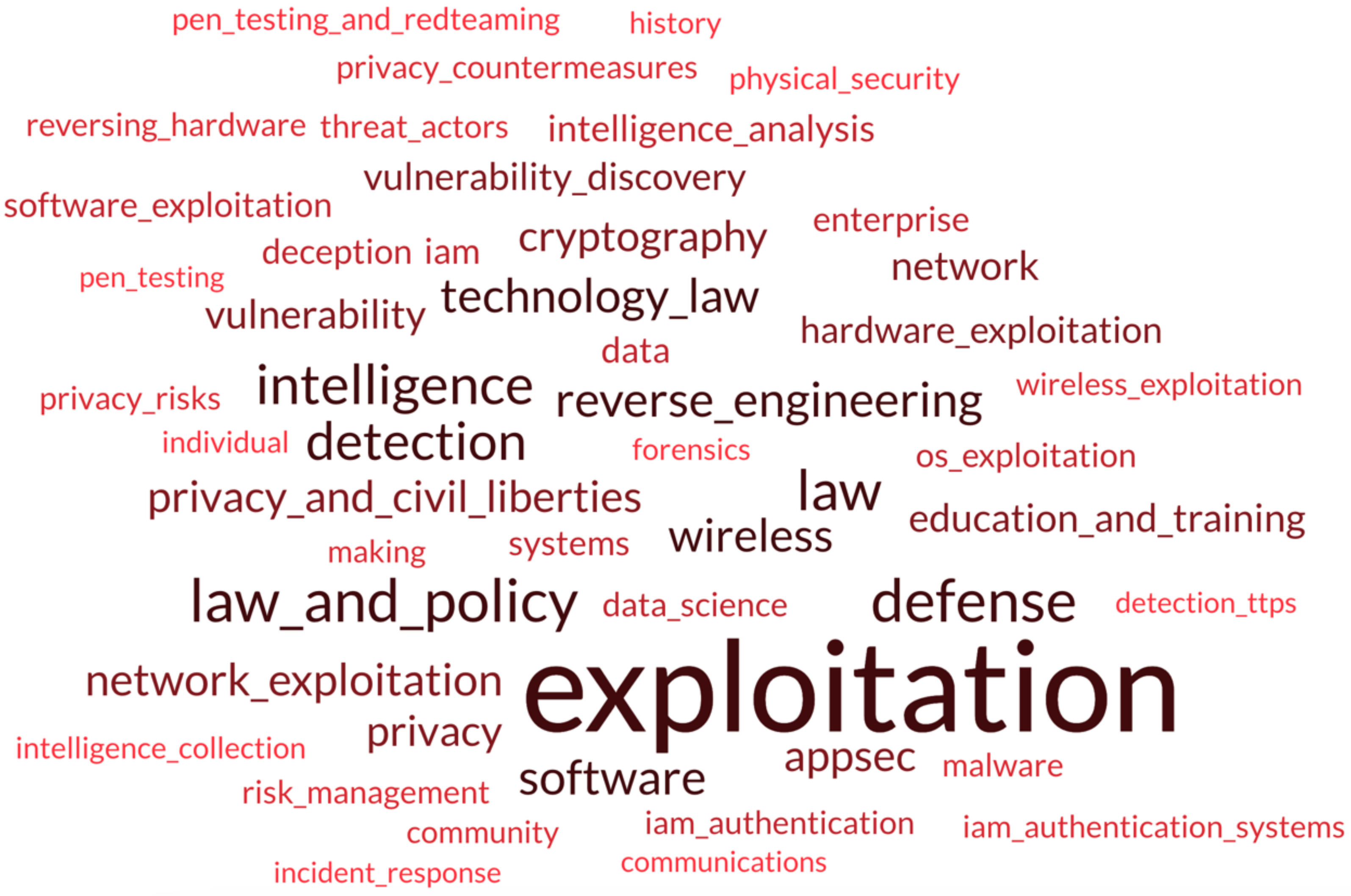

10:48
HW
HARDWARE
HW HACKING
ACPI
REPURPOSING
HW/SW INTERFACE
SB
BUS EXPLOITS
WALLETS
SNAP STATION
FLASH DRIVES
CHIPS
RE
MMU
DRIVERS
PROCESSORS
FPGA
SUPPLY CHAIN
RAM
HACKER MALICIOUS HW
GREAT SCOTT GADGETS
FIRMWARE
EXPLOITS X2
EMERGING TECH
OLDER TECH
CCTV
PHYSICAL SECURITY
PHYSICAL PENTESTING
LOCK PICKING
IAM
IDENTITY
OS AUTHENTICATION
PROTOCOLS
HARDWARE TOKENS
ACCESS CONTROL
SPARE
ANALYSIS
ANALYTICS
VISUALIZATION
PANELS
OPENING/CLOSING REMARKS
HIGH LEVEL DISCUSSIONS
CONFERENCE META TALK
KEYNOTES
OWN THE CON
BUILDINGS
911
AI
CRITICAL INFRA
CARS
CAN
RAILWAYS
CCTV
ISP?
IOT
ICS
SIGNAL
MITIGATIONS
SYSTEMS (VS HW/SW)
TRUSTED COMPUTING
VOIP
BOOTING
SECURE BOOT
UEFI
UNIX
MAC OS
WINDOWS
OS
MOBILE
IOS
ANDROID
PC/ENDPOINT
EMBEDDED
KERNEL
PATCHING
EXPLOITS
ASSURANCE
IOT
CASE STUDIES
POS
LIGHTING
CLOUD
THREAT INTEL
THREAT ACTORS
OSINT
TTPS
PERSISTENCE
OPERATIONALIZING
ATTRIBUTION
THREAT INFO SHARING
INFRASTRUCTURE
CASE STUDIES
ELECTIONS
O365
STATE ACTORS
NSA
CRIMINAL GROUPS
FRAUD
ID THEFT
DARK WEB
COSTS
INCENTIVES
THREAT EMULATION
THINKING LIKE
ARE INTEL PROCESS STEPS RELEVANT HERE?
ECONOMICS
CRYPTOGRAPHY
ELLIPTIC CURVES
BLOCK CHAIN
COMMON MISTAKES
CASE STUDIES
CRYPTANALYSIS
CRYPTO CURRENCY
QUANTUM / POST QUANTUM
DEFENSIVE BEST PRACTICES
CRYPTOGRAPHIC STANDARD
ENTERPRISE
PATCHING AND UPDATES
VENDORS
SECURITY ARCH
ANTIVIRUS / DETECTION
EDR
EVASION
PATCHING
BEST PRACTICES
FIRMWARE
POLICY
SIEM
CISO
WEB
GOOGLE HACKING
XSS
APPS
EXPLOITS
LOTL
VIM
TEXT EDITOR
PRIVACY
COUNTER MEASURES
IPHONE
ENCRYPTED EMAIL
VPN?
ACTIVISM
TOOLS
WHISTLE BLOWERS
DATA BREACHES
DIGITAL PRIVACY
ANONYMITY NETWORKS
DARK WEB
USER TRACKING
FAILS?
PHYSICAL
ONLINE
COMMUNITY
SELF-REFLECTION
ACTIVISM
EFF
HACKERS 4 CHARITY
STRUCTURE
SOCIAL MEDIA
RESEARCH
FRAMEWORKS
CLOUD SECURITY
CLOUD
THEORETICAL TOOLS & SCIENCE
TOOLS EVOLUTION
GAME THEORY
ATK SURFACE
QUANTUM
AI
JAIL BREAKING
POISONING
TRAINING
TOOLS
EFFECTS
COMMUNICATION
MIL
SCANNING
LARGE SCALE
SMALL SCALE
SUPPLY CHAIN
QA
CODING / SW DEV
SECURE SW DEV
LANG SEC
CI/CD
OPEN SOURCE
SW
MALWARE
C2
FILELESS
IN MEMORY
BUG HUNTING
FUZZING
EXPLOITS
RE
THEORY
TOOLS
DIFFING
COLLABORATION TOOLS
DATA
DATABASES
SQL
SQL INJECTION
CORRELATION + FUSION
EXPLOITS
INPUT VALIDATION
PARSING
VULNS?
EXPLOITATION
CASE STUDIES
IN MEMORY
CREDENTIAL HARVESTING
IMPLANTS
MEMORY CORRUPTION
EVASION
IR
HACKING OF IR TEAMS
VULN
DISCLOSURE
RESPONSIBLE
BUG BOUNTIES
FORENSICS
MEMORY FORENSICS
IMAGING
DATA RECOVERY
CASE STUDIES
INTERESTING TECH
REDTEAMING PENTESTING
HUNTING
APT
RECON
TOOLS
SENSING
INTERNET BACKGROUND NOISE
EW
DF
ENUMERATION
CLOUD
SCOTCH WHISKEY
/DEV/ RANDOM OR "OTHER"
NETWORK
TELECOM
CELLULAR
LTE
WIRELESS
RFID
IDS
SCANNING
RECON
FRAMEWORKS
PROTOCOLS
IPV6
APIS
ARCH
SHODAN
DETECTION
HUMANS
PHISHING
WORKFORCE
SKILLSET COMPOSITION
DEI
CAREERS
DECEPTION
HELP DESK
SOCIAL ENG
MENTAL HEALTH
MENTORSHIP
SKILL BUILDING
CYBER RANGES
COMPETITIONS
POST MORTEMS
CTF
DARPA
CYBER KNIGHTS
LAW
TREATIES
CFAA
GDPR
CYBER WAR
CYBER LAW
TEEN
PRIVACY
COURT CASES
GOV
OUTREACH
PHILOSOPHY
ASSUME BREACH
ZEN SECURITY
HISTORY
BLETCHLEY PARK
CLEVER HACKS
CHRISTMAS LIGHTS
SPACE
RE
STATIC
DYNAMIC
FUZZING
INTELLIGENCE J2
THREAT INTEL
INSIDER THREAT
ROBOTS
CYBER OPS/WARFARE
CASE STUDIES
OPERATIONS J3
SOC
TACTICS
STRATEGY
DECEPTION
CODE
AI
SOCIAL MEDIA
INFORMATION
OPSEC
FOIA
MEDIA
IO
SOCK PUPPETS
BOTS/FAKE ACCTS
FAILS
RISK
THREAT MODELING
RISK ASSESSMENT
RISK REPORTING
RISK MGMT
RISK MITIGATION
-MITRE ATK
-KILL CHAIN STEPS
411 ON 419
-> OPSEC OR FRAUD
OUR 51% RULE
-SOME TALKS MIGHT BE SOME MISSING (FIRE TALKS?)
TITLE
-> ABSTRACT
-> SLIDES
-> VIDEO
HW
SW
-TAXONOMY INFLUENCED BY SHMOOCON CONTENT
HACKING QUOTES
RESEARCH CSO
THIS IS MORE A GRAPH THAN A HIERARCHY
-SUPPLY CHAIN
-PRIVATE
-CRIME
-DEALING W/ ORPHAN NOTES
-> OPPORTUNITY FOR EXPANSION?
-NOUNS/VERBS
-ACTORS TARGET
-GENERALIZABLE BEYOND SHMOO
-BISHOP'S COMPUTER SECURITY, INDEX / GLOSSARY
-YOUTUBE VIDEOS
-GROK
-EVERY THING NEEDS A BUCKET
-ATTACK, DEFENSE, (EXPLOITATION)
-FUTURE # OF TALK VIEWS, AGE
-PROMOTE RE?
-VS RSA, BH, DC, HOPE
*2018 -> TWITTER ANALYSIS
-PAPERS
-PEOPLE PROCESS TECH
-TIME WILL FILL THIS OUT
-CC LICENSE
-TO DECADE
-ADDRESS SECTION TO TAX
-AN EMERGENT TAXONOMY
-NEED TO OPTIMIZE EACH HIGH-LEVEL CATEGORY
-RAPID GROWTH OF GRAPH
-ONTOLOGY VS. TAXONOMY
TODAY IS NOT THE DAY
ALL CAN NOT GET CATEGORIZED EVERY HACKER TALK OF EVERY CON EVER GROWN (TRY IT IN CATEGORY?)
VALUE IN STUDYING THE "TOPOLOGY" OF HACKER COMMUNITY RESEARCH
MANY TALKS CREATE NEW NODES
REPRESENTATIVE EXAMPLES BY YEAR
COULD GO (MUCH) DEEPER ON ANY CATEGORY

Taxonomy - design decisions



- Depth vs. breadth
- Target vs. technique
- InfoSec vs. military framing
- Original vs. current terminology
- Generic vs. precise
- Large and/or reoccurring subcategories

Taxonomy Summary

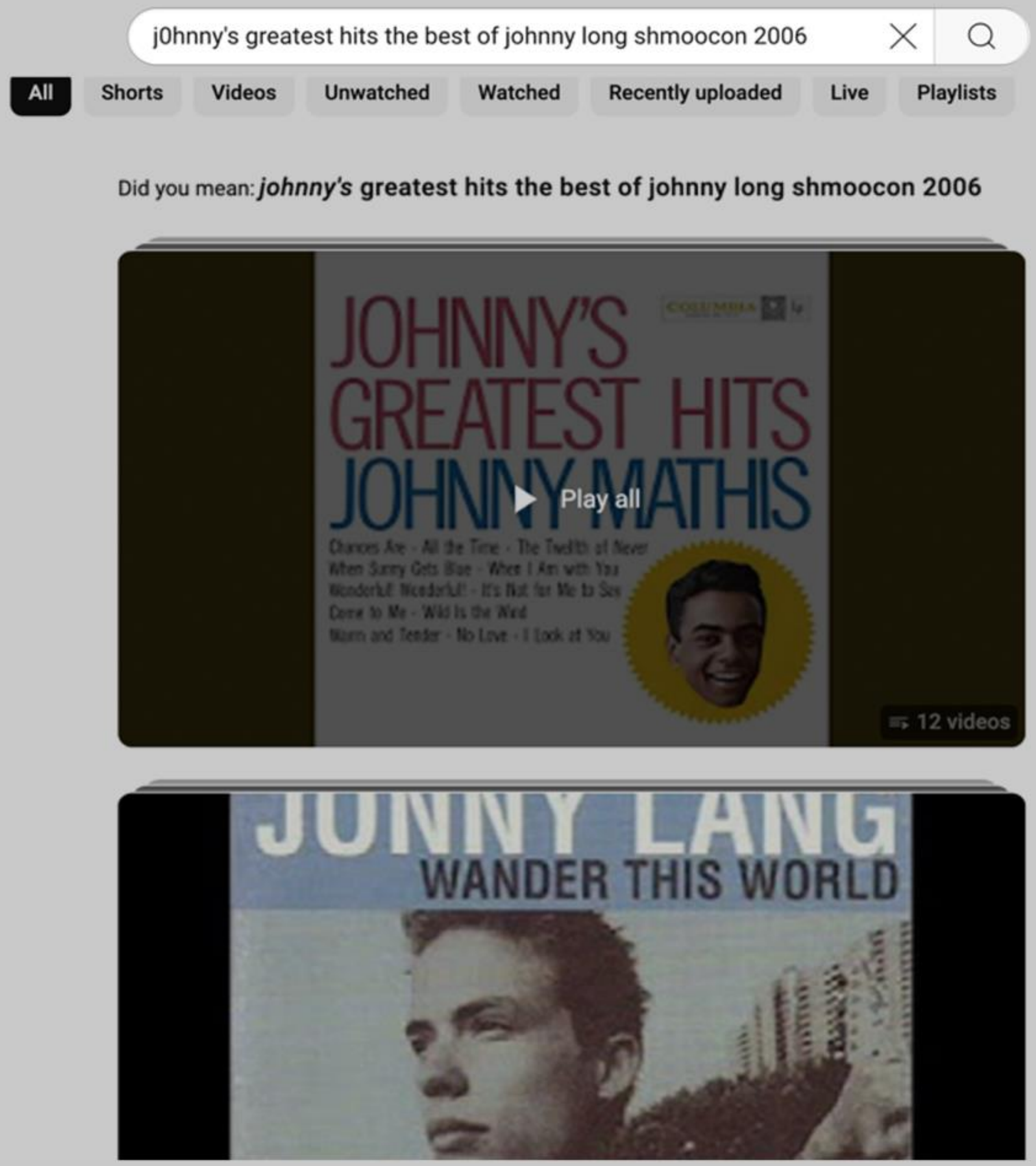


Most frequent taxonomy nodes

- 45 high-level categories – from Art to Wireless
- 543 unique taxonomy paths
- Example categories
  - Exploitation (91)
  - Law and Policy (34)
  - Defense (33)
  - Detection (27)
  - Intelligence (27)

Labeling heuristics

- Abstract + title > video > (in rare cases <1%) news, blogs, etc.
- Review materials to determine majority (51% rule)
- If you can't apply 51% rule, assign to level up or create a general category
- More specialized talks reside at the leaf nodes
- More generic talks in the next tier up
- If a (sane) home for a talk doesn't exist, then expand
- Discern intent (defend, exploit/attack, explain)



j0hnny's greatest hits the best of johnny long shmoocon 2006

Did you mean: ***johnny's*** **greatest hits the best of johnny long shmoocon 2006**

Labeling examples

ShmooCon 2012: And That's How I Didn't Lose an Eye: Emergency Data Destruction (EN)

And that's how I didn't lose an eye: emergency data destruction

Skunkworks, 2012

physical_security -> physical_infrastructure_destruction

SHMOOCON
2019
iPhone Surgery for the Practically Paranoid
Evan Jensen and Rudy Cuevas

iPhone Surgery for the Practically Paranoid - Evan Jensen & Rudy Cuevas

iPhone surgery for the practically paranoid

Jensen & Cuevas, 2019

defense -> sensors -> disabling_sensors

Building Absurd Christmas Light Shows - Rob Joyce

Building absurd Christmas light shows

Rob Joyce, 2018

making -> christmas_light_shows

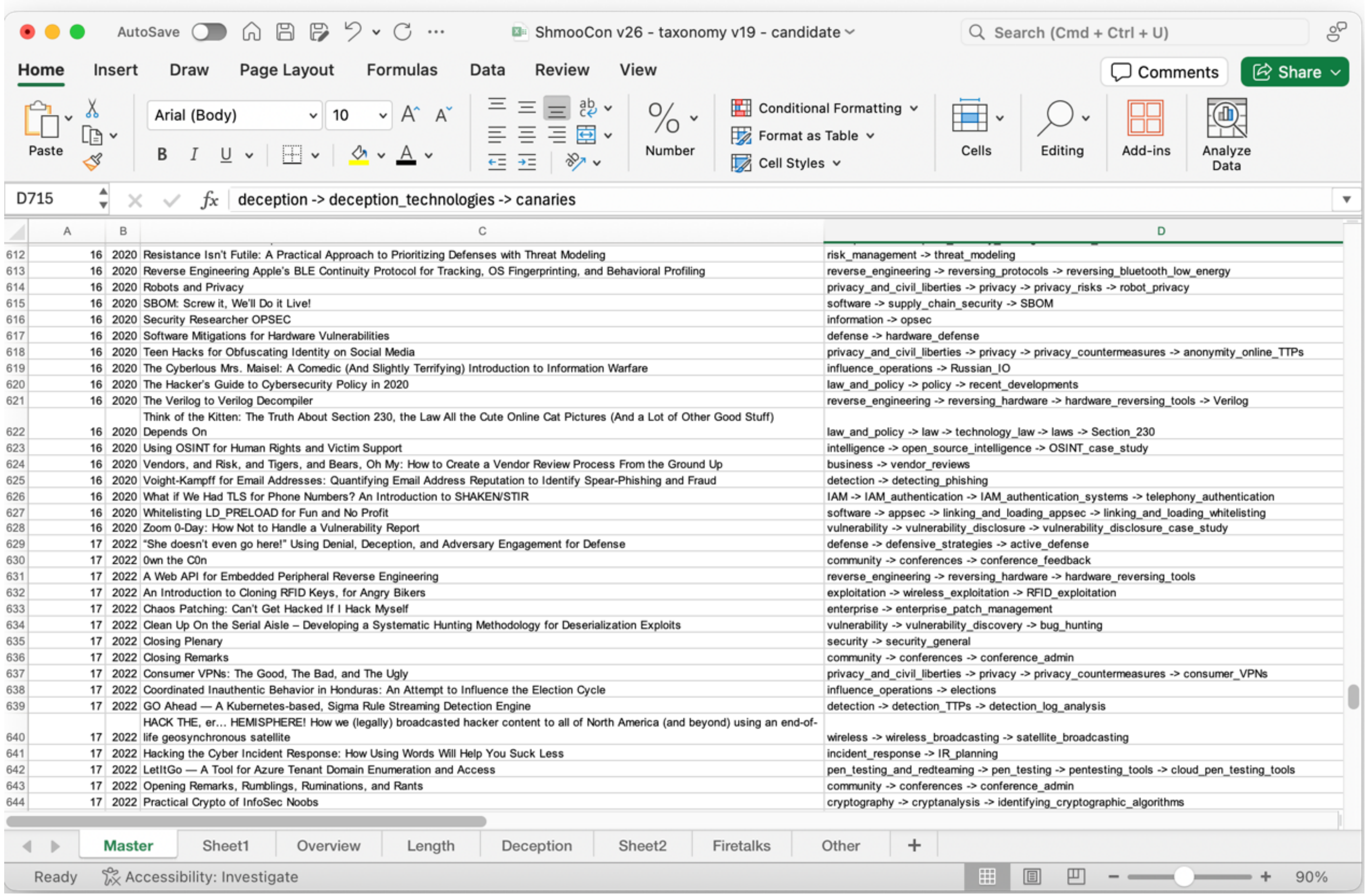
35yrs Of Cyberwar, The Squirrels are Winning - Shmoocon 2017

35 years of cyberwar: the squirrels are winning

Space Rogue, 2017

intelligence -> intelligence_analysis -> threat_actors -> squirrels

Labeling Summary

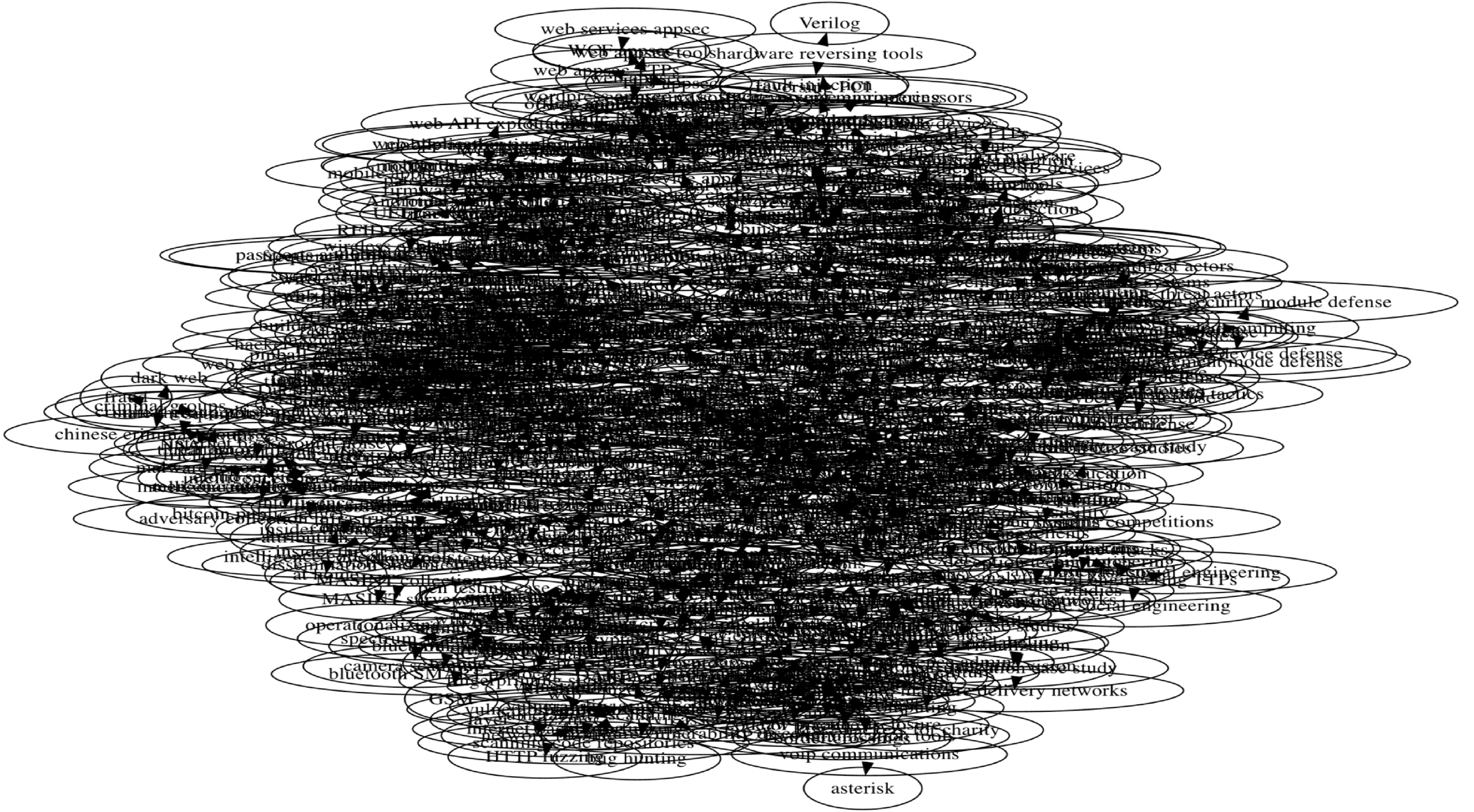


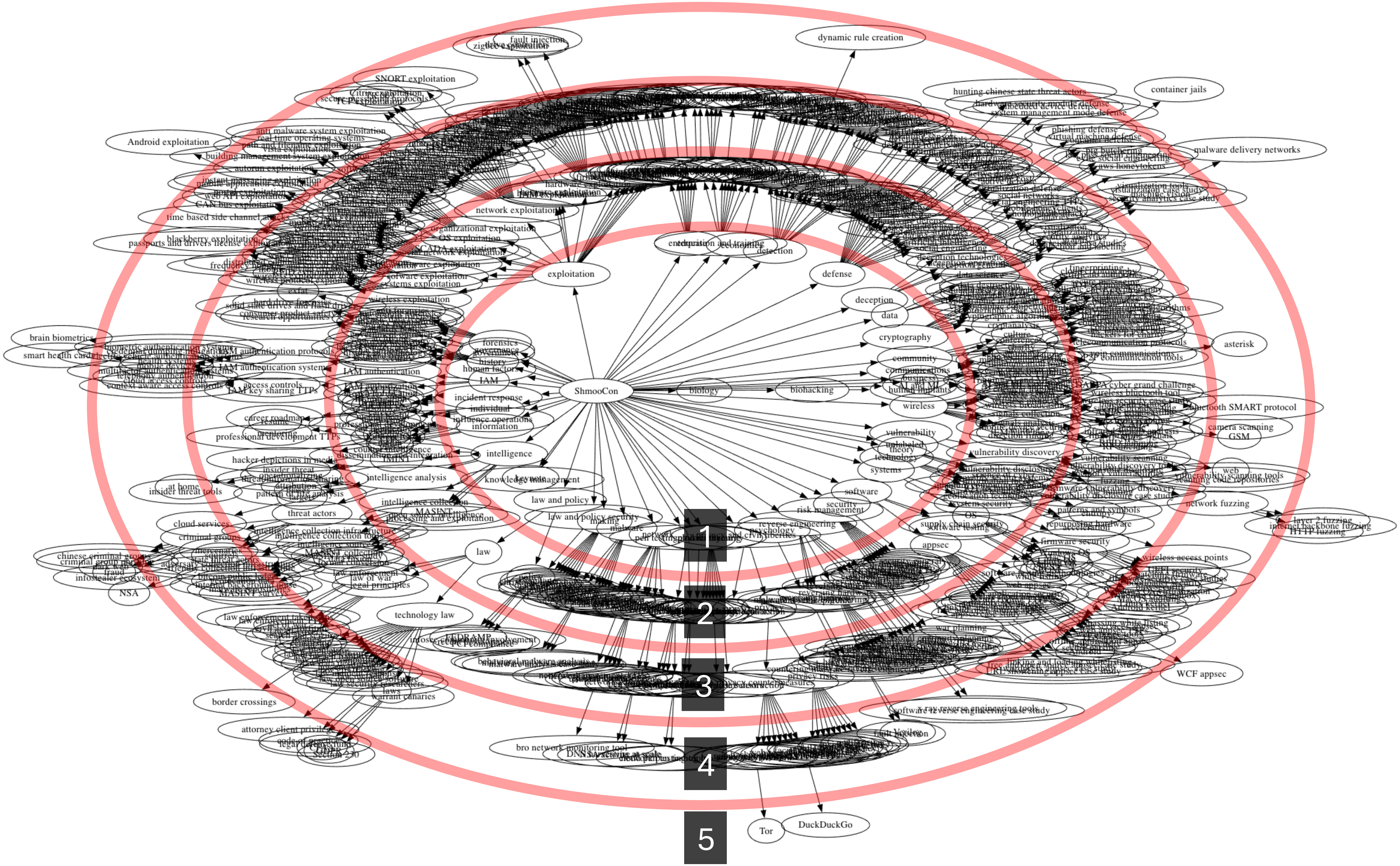
D715 deception -> deception_technologies -> canaries

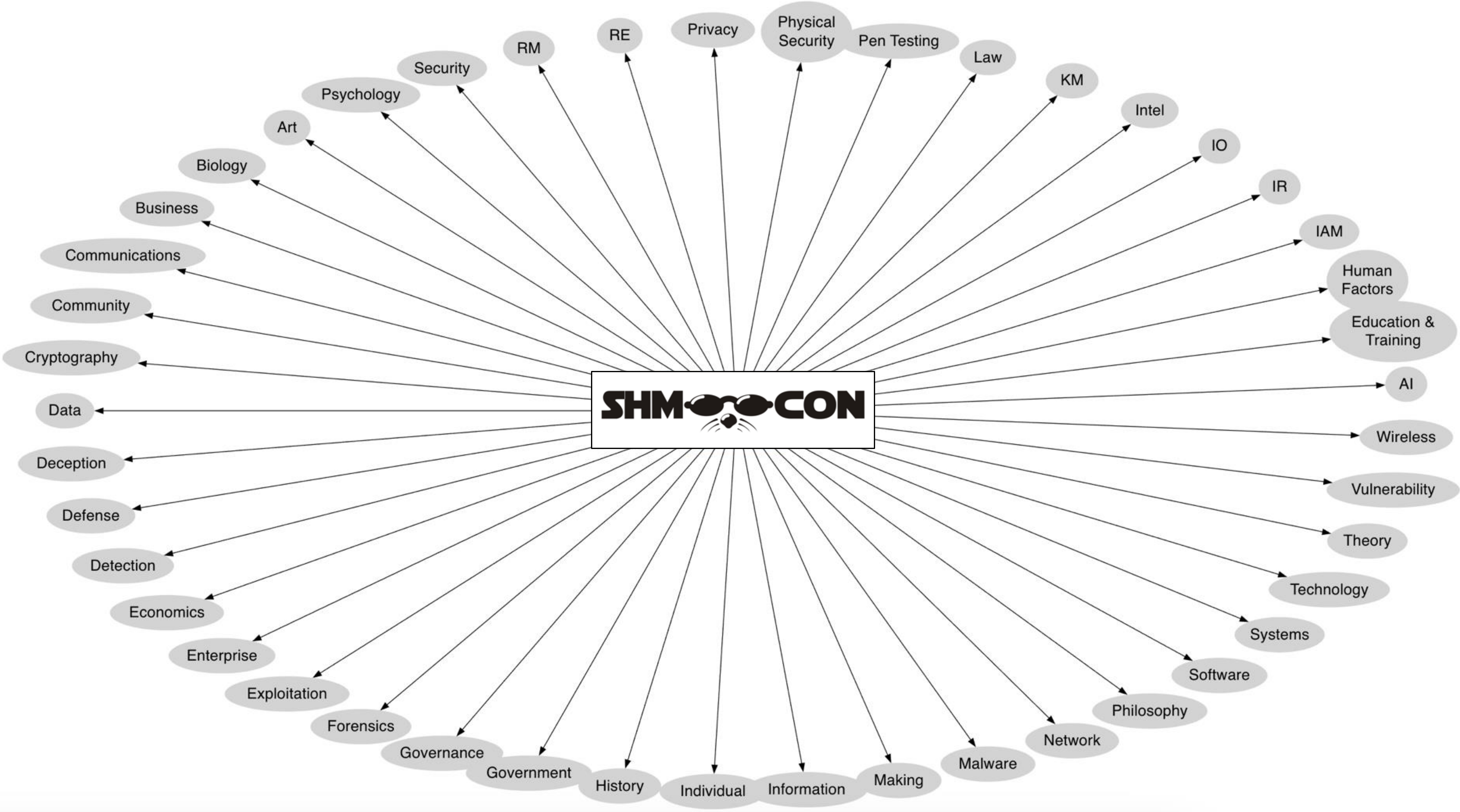
	A	B	C	D
612	16	2020	Resistance Isn't Futile: A Practical Approach to Prioritizing Defenses with Threat Modeling	risk_management -> threat_modeling
613	16	2020	Reverse Engineering Apple's BLE Continuity Protocol for Tracking, OS Fingerprinting, and Behavioral Profiling	reverse_engineering -> reversing_protocols -> reversing_bluetooth_low_energy
614	16	2020	Robots and Privacy	privacy_and_civil_liberties -> privacy -> privacy_risks -> robot_privacy
615	16	2020	SBOM: Screw it, We'll Do it Live!	software -> supply_chain_security -> SBOM
616	16	2020	Security Researcher OPSEC	information -> opsec
617	16	2020	Software Mitigations for Hardware Vulnerabilities	defense -> hardware_defense
618	16	2020	Teen Hacks for Obfuscating Identity on Social Media	privacy_and_civil_liberties -> privacy -> privacy_countermeasures -> anonymity_online_TTPs
619	16	2020	The Cyberlous Mrs. Maisel: A Comedic (And Slightly Terrifying) Introduction to Information Warfare	influence_operations -> Russian_IO
620	16	2020	The Hacker's Guide to Cybersecurity Policy in 2020	law_and_policy -> policy -> recent_developments
621	16	2020	The Verilog to Verilog Decompiler	reverse_engineering -> reversing_hardware -> hardware_reversing_tools -> Verilog
622	16	2020	Think of the Kitten: The Truth About Section 230, the Law All the Cute Online Cat Pictures (And a Lot of Other Good Stuff) Depends On	law_and_policy -> law -> technology_law -> laws -> Section_230
623	16	2020	Using OSINT for Human Rights and Victim Support	intelligence -> open_source_intelligence -> OSINT_case_study
624	16	2020	Vendors, and Risk, and Tigers, and Bears, Oh My: How to Create a Vendor Review Process From the Ground Up	business -> vendor_reviews
625	16	2020	Voight-Kampff for Email Addresses: Quantifying Email Address Reputation to Identify Spear-Phishing and Fraud	detection -> detecting_phishing
626	16	2020	What if We Had TLS for Phone Numbers? An Introduction to SHAKEN/STIR	IAM -> IAM_authentication -> IAM_authentication_systems -> telephony_authentication
627	16	2020	Whitelisting LD_PRELOAD for Fun and No Profit	software -> appsec -> linking_and_loading_appsec -> linking_and_loading_whitelisting
628	16	2020	Zoom 0-Day: How Not to Handle a Vulnerability Report	vulnerability -> vulnerability_disclosure -> vulnerability_disclosure_case_study
629	17	2022	"She doesn't even go here!" Using Denial, Deception, and Adversary Engagement for Defense	defense -> defensive_strategies -> active_defense
630	17	2022	0wn the C0n	community -> conferences -> conference_feedback
631	17	2022	A Web API for Embedded Peripheral Reverse Engineering	reverse_engineering -> reversing_hardware -> hardware_reversing_tools
632	17	2022	An Introduction to Cloning RFID Keys, for Angry Bikers	exploitation -> wireless_exploitation -> RFID_exploitation
633	17	2022	Chaos Patching: Can't Get Hacked If I Hack Myself	enterprise -> enterprise_patch_management
634	17	2022	Clean Up On the Serial Aisle – Developing a Systematic Hunting Methodology for Deserialization Exploits	vulnerability -> vulnerability_discovery -> bug_hunting
635	17	2022	Closing Plenary	security -> security_general
636	17	2022	Closing Remarks	community -> conferences -> conference_admin
637	17	2022	Consumer VPNs: The Good, The Bad, and The Ugly	privacy_and_civil_liberties -> privacy -> privacy_countermeasures -> consumer_VPNs
638	17	2022	Coordinated Inauthentic Behavior in Honduras: An Attempt to Influence the Election Cycle	influence_operations -> elections
639	17	2022	GO Ahead — A Kubernetes-based, Sigma Rule Streaming Detection Engine	detection -> detection_TTPs -> detection_log_analysis
640	17	2022	HACK THE, er… HEMISPHERE! How we (legally) broadcasted hacker content to all of North America (and beyond) using an end-of-life geosynchronous satellite	wireless -> wireless_broadcasting -> satellite_broadcasting
641	17	2022	Hacking the Cyber Incident Response: How Using Words Will Help You Suck Less	incident_response -> IR_planning
642	17	2022	LetItGo — A Tool for Azure Tenant Domain Enumeration and Access	pen_testing_and_redteaming -> pen_testing -> pentesting_tools -> cloud_pen_testing_tools
643	17	2022	Opening Remarks, Rumblings, Ruminations, and Rants	community -> conferences -> conference_admin
644	17	2022	Practical Crypto of InfoSec Noobs	cryptography -> cryptanalysis -> identifying_cryptographic_algorithms

801 labeled talks

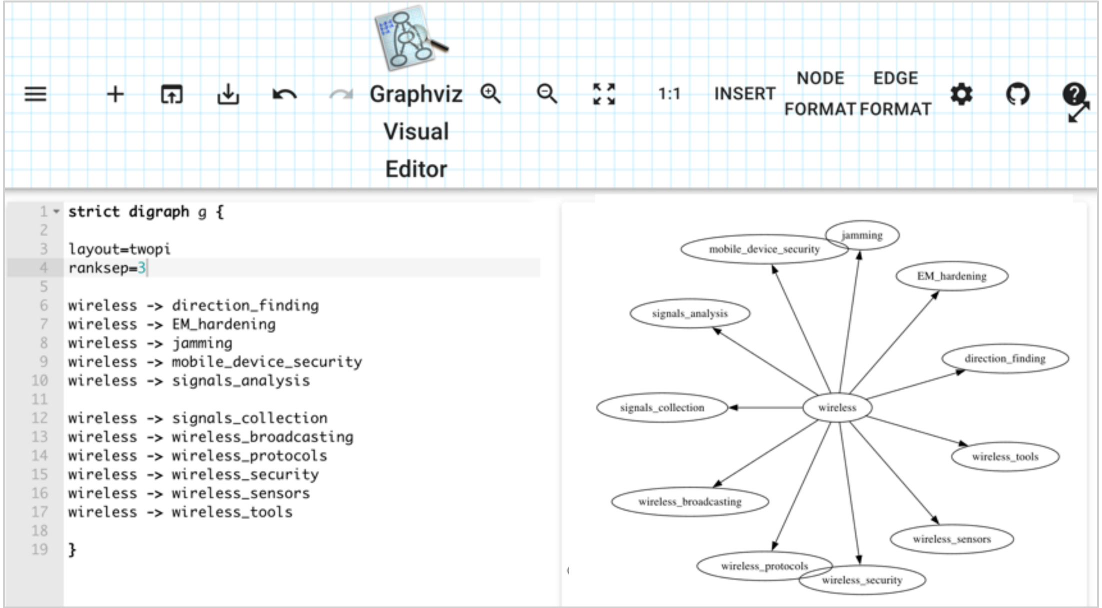
We are proud to unveil the complete taxonomy for your viewing pleasure!


web services appsec
Verilog
WCF appsec
hardware reversing tools
web appsec TTPs
fault injection
web API exploitation
mobile application
security module defense
device defense
social engineering
competitions
dark web
fraud
criminal groups
chinese criminal groups
adversary collection
bitcoin
MASINT collection
pen testing case studies
operational
spectrum
camera security
bluetooth SMART protocol
GSM
malware delivery networks
case study
scanning code repositories
HTTP fuzzing
bug hunting
voip communications
asterisk


ShmooCon
1
2
3
4
5
exploitation
defense
education and training
detection
deception
data
cryptography
community
communications
business
human implants
wireless
biology
biohacking
vulnerability
unlabeled
theory
technology
systems
software
security
risk management
reverse engineering
psychology
appsec
OS
supply chain security
software testing
law and policy
law and policy security
making
malware
law
technology law
intelligence
intelligence analysis
knowledge management
keynote
incident response
individual
influence operations
information
forensics
governance
history
human factors
IAM
dynamic rule creation
fault injection
zigbee exploitation
SNORT exploitation
Citrix exploitation
TCP exploitation
Android exploitation
anti malware system exploitation
real time operating systems
building management system exploitation
autorun exploitation
mobile application exploitation
CAN bus exploitation
passports and drivers license exploitation
blackberry exploitation
network exploitation
organizational exploitation
OS exploitation
SCADA exploitation
firmware exploitation
software exploitation
systems exploitation
wireless exploitation
exfil
brain biometrics
smart health cards
IAM authentication protocols
IAM authentication systems
access controls
IAM key sharing TTPs
context aware access controls
telephony authentication
cloud access controls
IAM authentication
career roadmaps
professional development TTPs
hacker depictions in media
insider threat
at home
insider threat tools
threat intelligence sharing
pattern of life analysis
threat actors
cloud services
criminal groups
chinese criminal groups
fraud
infostealer ecosystem
NSA
intelligence collection infrastructure
intelligence collection tools
MASINT collection
law enforcement
law of war
legal principles
MASINT survey
bitcoin public ledger
border crossings
attorney client privilege
Section 230
laws
warrant canaries
intelligence collection
MASINT
processing and exploitation
counterintelligence
dissemination and integration
IMINT
hunting chinese state threat actors
container jails
hardware security module defense
embedded device defense
system management mode defense
phishing defense
virtual machine defense
malware delivery networks
pig butchering
aws honeytokens
visualization tools
security analytics case study
social networks
social engineering TTPs
deception technologies
deception operations
data science
cryptographic algorithms
cryptanalysis
culture
conference
fingerprinting
asterisk
telecommunication protocols
P2P communication tools
DARPA cyber grand challenge
wireless bluetooth tool
bluetooth SMART protocol
camera scanning
GSM
signals collection
vulnerability discovery
vulnerability scanning
web
vulnerability scanning tools
scanning code repositories
network fuzzing
layer 2 fuzzing
internet backbone fuzzing
HTTP fuzzing
patterns and symbols
entropy
repurposing hardware
firmware security
wireless access points
Windows OS
UEFI security
Linux kernel
web appsec
war planning
WCF appsec
URL shortening appsec case study
raw reverse engineering tools
software reverse engineering case study
Verilog
Tor
DuckDuckGo
bro network monitoring tool
DNS
behavioral malware analysis
FEDRAMP
PCI compliance
privacy risks
countermeasures


SHMOOCON
Art
Biology
Business
Communications
Community
Cryptography
Data
Deception
Defense
Detection
Economics
Enterprise
Exploitation
Forensics
Governance
Government
History
Individual
Information
Making
Malware
Network
Philosophy
Software
Systems
Technology
Theory
Vulnerability
Wireless
AI
Education & Training
Human Factors
IAM
IR
IO
Intel
KM
Law
Pen Testing
Physical Security
Privacy
RE
RM
Security
Psychology

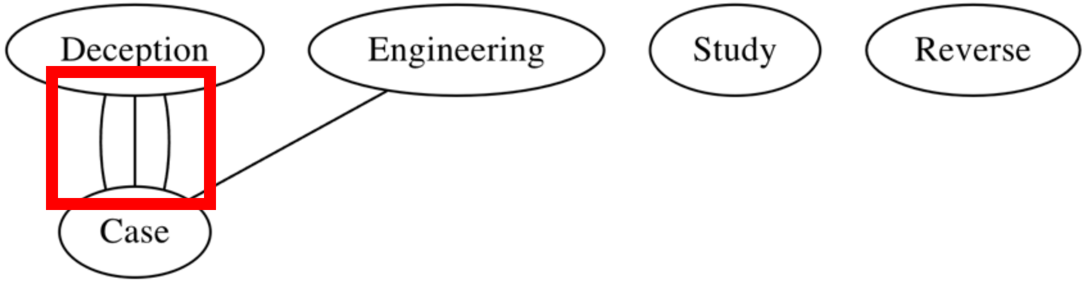
GraphViz and DOT



```
strict digraph g {

layout=twopi
ranksep=3

wireless -> direction_finding
wireless -> EM_hardening
wireless -> jamming
wireless -> mobile_device_security
wireless -> signals_analysis

wireless -> signals_collection
wireless -> wireless_broadcasting
wireless -> wireless_protocols
wireless -> wireless_security
wireless -> wireless_sensors
wireless -> wireless_tools

}
```

[GraphViz Visual Editor]

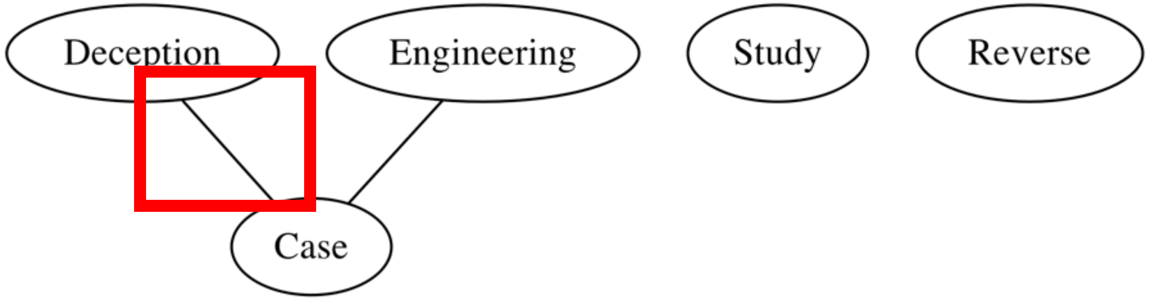
- DOT – graph description language
- GraphViz
  - open source graph viewing package
  - supports options: layout, scaling, color, …
- Secret handshakes: reserved words, non-alphanumeric characters



Talk A – Deception case study
Talk B – Another deception case study
Talk C – Another deception case study
Talk D – Reverse engineering case study

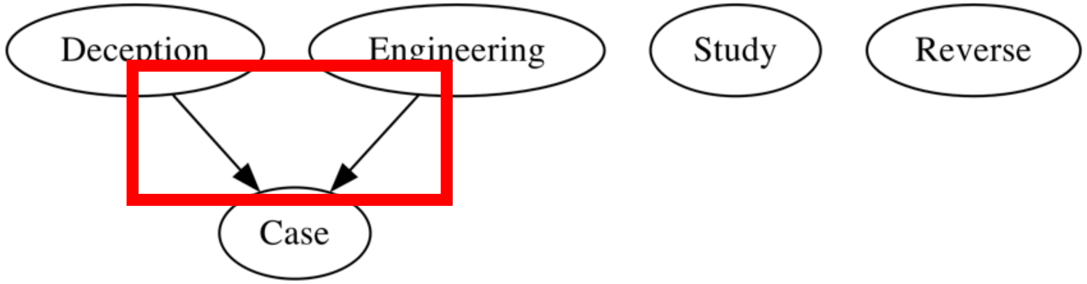
```
graph g {
Deception -- case study
Deception -- case study
Deception -- case study
Reverse Engineering -- case study
}
```

1. Remove duplicate links



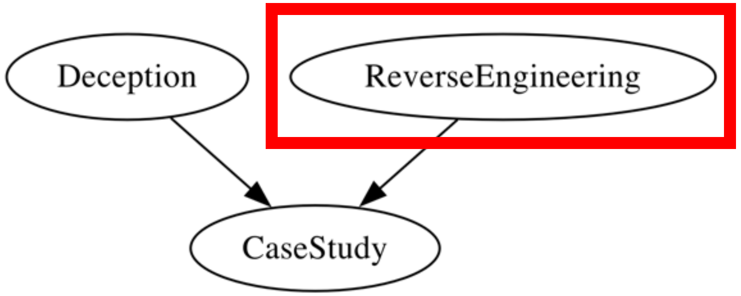
```
strict graph g {
Deception  -- case study
Deception  -- case study
Deception  -- case study
Reverse engineering  -- case study
}
```

2. Directional graph



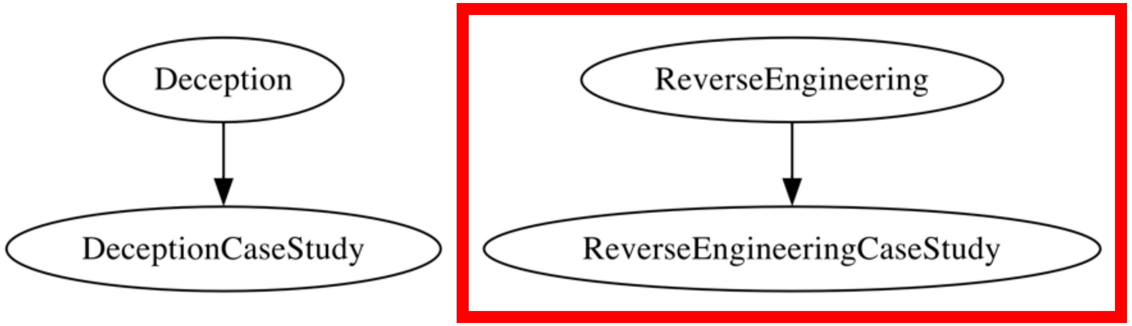
```
strict digraph g {
Deception -> case study
Deception -> case study
Deception -> case study
Reverse Engineering -> case study
}
```

3. Remove spaces in node names



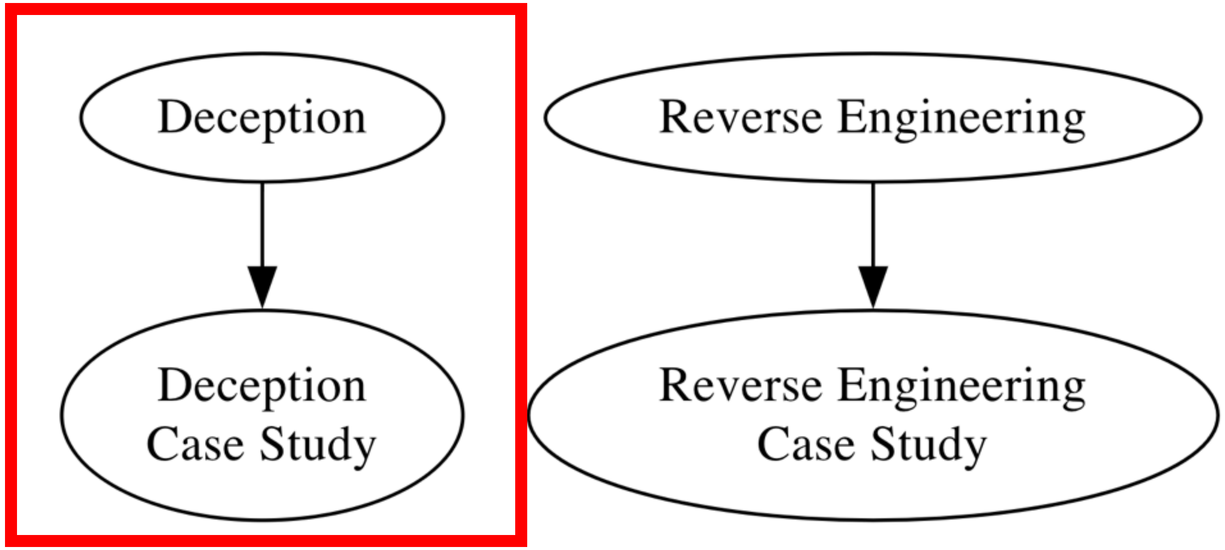
```
strict digraph g {
Deception -> CaseStudy
Deception -> CaseStudy
Deception -> CaseStudy
ReverseEngineering -> CaseStudy
}
```

4. Unique node names

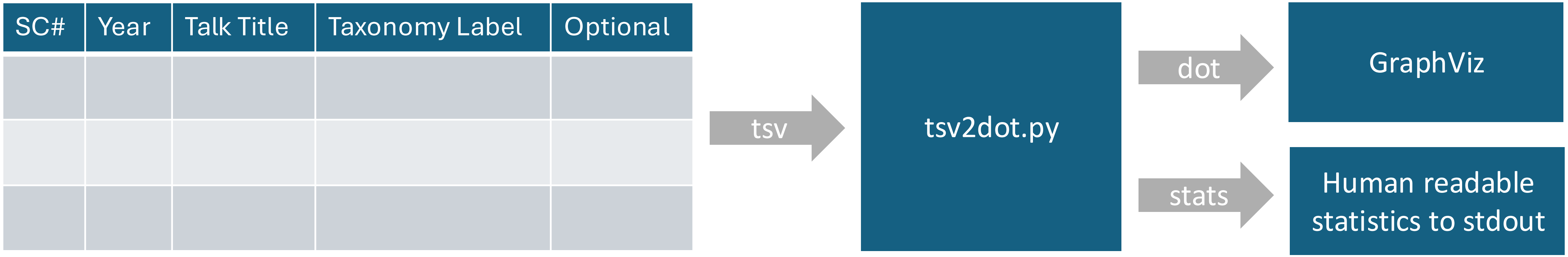


```
strict digraph g {
Deception -> DeceptionCaseStudy
Deception -> DeceptionCaseStudy
Deception -> DeceptionCaseStudy
ReverseEngineering -> ReverseEngineeringCaseStudy
}
```

Final: Label Nodes



```
strict digraph g {
Deception [label="Deception"]
DeceptionCaseStudy [label="Deception \nCase Study"]
ReverseEngineering [label="Reverse Engineering"]
ReverseEngineeringCaseStudy [label="Reverse Engineering \nCase Study"]
Deception -> DeceptionCaseStudy
Deception -> DeceptionCaseStudy
Deception -> DeceptionCaseStudy
ReverseEngineering -> ReverseEngineeringCaseStudy
}
```



SC#	Year	Talk Title	Taxonomy Label	Optional

tsv

tsv2dot.py

dot

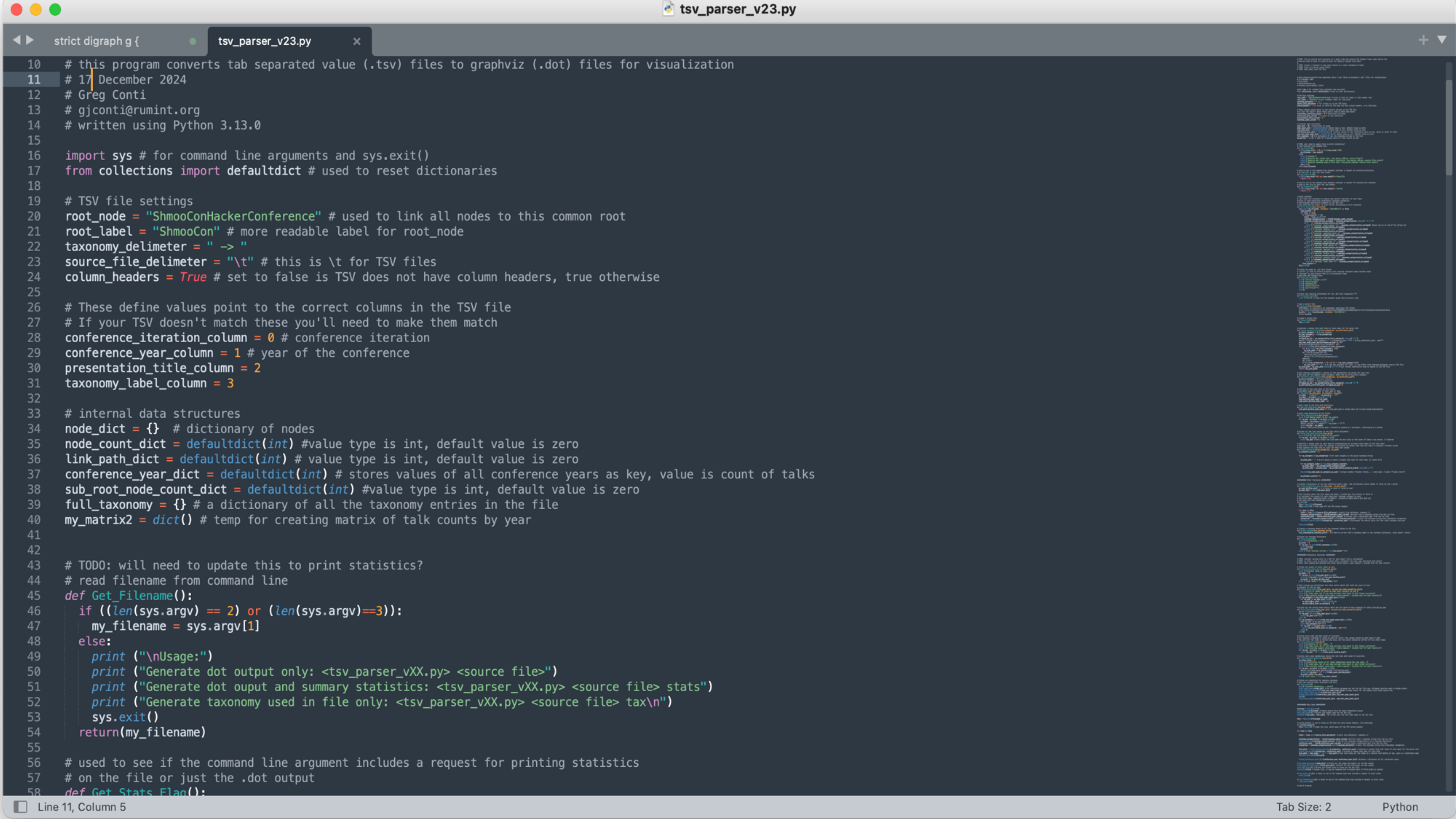
GraphViz

stats

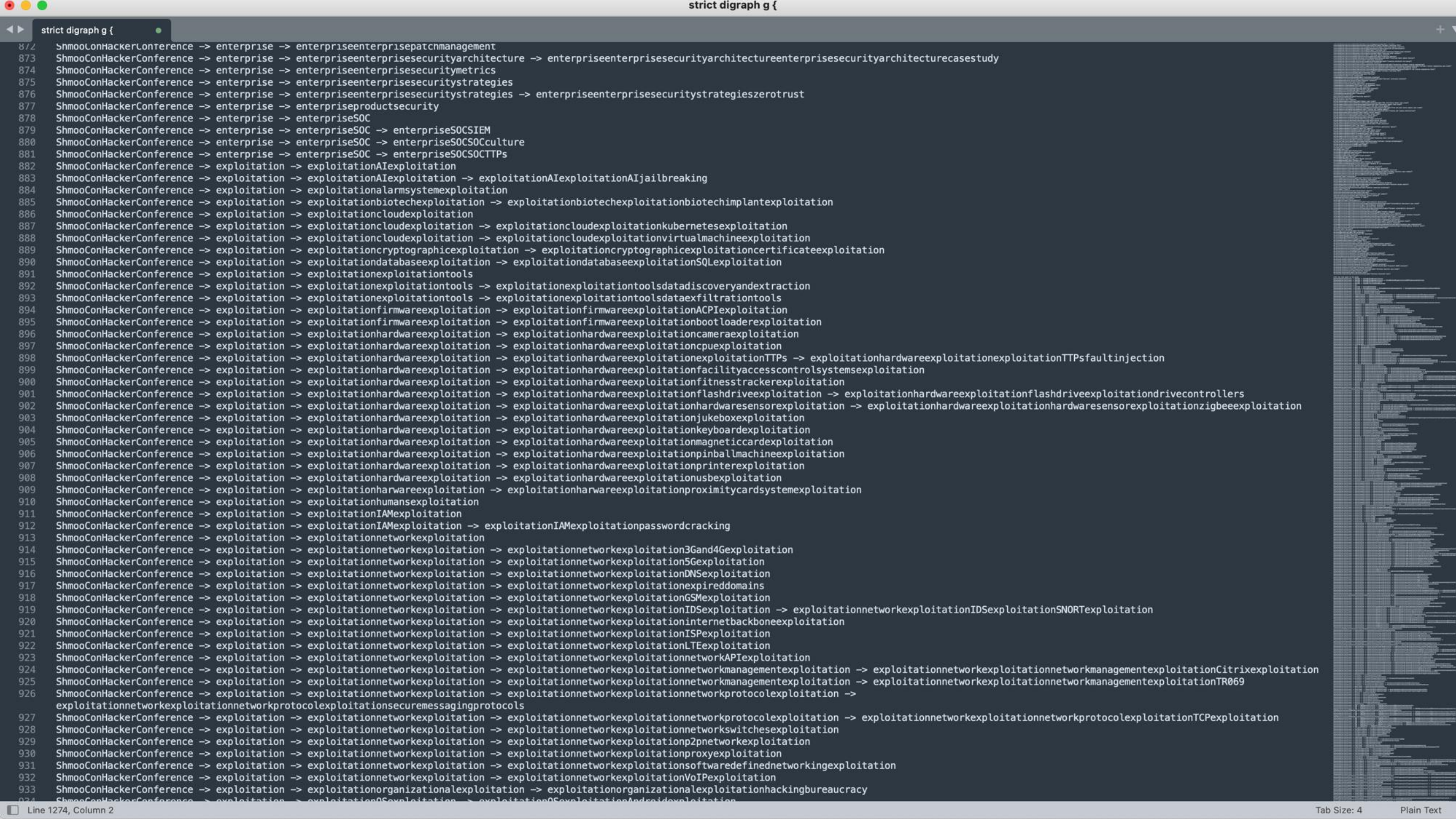
Human readable statistics to stdout

Usage

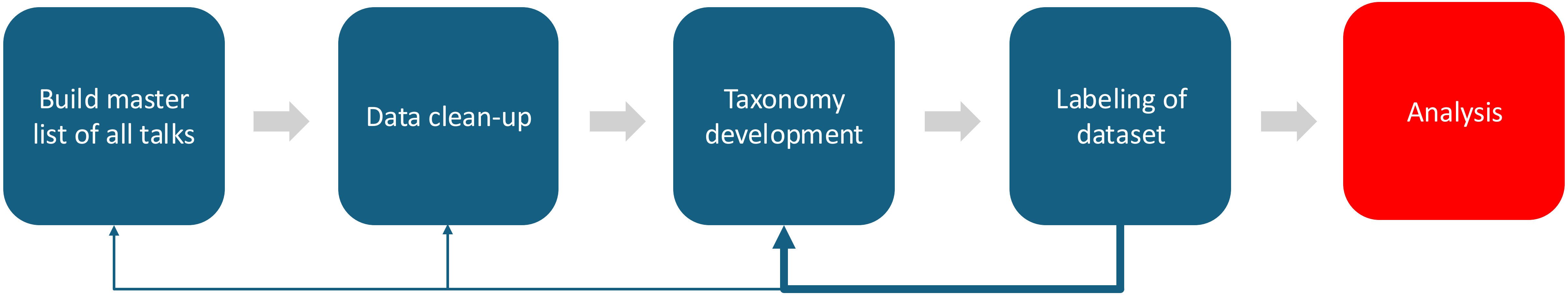
```
dot output only: <tsv_parser_vXX.py> <source file>
python3 tsv_parser_v23.py labeled_SC.tsv

dot output and summary statistics: <tsv_parser_vXX.py> <source file> stats
python3 tsv_parser_v23.py labeled_SC.tsv stats

Generate taxonomy used in file only: <tsv_parser_vXX.py> <source file> tax
python3 tsv_parser_v23.py labeled_SC.tsv tax
```



```python
# this program converts tab separated value (.tsv) files to graphviz (.dot) files for visualization
# 17 December 2024
# Greg Conti
# gjconti@rumint.org
# written using Python 3.13.0

import sys # for command line arguments and sys.exit()
from collections import defaultdict # used to reset dictionaries

# TSV file settings
root_node = "ShmooConHackerConference" # used to link all nodes to this common root
root_label = "ShmooCon" # more readable label for root_node
taxonomy_delimeter = " -> "
source_file_delimeter = "\t" # this is \t for TSV files
column_headers = True # set to false is TSV does not have column headers, true otherwise

# These define values point to the correct columns in the TSV file
# If your TSV doesn't match these you'll need to make them match
conference_iteration_column = 0 # conference iteration
conference_year_column = 1 # year of the conference
presentation_title_column = 2
taxonomy_label_column = 3

# internal data structures
node_dict = {}  # dictionary of nodes
node_count_dict = defaultdict(int) #value type is int, default value is zero
link_path_dict = defaultdict(int) # value type is int, default value is zero
conference_year_dict = defaultdict(int) # stores values of all conference years as key, value is count of talks
sub_root_node_count_dict = defaultdict(int) #value type is int, default value is zero
full_taxonomy = {} # a dictionary of all the taxonomy entries in the file
my_matrix2 = dict() # temp for creating matrix of talk counts by year


# TODO: will need to update this to print statistics?
# read filename from command line
def Get_Filename():
  if ((len(sys.argv) == 2) or (len(sys.argv)==3)):
    my_filename = sys.argv[1]
  else:
    print ("\nUsage:")
    print ("Generate dot output only: <tsv_parser_vXX.py> <source file>")
    print ("Generate dot ouput and summary statistics: <tsv_parser_vXX.py> <source file> stats")
    print ("Generate taxonomy used in file only: <tsv_parser_vXX.py> <source file> tax\n")
    sys.exit()
  return(my_filename)

# used to see if the command line argument includes a request for printing statistics
# on the file or just the .dot output
def Get_Stats_Flag():
```



```
ShmooConHackerConference -> enterprise -> enterpriseenterprisepatchmanagement
ShmooConHackerConference -> enterprise -> enterpriseenterprisesecurityarchitecture -> enterpriseenterprisesecurityarchitectureenterprisesecurityarchitecturecasestudy
ShmooConHackerConference -> enterprise -> enterpriseenterprisesecuritymetrics
ShmooConHackerConference -> enterprise -> enterpriseenterprisesecuritystrategies
ShmooConHackerConference -> enterprise -> enterpriseenterprisesecuritystrategies -> enterpriseenterprisesecuritystrategieszerotrust
ShmooConHackerConference -> enterprise -> enterpriseproductsecurity
ShmooConHackerConference -> enterprise -> enterpriseSOC
ShmooConHackerConference -> enterprise -> enterpriseSOC -> enterpriseSOCSIEM
ShmooConHackerConference -> enterprise -> enterpriseSOC -> enterpriseSOCSOCculture
ShmooConHackerConference -> enterprise -> enterpriseSOC -> enterpriseSOCSOCTTPs
ShmooConHackerConference -> exploitation -> exploitationAIexploitation
ShmooConHackerConference -> exploitation -> exploitationAIexploitation -> exploitationAIexploitationAIjailbreaking
ShmooConHackerConference -> exploitation -> exploitationalarmsystemexploitation
ShmooConHackerConference -> exploitation -> exploitationbiotechexploitation -> exploitationbiotechexploitationbiotechimplantexploitation
ShmooConHackerConference -> exploitation -> exploitationcloudexploitation
ShmooConHackerConference -> exploitation -> exploitationcloudexploitation -> exploitationcloudexploitationkubernetesexploitation
ShmooConHackerConference -> exploitation -> exploitationcloudexploitation -> exploitationcloudexploitationvirtualmachineexploitation
ShmooConHackerConference -> exploitation -> exploitationcryptographicexploitation -> exploitationcryptographicexploitationcertificateexploitation
ShmooConHackerConference -> exploitation -> exploitationdatabaseexploitation -> exploitationdatabaseexploitationSQLexploitation
ShmooConHackerConference -> exploitation -> exploitationexploitationtools
ShmooConHackerConference -> exploitation -> exploitationexploitationtools -> exploitationexploitationtoolsdatadiscoveryandextraction
ShmooConHackerConference -> exploitation -> exploitationexploitationtools -> exploitationexploitationtoolsdataexfiltrationtools
ShmooConHackerConference -> exploitation -> exploitationfirmwareexploitation -> exploitationfirmwareexploitationACPIexploitation
ShmooConHackerConference -> exploitation -> exploitationfirmwareexploitation -> exploitationfirmwareexploitationbootloaderexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationcameraexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationcpuexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationexploitationTTPs -> exploitationhardwareexploitationexploitationTTPsfaultinjection
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationfacilityaccesscontrolsystemsexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationfitnesstrackerexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationflashdriveexploitation -> exploitationhardwareexploitationflashdriveexploitationdrivecontrollers
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationhardwaresensorexploitation -> exploitationhardwareexploitationhardwaresensorexploitationzigbeeexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationjukeboxexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationkeyboardexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationmagneticcardexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationpinballmachineexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationprinterexploitation
ShmooConHackerConference -> exploitation -> exploitationhardwareexploitation -> exploitationhardwareexploitationusbexploitation
ShmooConHackerConference -> exploitation -> exploitationharwareexploitation -> exploitationharwareexploitationproximitycardsystemexploitation
ShmooConHackerConference -> exploitation -> exploitationhumansexploitation
ShmooConHackerConference -> exploitation -> exploitationIAMexploitation
ShmooConHackerConference -> exploitation -> exploitationIAMexploitation -> exploitationIAMexploitationpasswordcracking
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitation3Gand4Gexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitation5Gexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationDNSexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationexpireddomains
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationGSMexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationIDSexploitation -> exploitationnetworkexploitationIDSexploitationSNORTexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationinternetbackboneexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationISPexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationLTEexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationnetworkAPIexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationnetworkmanagementexploitation -> exploitationnetworkexploitationnetworkmanagementexploitationCitrixexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationnetworkmanagementexploitation -> exploitationnetworkexploitationnetworkmanagementexploitationTR069
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationnetworkprotocolexploitation -> exploitationnetworkexploitationnetworkprotocolexploitationsecuremessagingprotocols
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationnetworkprotocolexploitation -> exploitationnetworkexploitationnetworkprotocolexploitationTCPexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationnetworkswitchesexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationp2pnetworkexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationproxyexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationsoftwaredefinednetworkingexploitation
ShmooConHackerConference -> exploitation -> exploitationnetworkexploitation -> exploitationnetworkexploitationVoIPexploitation
ShmooConHackerConference -> exploitation -> exploitationorganizationalexploitation -> exploitationorganizationalexploitationhackingbureaucracy
ShmooConHackerConference -> exploitation -> exploitationOSexploitation -> exploitationOSexploitationAndroidexploitation
```

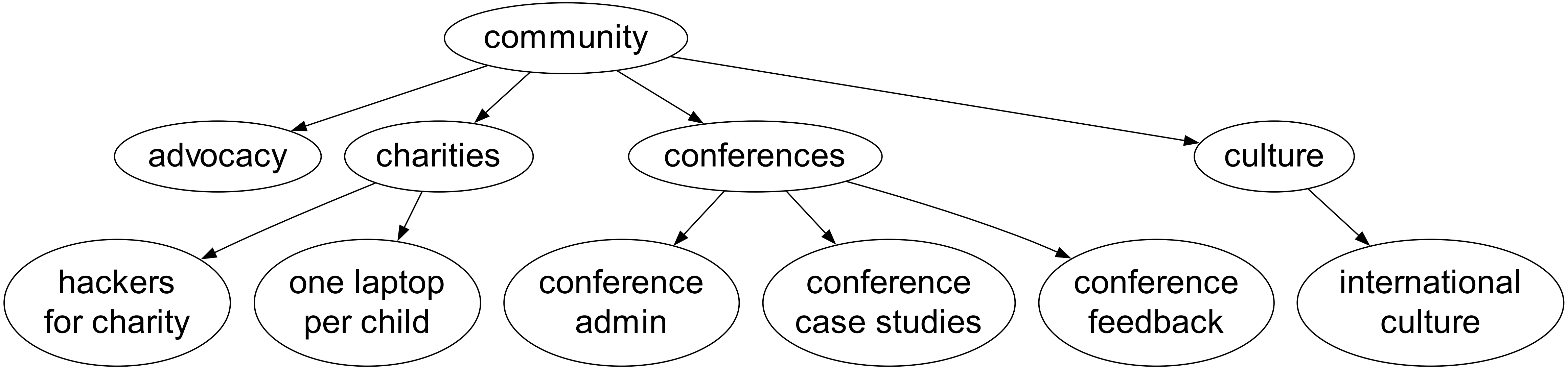

Build master list of all talks

Data clean-up

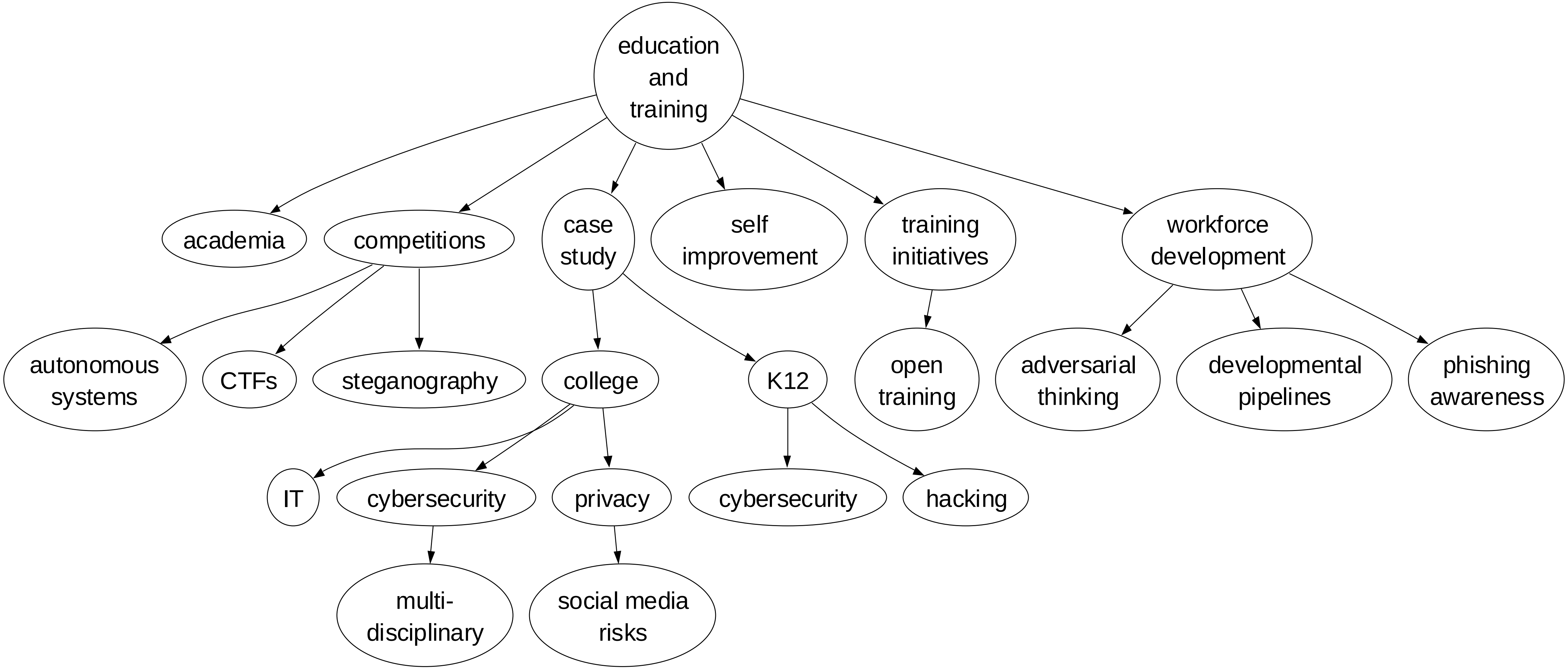
Taxonomy development

Labeling of dataset

Analysis

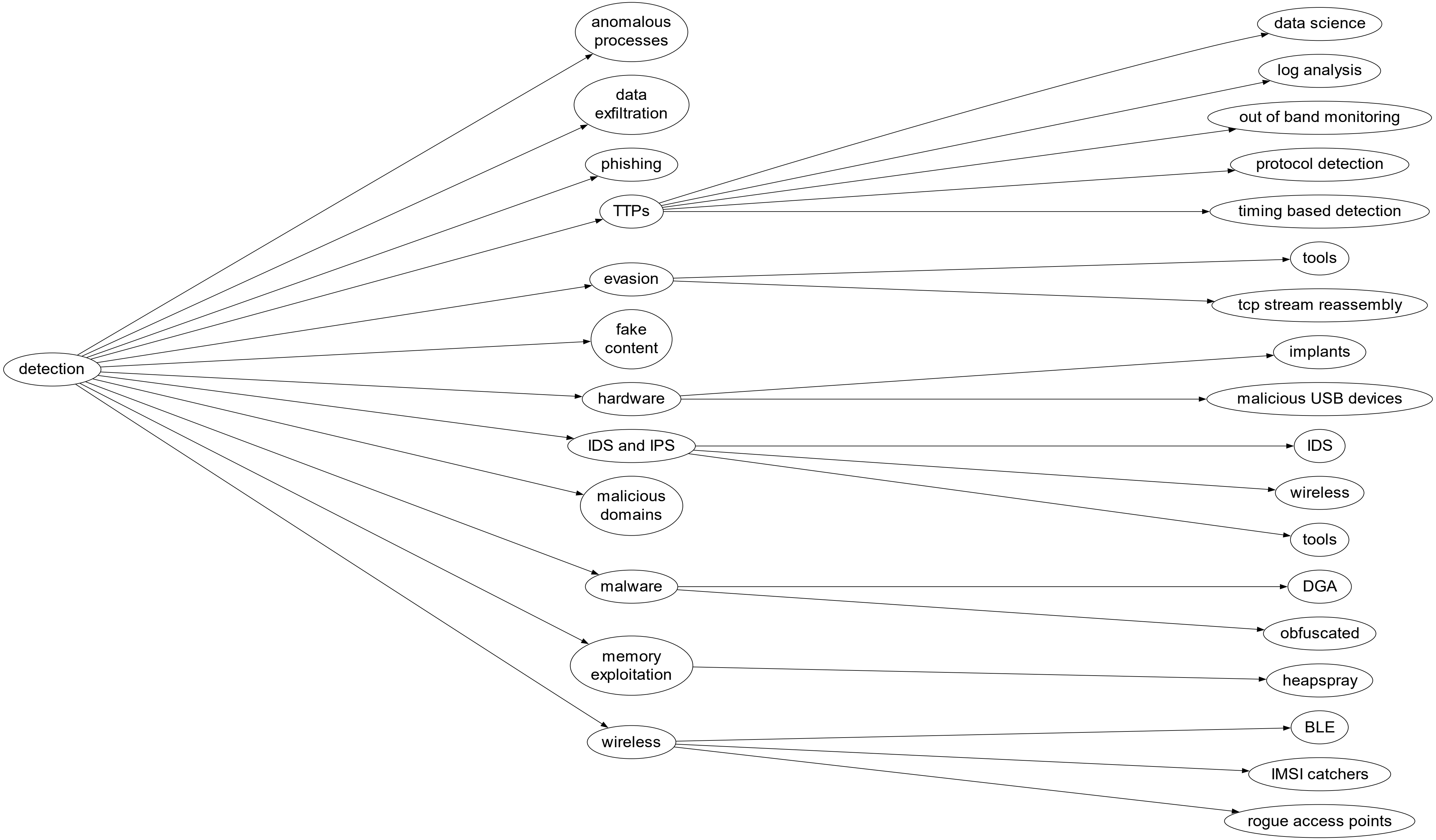


Community (46 talks – 2.3 talks per ShmooCon)



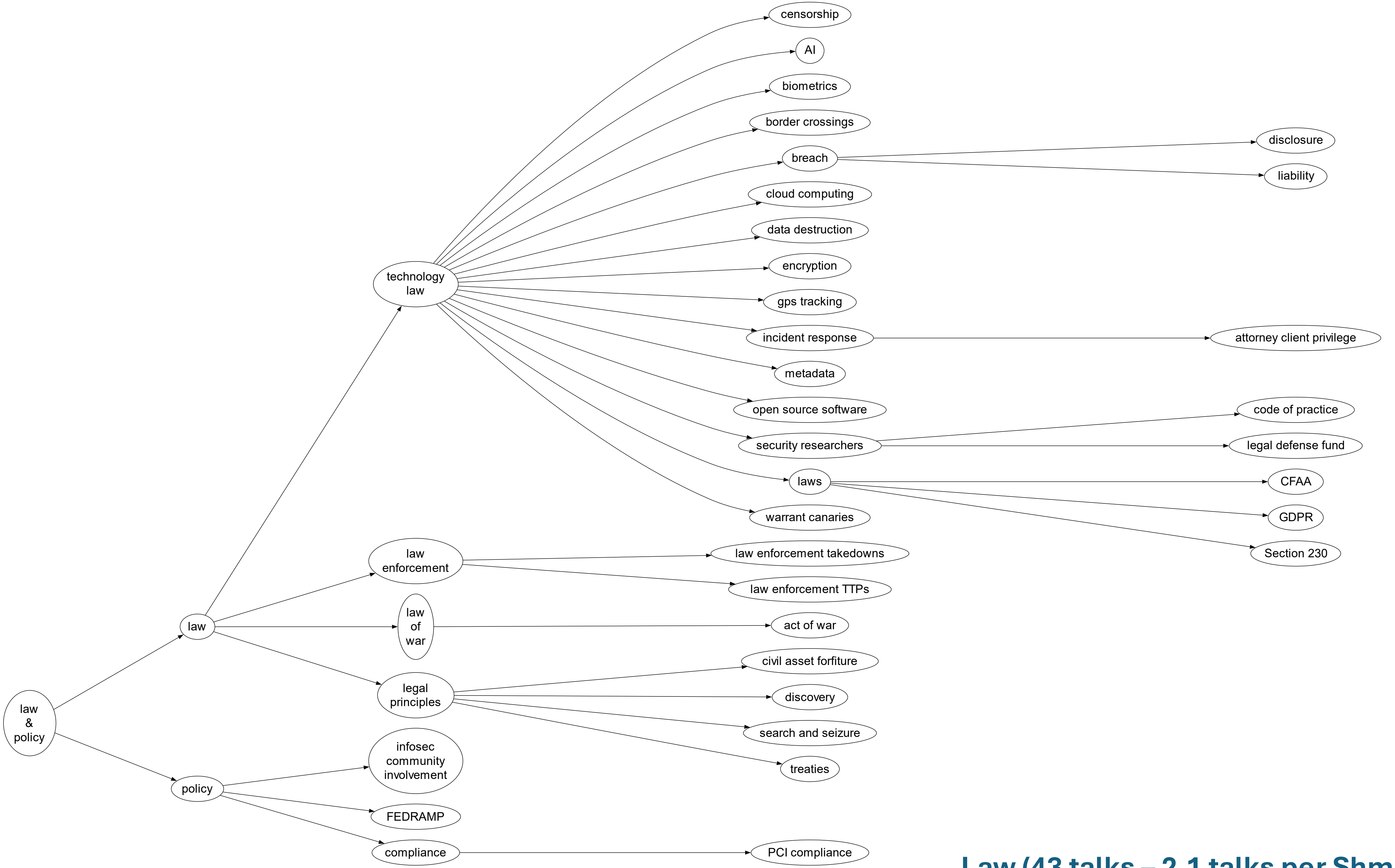
- education and training
  - academia
  - competitions
    - autonomous systems
    - CTFs
    - steganography
  - case study
    - college
      - IT
      - cybersecurity
        - multi-disciplinary
      - privacy
        - social media risks
    - K12
      - cybersecurity
      - hacking
  - self improvement
  - training initiatives
    - open training
  - workforce development
    - adversarial thinking
    - developmental pipelines
    - phishing awareness

Education and Training (20 talks – 1 talk per ShmooCon)

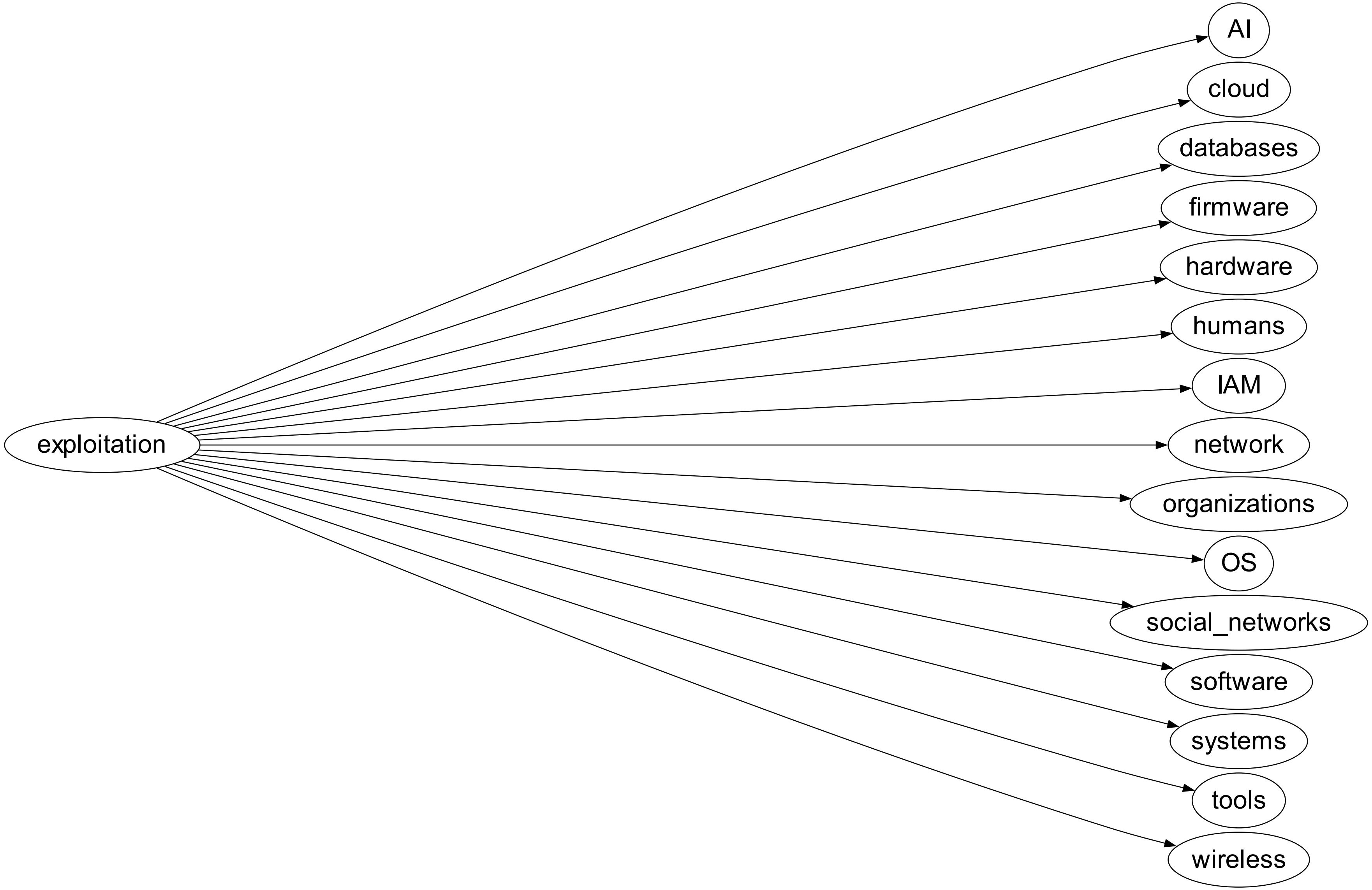


Detection (32 talks – 1.6 talks per ShmooCon)

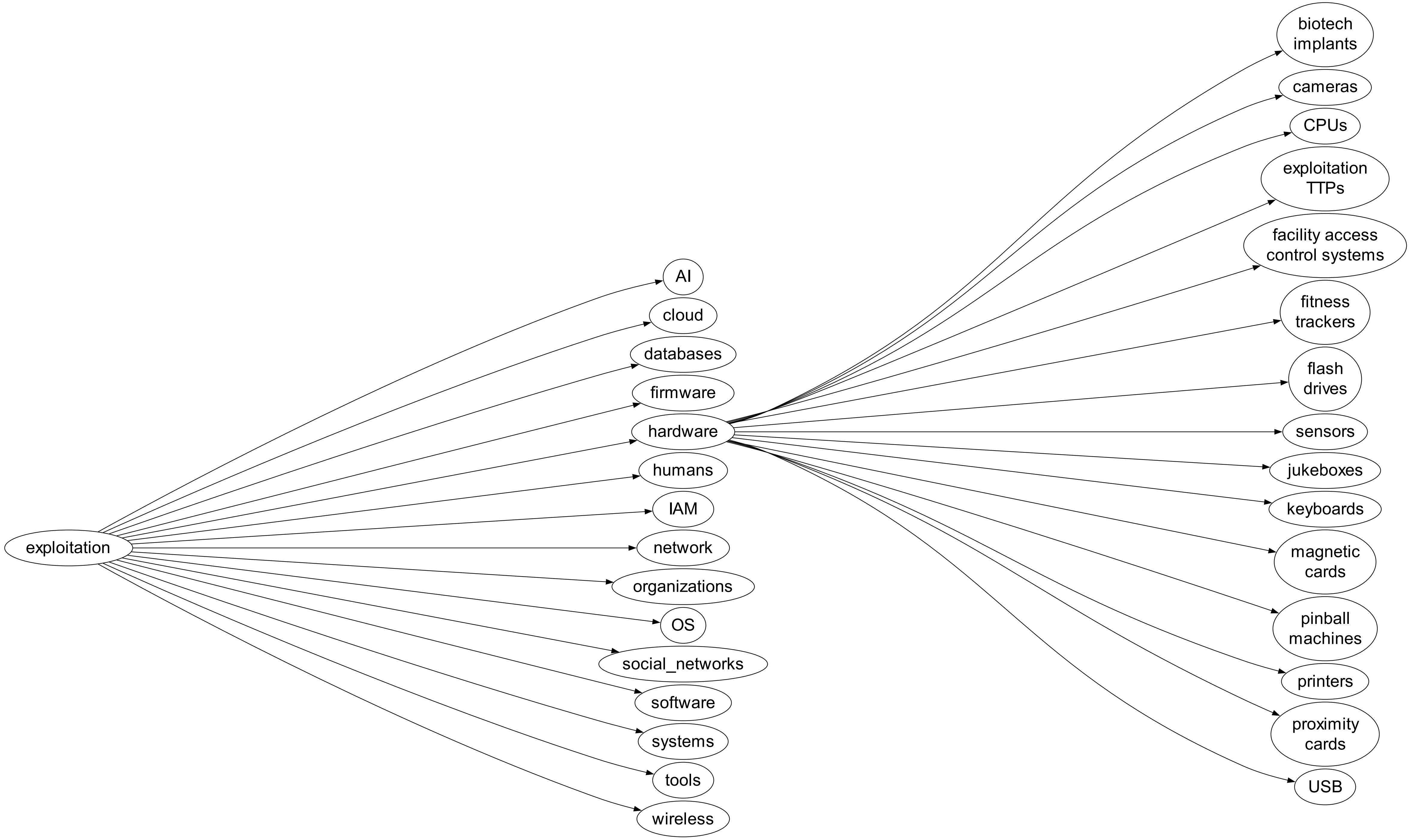
Law (43 talks – 2.1 talks per ShmooCon)



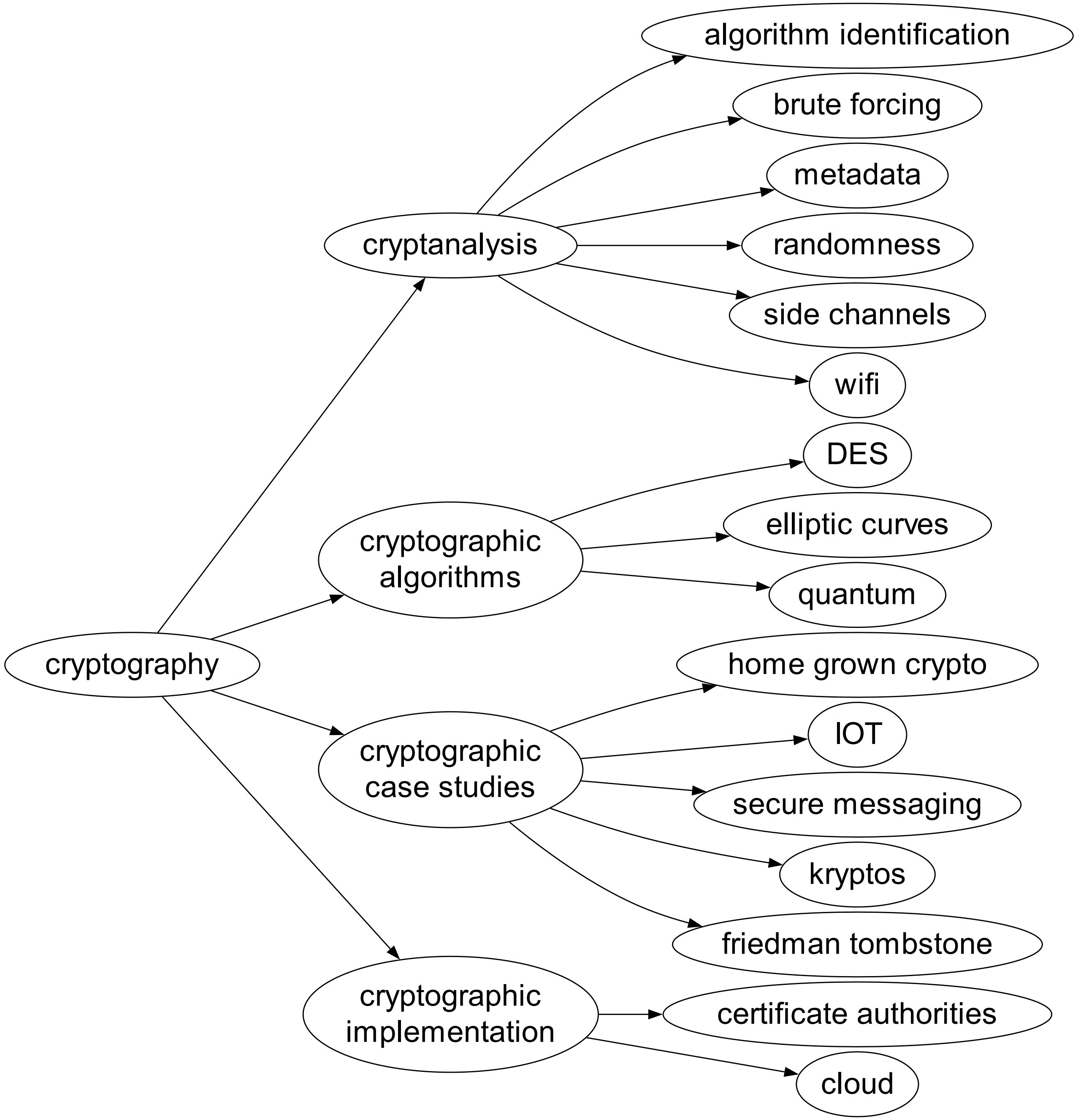
- law & policy
  - law
    - technology law
      - censorship
      - AI
      - biometrics
      - border crossings
      - breach
        - disclosure
        - liability
      - cloud computing
      - data destruction
      - encryption
      - gps tracking
      - incident response
        - attorney client privilege
      - metadata
      - open source software
      - security researchers
        - code of practice
        - legal defense fund
      - laws
        - CFAA
        - GDPR
        - Section 230
      - warrant canaries
    - law enforcement
      - law enforcement takedowns
      - law enforcement TTPs
    - law of war
      - act of war
    - legal principles
      - civil asset forfiture
      - discovery
      - search and seizure
      - treaties
  - policy
    - infosec community involvement
    - FEDRAMP
    - compliance
      - PCI compliance



Exploitation (118 talks – 5.9 talks per ShmooCon)



exploitation
AI
cloud
databases
firmware
hardware
humans
IAM
network
organizations
OS
social_networks
software
systems
tools
wireless
biotech implants
cameras
CPUs
exploitation TTPs
facility access control systems
fitness trackers
flash drives
sensors
jukeboxes
keyboards
magnetic cards
pinball machines
printers
proximity cards
USB



- cryptography
  - cryptanalysis
    - algorithm identification
    - brute forcing
    - metadata
    - randomness
    - side channels
    - wifi
  - cryptographic algorithms
    - DES
    - elliptic curves
    - quantum
  - cryptographic case studies
    - home grown crypto
    - IOT
    - secure messaging
    - kryptos
    - friedman tombstone
  - cryptographic implementation
    - certificate authorities
    - cloud

2005 /applied cryptography/? oh, i skimmed through that book once.
2006 Breaking LanMan Forever
2006 Kryptos and the Cyrillic Projector Ciphers
2007 Three Crypto Geeks on the Current State of Cryptography and the Internet
2007 Hacking the Airwaves with FPGAs
2007 Home-grown Crypto
2010 Tales from the Crypto
2012 New Cool Crypto
2013 Crypto: You're Doing It Wrong
2014 SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography
2015 How Random is Your RNG?
2015 Eliminating Timing Side-channels. A Tutorial.
2015 NaCl: A New Crypto Library
2016 Crypto and Quantum and Post Quantum
2016 Using the Algebraic Eraser to Secure Low-Power and Passive IoT Devices
2017 The State of Secure Messaging
2018 Profiling and Detecting all Things SSL with JA3
2018 The Friedman Tombstone - A Cipher in Arlington National Cemetery
2018 CertGraph: A Tool to Crawl the Graph of SSL Certificate Alternate Names using Certificate Transparency
2019 Post-quantum Crypto: Today’s defense against tomorrow’s quantum hacker
2019 Un-f*$#ing Cloud Storage Encryption
2022 Practical Crypto of InfoSec Noobs
2024 Going Meta- Pulling info from Encrypted Radios
2024 NTLMv1-SSP DES Mechanics Explained

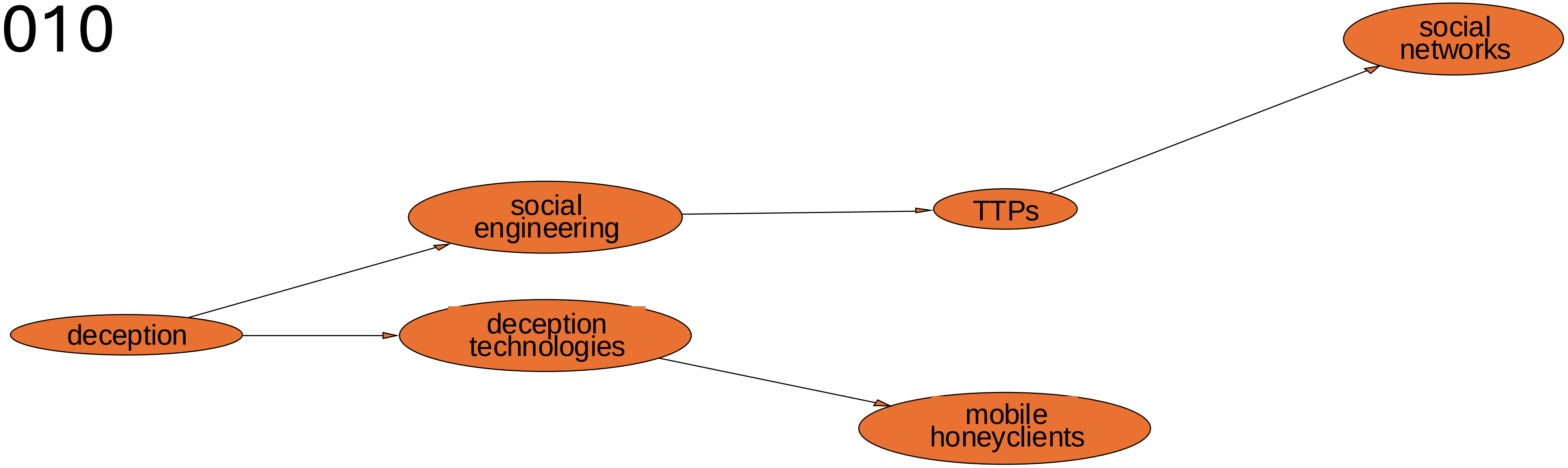
Cryptography (24 talks – 1.2 talks per ShmooCon)

2005-2009

No talks

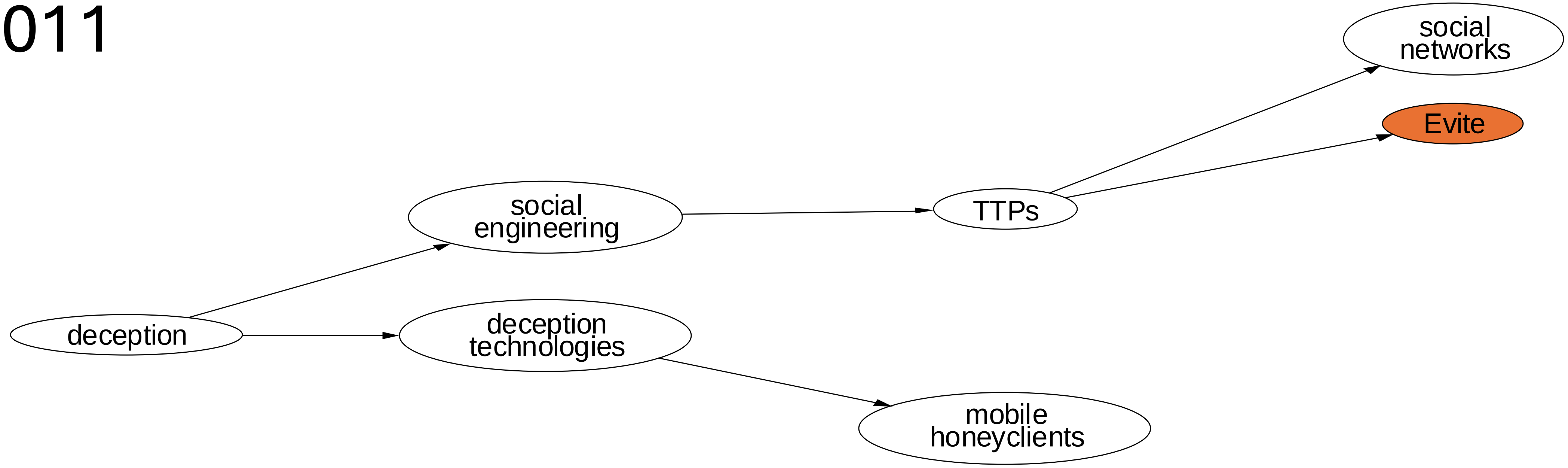
Deception (13 talks – 0.65 talks per ShmooCon)

2010



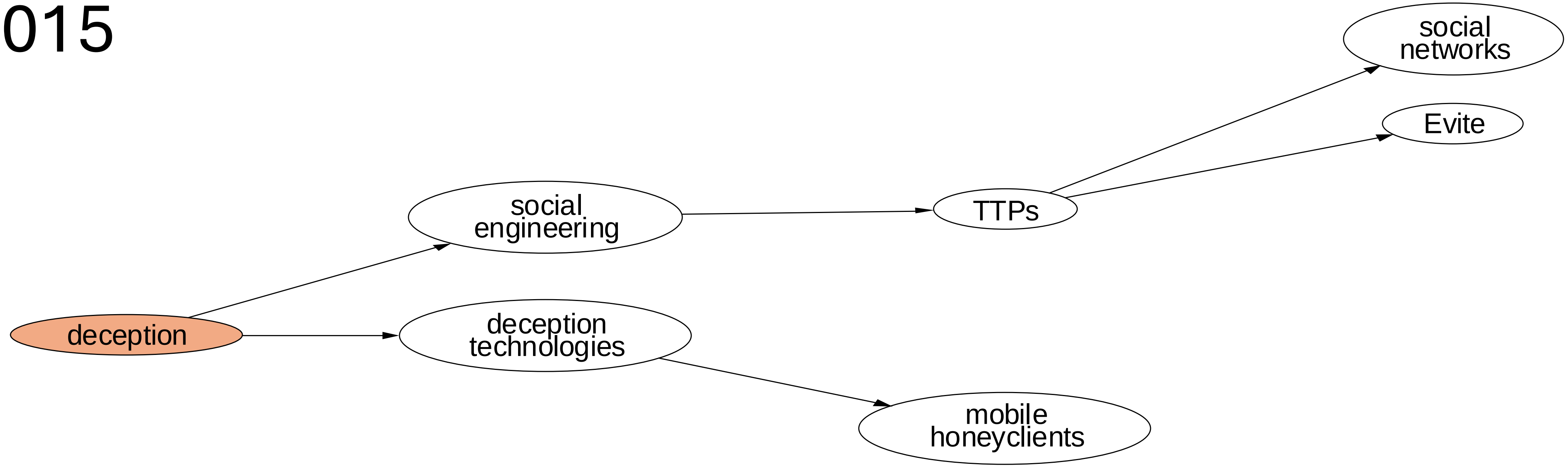
2010 Social Zombies II: Your Friends Need More Brains	deception -> social_engineering -> TTPs -> social_networks
2010 honeyM: A Framework For Virtual Mobile Device Honeyclients	deception -> deception_technologies -> mobile_honeyclients

2011



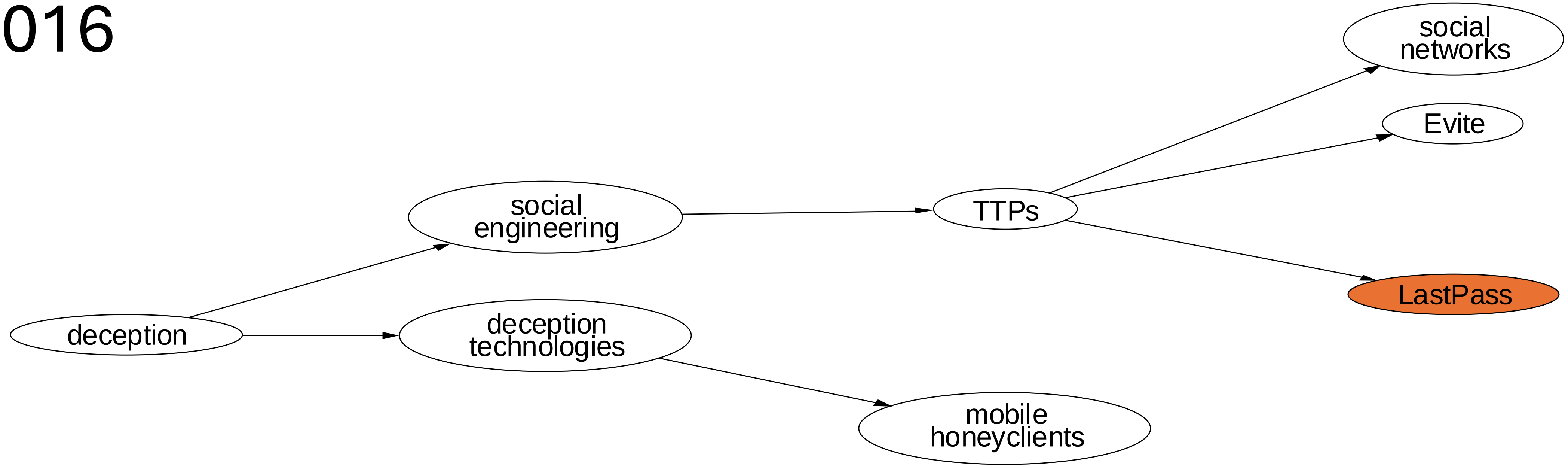
2010 Social Zombies II: Your Friends Need More Brains	deception -> social_engineering -> TTPs -> social_networks
2010 honeyM: A Framework For Virtual Mobile Device Honeyclients	deception -> deception_technologies -> mobile_honeyclients
2011 An Evite from Surbo? Probably an invitation for trouble	**deception -> social_engineering -> TTPs -> evite**

2015



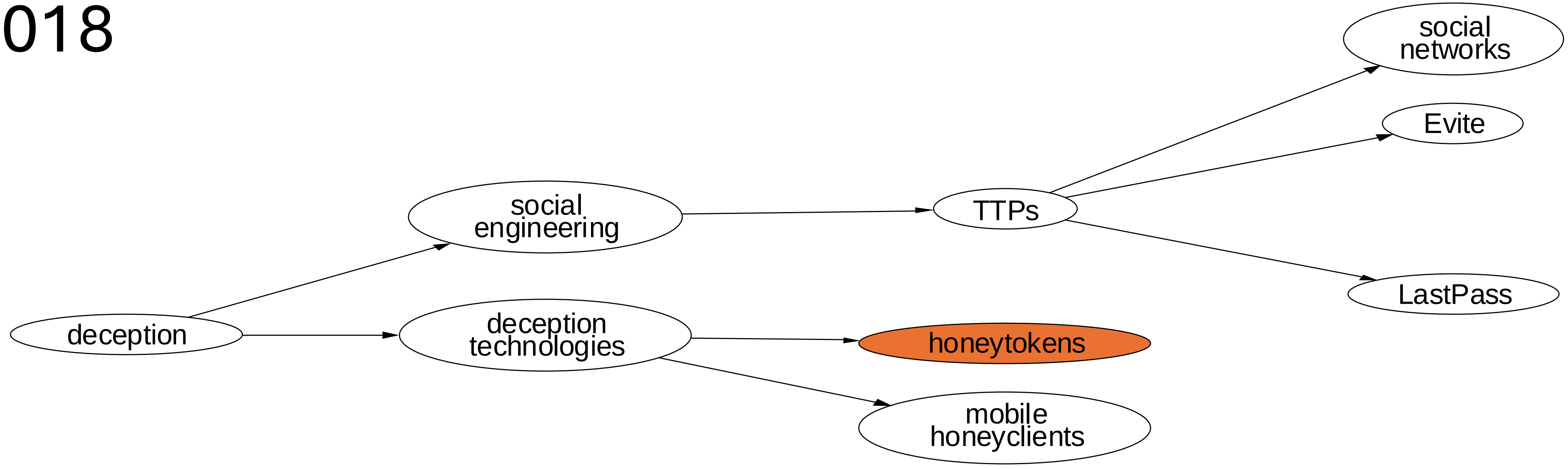
2010 Social Zombies II: Your Friends Need More Brains	deception -> social_engineering -> TTPs -> social_networks
2010 honeyM: A Framework For Virtual Mobile Device Honeyclients	deception -> deception_technologies -> mobile_honeyclients
2011 An Evite from Surbo? Probably an invitation for trouble	deception -> social_engineering -> TTPs -> evite
2015 Deception for the Cyber Defender: To Err is Human; to Deceive, Divine	deception

2016



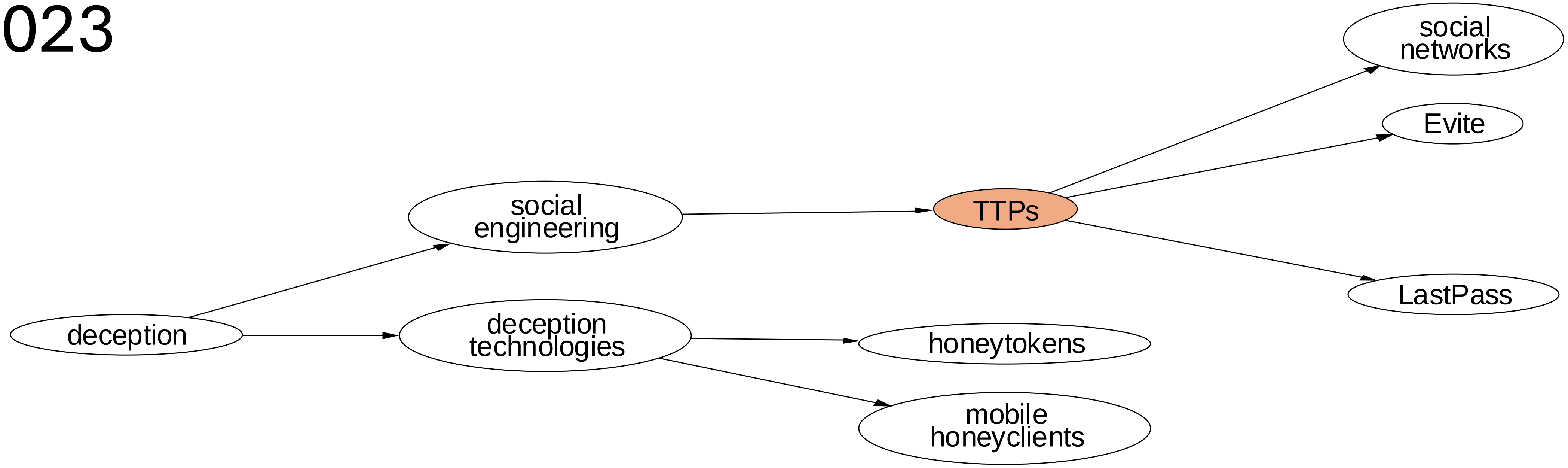
2010	Social Zombies II: Your Friends Need More Brains	deception -> social_engineering -> TTPs -> social_networks
2010	honeyM: A Framework For Virtual Mobile Device Honeyclients	deception -> deception_technologies -> mobile_honeyclients
2011	An Evite from Surbo? Probably an invitation for trouble	deception -> social_engineering -> TTPs -> evite
2015	Deception for the Cyber Defender: To Err is Human; to Deceive, Divine	deception
2016	**LostPass: Pixel-perfect LastPass Phishing**	**deception -> social_engineering -> TTPs -> last_pass**

2018



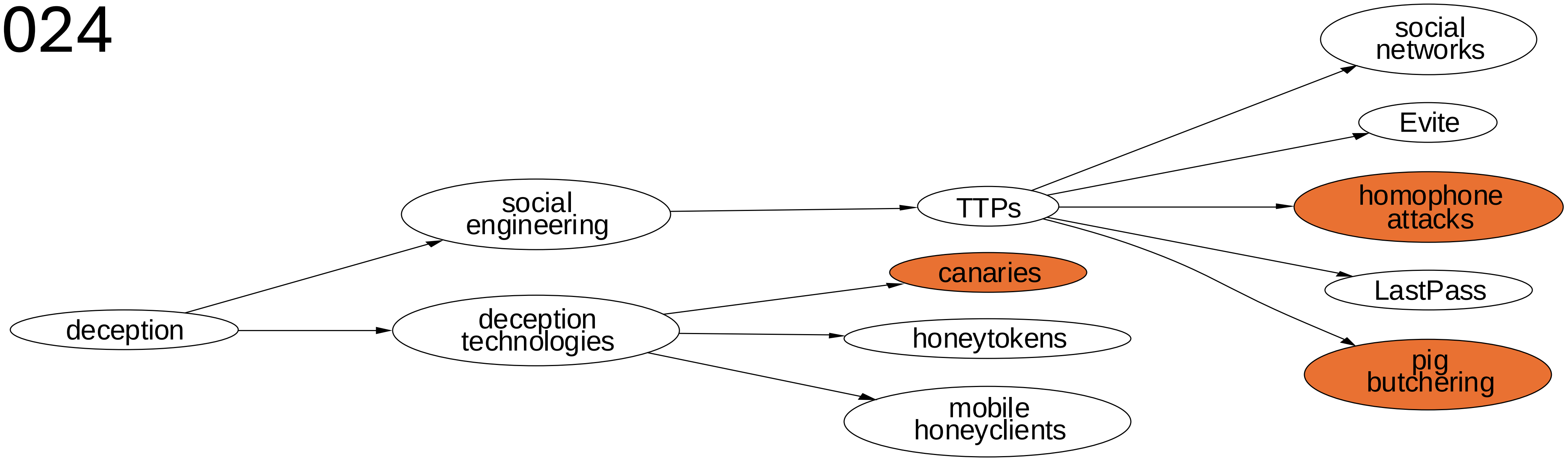
2010	Social Zombies II: Your Friends Need More Brains	deception -> social_engineering -> TTPs -> social_networks
2010	honeyM: A Framework For Virtual Mobile Device Honeyclients	deception -> deception_technologies -> mobile_honeyclients
2011	An Evite from Surbo? Probably an invitation for trouble	deception -> social_engineering -> TTPs -> evite
2015	Deception for the Cyber Defender: To Err is Human; to Deceive, Divine	deception
2016	LostPass: Pixel-perfect LastPass Phishing	deception -> social_engineering -> TTPs -> last_pass
2018	**AWS Honey Tokens with SPACECRAB**	**deception -> deception_technologies -> honeytokens**

2023



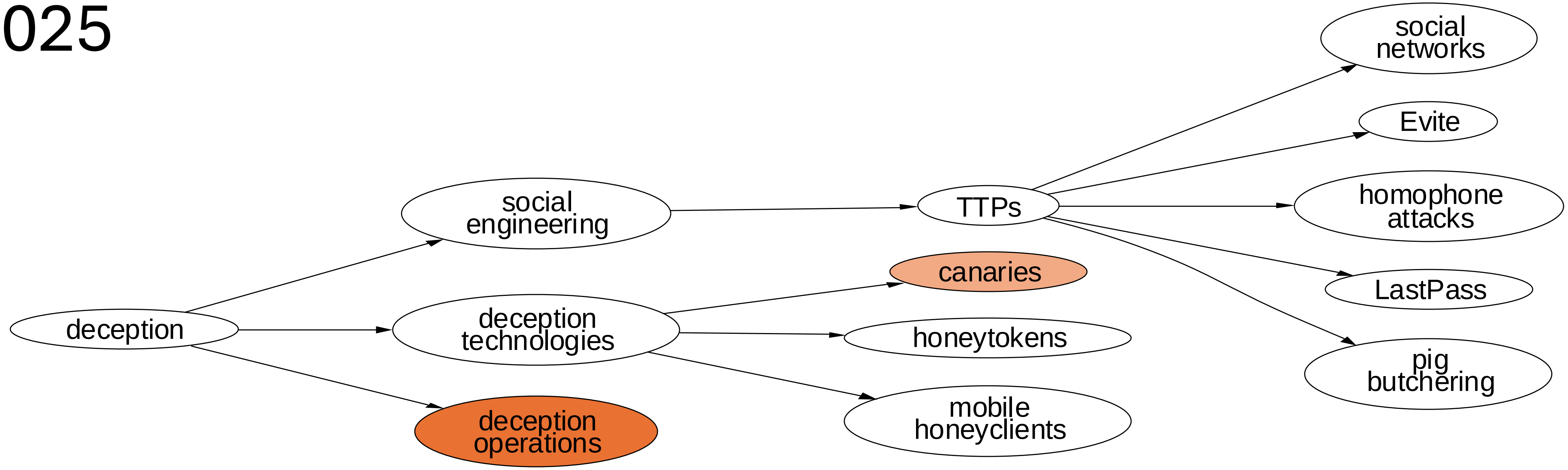
2010	Social Zombies II: Your Friends Need More Brains	deception -> social_engineering -> TTPs -> social_networks
2010	honeyM: A Framework For Virtual Mobile Device Honeyclients	deception -> deception_technologies -> mobile_honeyclients
2011	An Evite from Surbo? Probably an invitation for trouble	deception -> social_engineering -> TTPs -> evite
2015	Deception for the Cyber Defender: To Err is Human; to Deceive, Divine	deception
2016	LostPass: Pixel-perfect LastPass Phishing	deception -> social_engineering -> TTPs -> last_pass
2018	AWS Honey Tokens with SPACECRAB	deception -> deception_technologies -> honeytokens
2023	**Putting on a Big Show: Defending by Attacking Attacker Incentives**	**deception -> social_engineering -> TTPs**
2023	**Social Engineering from the Detective Perspective**	**deception -> social_engineering -> TTPs**

2024

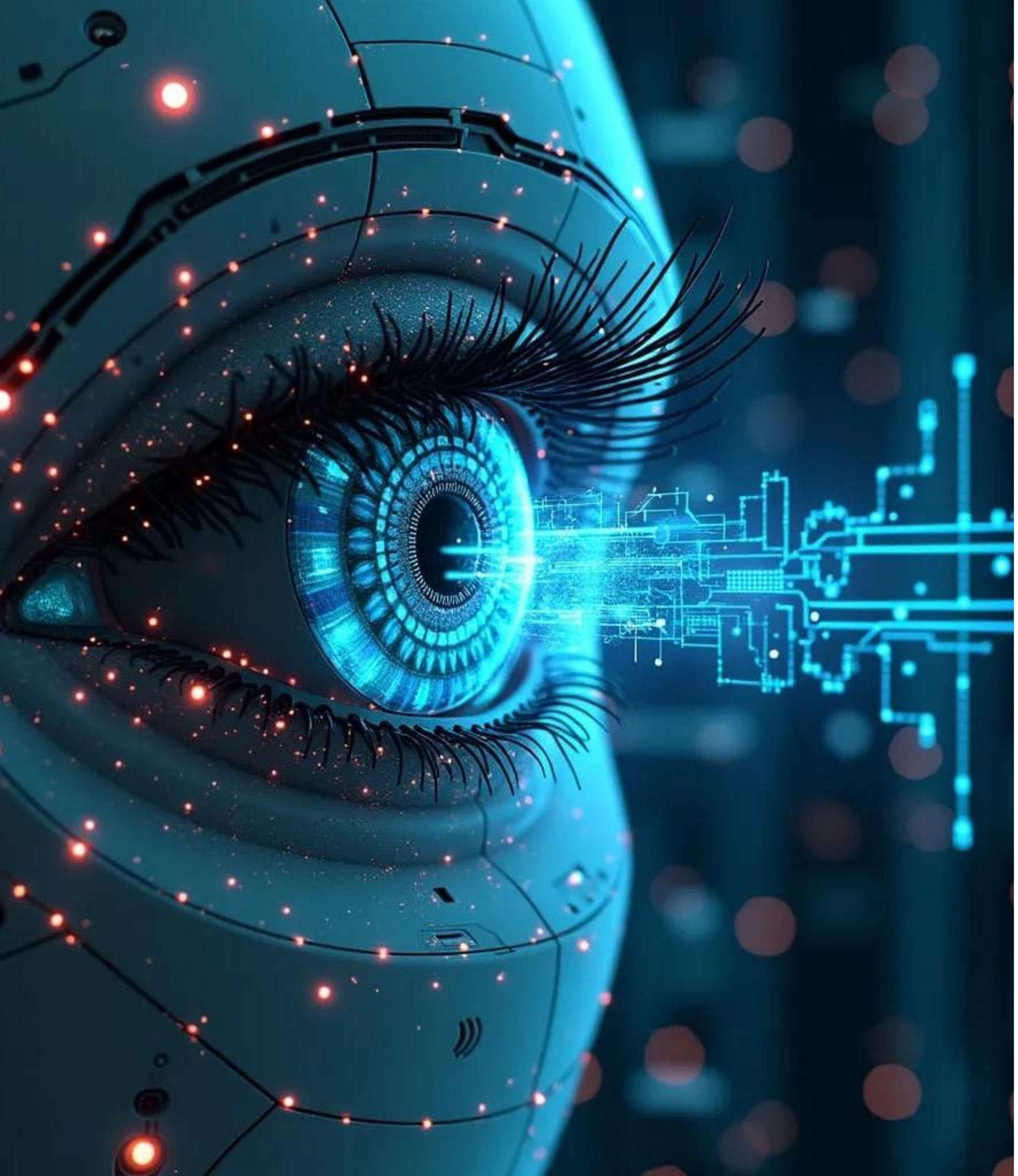


2010	Social Zombies II: Your Friends Need More Brains	deception -> social_engineering -> TTPs -> social_networks
2010	honeyM: A Framework For Virtual Mobile Device Honeyclients	deception -> deception_technologies -> mobile_honeyclients
2011	An Evite from Surbo? Probably an invitation for trouble	deception -> social_engineering -> TTPs -> evite
2015	Deception for the Cyber Defender: To Err is Human; to Deceive, Divine	deception
2016	LostPass: Pixel-perfect LastPass Phishing	deception -> social_engineering -> TTPs -> last_pass
2018	AWS Honey Tokens with SPACECRAB	deception -> deception_technologies -> honeytokens
2023	Putting on a Big Show: Defending by Attacking Attacker Incentives	deception -> social_engineering -> TTPs
2023	Social Engineering from the Detective Perspective	deception -> social_engineering -> TTPs
2024	**Ewe Cant Trusst Yore Eers: An Overview Homophone Attacks**	**deception -> social_engineering -> TTPs -> homophone_attacks**
2024	**Bad Romance: The TTPs of "pig butchering" scammers**	**deception -> social_engineering -> TTPs -> pig_butchering**
2024	**Building Canaries with ELK and ElastAlert**	**deception -> deception_technologies -> canaries**

2025

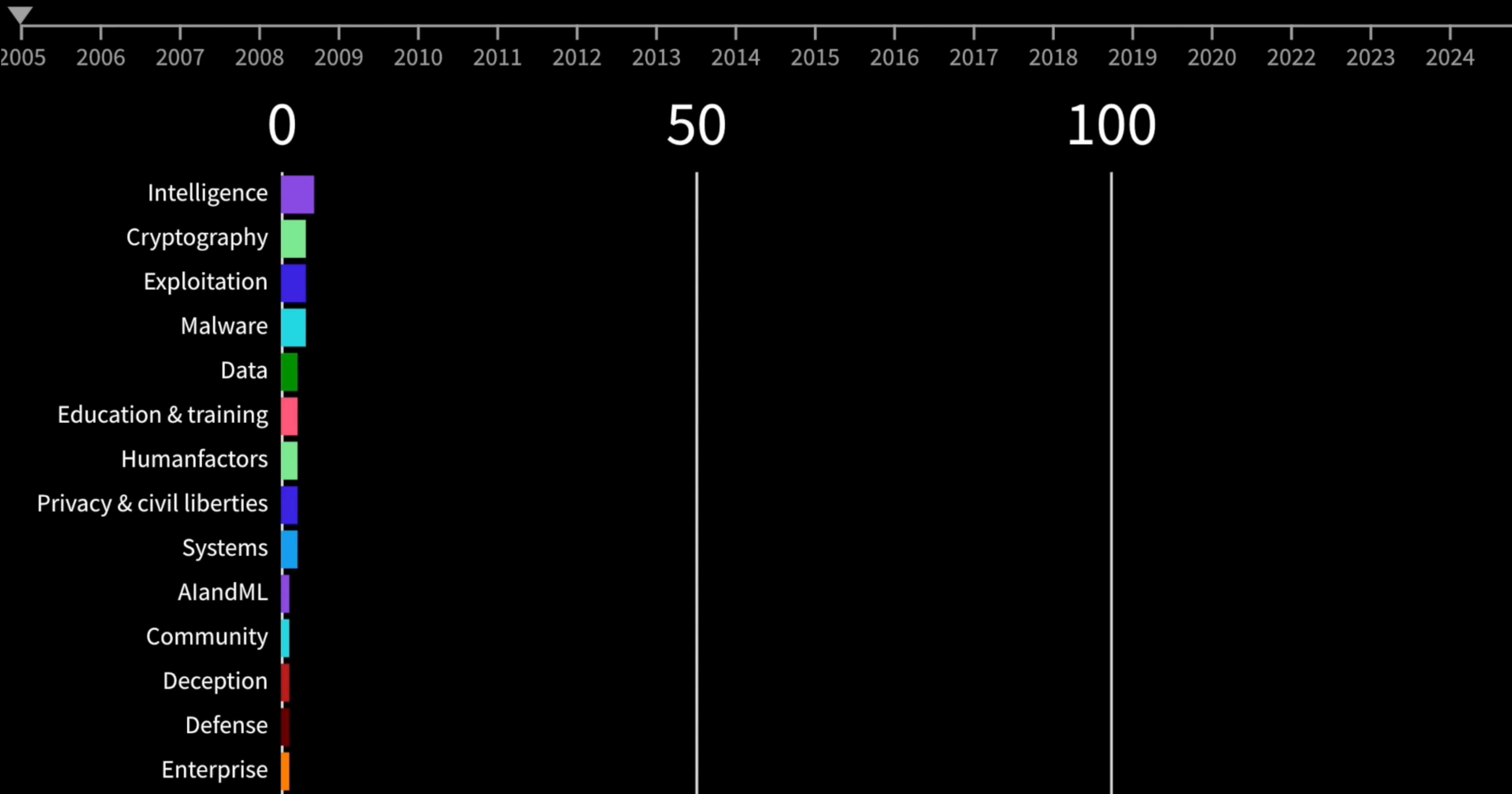


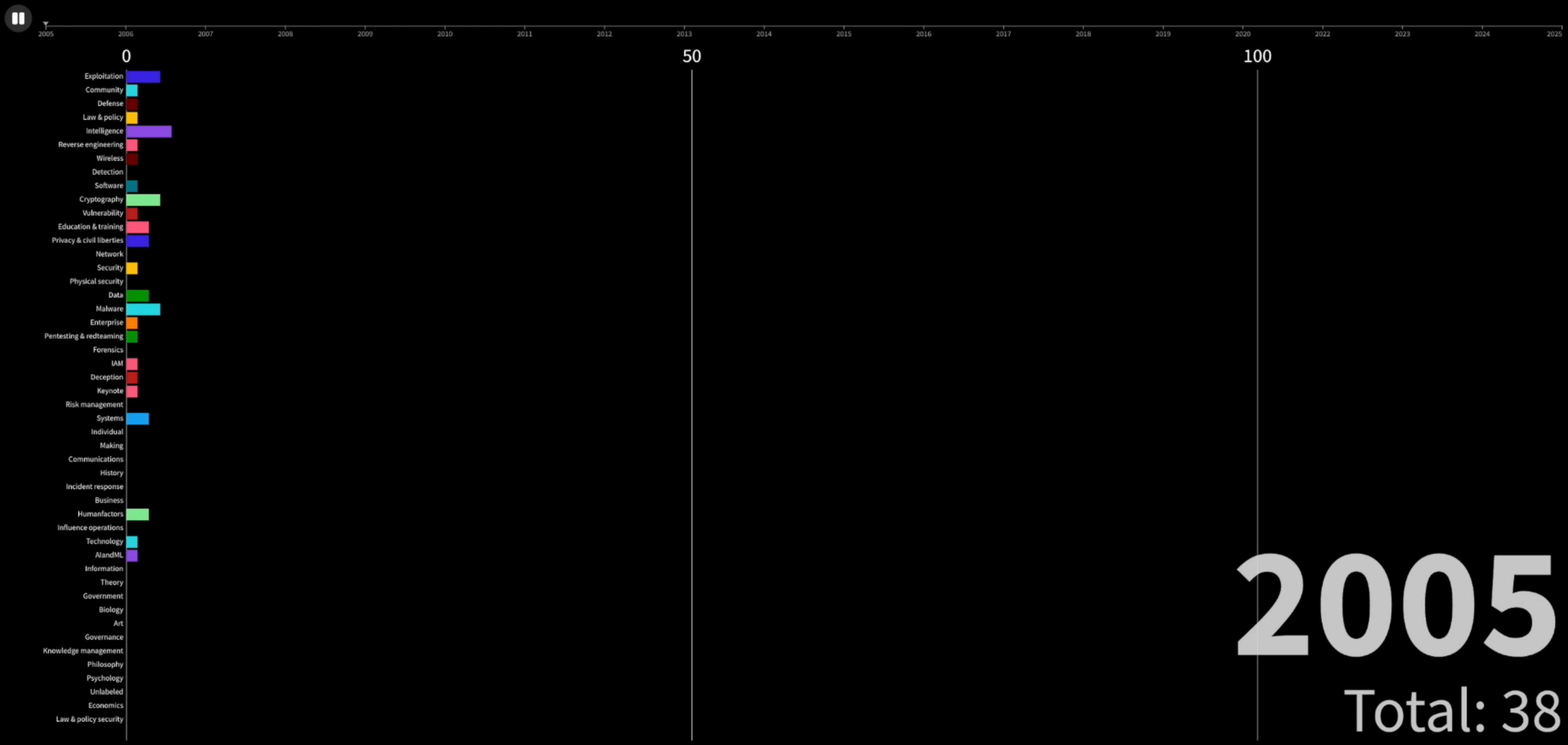
2010	Social Zombies II: Your Friends Need More Brains	deception -> social_engineering -> TTPs -> social_networks
2010	honeyM: A Framework For Virtual Mobile Device Honeyclients	deception -> deception_technologies -> mobile_honeyclients
2011	An Evite from Surbo? Probably an invitation for trouble	deception -> social_engineering -> TTPs -> evite
2015	Deception for the Cyber Defender: To Err is Human; to Deceive, Divine	deception
2016	LostPass: Pixel-perfect LastPass Phishing	deception -> social_engineering -> TTPs -> last_pass
2018	AWS Honey Tokens with SPACECRAB	deception -> deception_technologies -> honeytokens
2023	Putting on a Big Show: Defending by Attacking Attacker Incentives	deception -> social_engineering -> TTPs
2023	Social Engineering from the Detective Perspective	deception -> social_engineering -> TTPs
2024	Ewe Cant Trusst Yore Eers: An Overview Homophone Attacks	deception -> social_engineering -> TTPs -> homophone_attacks
2024	Bad Romance: The TTPs of "pig butchering" scammers	deception -> social_engineering -> TTPs -> pig_butchering
2024	Building Canaries with ELK and ElastAlert	deception -> deception_technologies -> canaries
2025	**Deception & Operations Planning Frameworks**	**deception -> deception_operations**
2025	**Windows Projected File System — The Reality Stone**	**deception -> deception_technologies -> canaries**



Insights

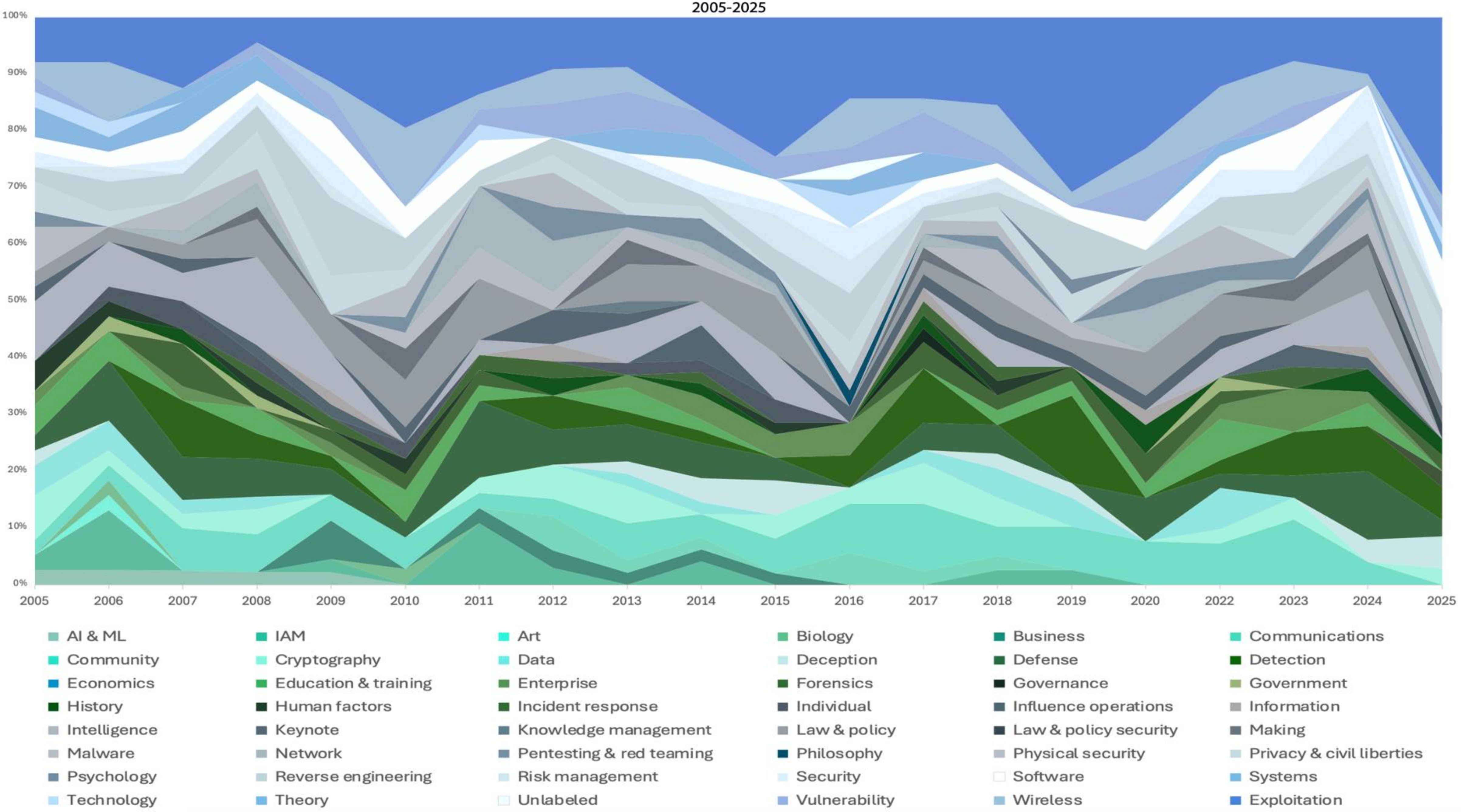
- From chips to the entire internet and space!
- Taxonomy didn’t converge
- Other hacker conferences are compatible
- A fully connected graph? An ontology?
- Leaf nodes point to interesting open problems
- Future community research would fill out the taxonomy and graph in amazing ways


2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2022
2023
2024
0
50
100
Intelligence
Cryptography
Exploitation
Malware
Data
Education & training
Humanfactors
Privacy & civil liberties
Systems
AIandML
Community
Deception
Defense
Enterprise



ShmooCon talks by topic

SHMOOCON
2005-2025



SHMOOCON
2005-2025
KOPIDION

Future work

- Refine and expand the dataset
- Refine and expand the taxonomy
- Apply to other hacker conferences
- Automation opportunities
- Integration opportunities

Takeaways

- A huge thank you to ShmooCon!
- We are living in a golden age of hacking, let’s document it
- Archive content and meta-data now… the future will thank you
- Standardize a taxonomy and normalize author labeling at inception
- Support archivists and archive sites
- Lots of opportunity for future work
- Try this yourself, it’s an excellent learning experience

Sources

ShmooCon's conference website

Internet Archive's ShmooCon archive and Wayback Machine

Thinkst's conference archive

InfoConDB's conference archive

Edward Tufte's Popular Music: The Classic Graphic by Reebee Garofalo

Rebee Garafalo's Genealogy of Pop/Rock Music

YouTube's ShmooCon videos

InfoCon's conference archive

Exploding the Phone's YIPL/TAP Phone Phreak Convention Flyers

To explore further

Heidi Potter's 0wn the C0n talks at ShmooCon

Jason Scott's A History of Hacker Conferences, DEFCON Documentary and works

Nick Percoco and Jonathan Tomek's The History of the Thotcon Hacking Conference

Ashley Schwartau's Hackers are People Too

Computer History Museum's Timeline of Computer History

RSA talk on RSA talks using AI (source?)

DEFCON's Media Server

Taxonomies: NIST's Cybersecurity Framework, ACM's Computing Classification System, IEEE's Taxonomy, Purdue's New Hacker Taxonomy, European Commission's **Cybersecurity Taxonomy**

Download poster, art, slides, code, and dataset here…

https://kopidion.com/projects.html

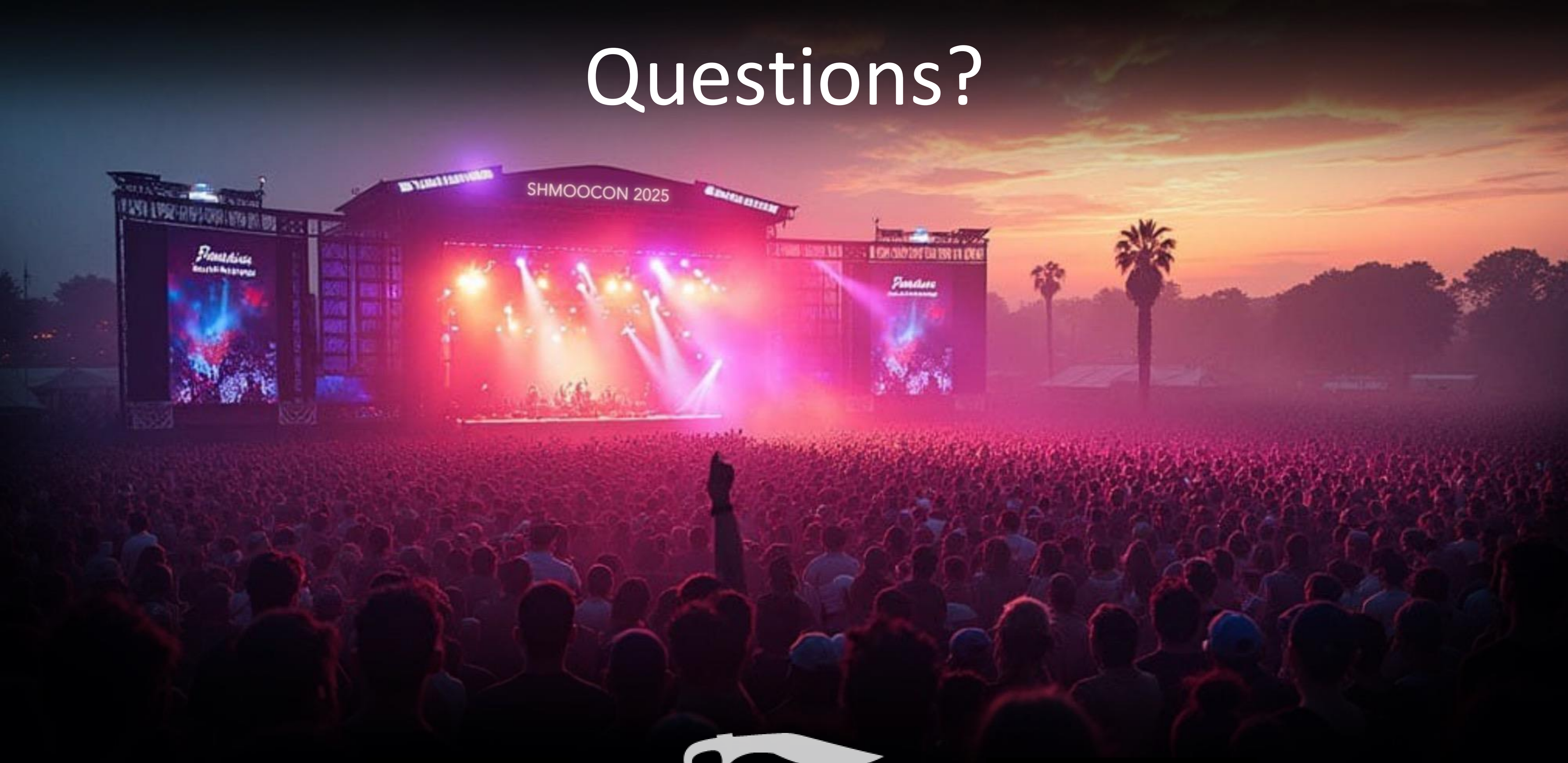
A heartfelt tip o’ the hat

To all the people who make ShmooCon happen!

Internet Archive
InfoConDB and InfoCon
Thinkst
GraphViz sandbox

0xdade
Christiaan008
Heidi Potter
Bruce Potter
Jason Scott
Joe Adams
Tom Cross
Jack Daniel

Questions?



Greg Conti

KOPIDION

Danielle Scalera

KOPIDION.COM

backup slides

Future work – detailed

Refining and expanding the dataset
Add speakers and demographics
Add other conferences and beyond
Fix errors

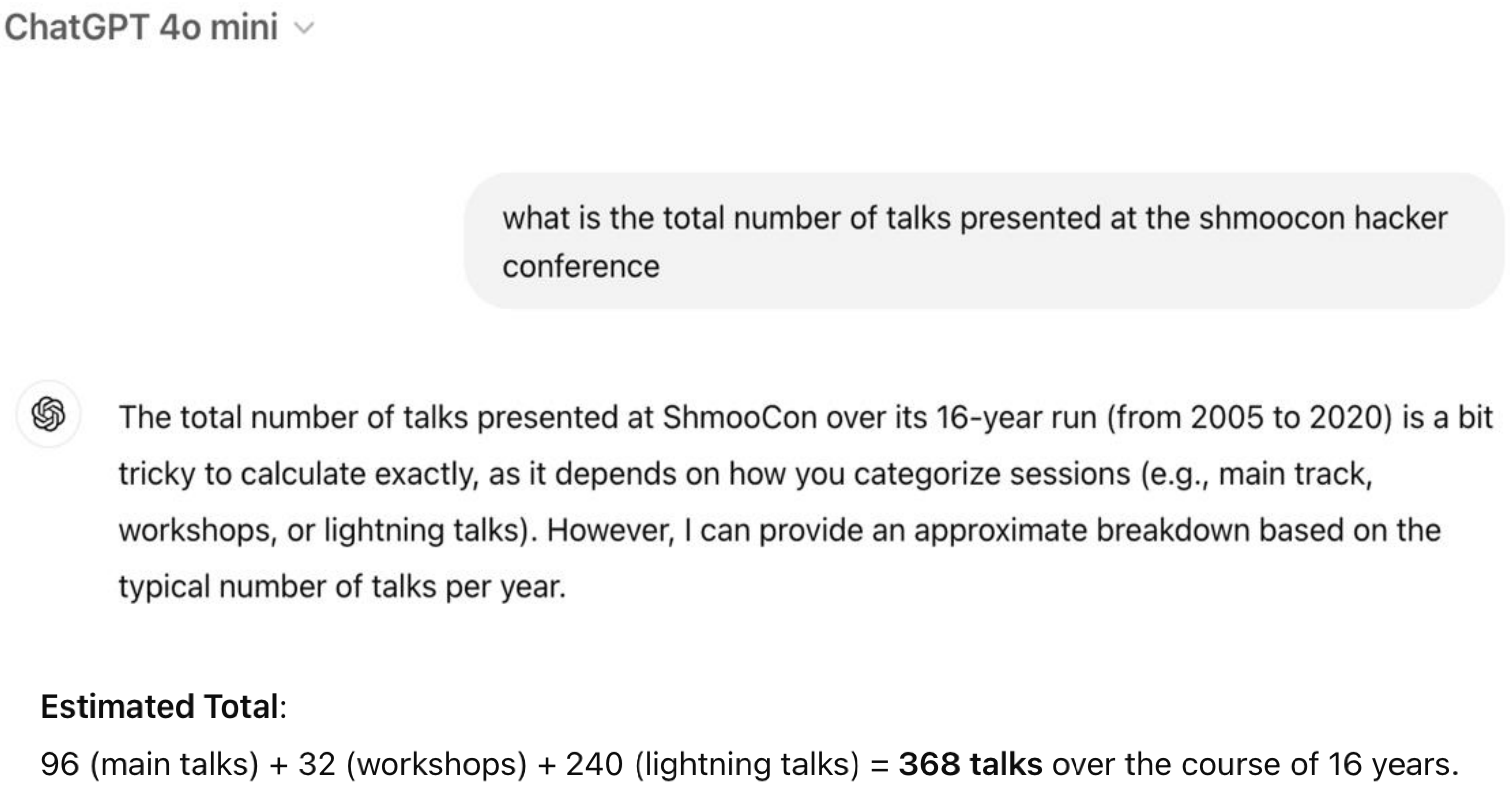
Refining and expanding the taxonomy
Finer grain resolution of taxonomy categories
Revise and tune categories
Go from emergent to comprehensive
Consider other nearby taxonomies and frameworks for new ideas
Conduct formal validation of taxonomy

Analysis opportunities
Research arcs by speaker over time
Use of LLMs and other automation to assist
Analyze multiple cons

Integration opportunities
Can the process be automated (AI or otherwise)
Integrate analysis techniques into archive sites
Standardize process to have authors' self-label at inception
Create norm that all content and metadata must be archived

Other
Support existing archive sites
There is a nice research paper here, perhaps a master's thesis

Why not AI? Today is not the day.



ChatGPT 4o mini

what is the total number of talks presented at the shmoocon hacker conference

The total number of talks presented at ShmooCon over its 16-year run (from 2005 to 2020) is a bit tricky to calculate exactly, as it depends on how you categorize sessions (e.g., main track, workshops, or lightning talks). However, I can provide an approximate breakdown based on the typical number of talks per year.

Estimated Total:

96 (main talks) + 32 (workshops) + 240 (lightning talks) = **368 talks** over the course of 16 years.