

Security Visualization Past, Present, Future

Greg Conti
West Point
@cyberbgone

Disclaimer



The views expressed in this talk are those of the author and do not reflect the official policy or position of West Point, the Department of the Army, the Department of Defense, or the United States Government.



<http://vizsec.dbvis.de/>

VizSec Body of Work

All (149) Papers: 149 / 149

2014 (12)

2013 (9)

2012 (12)

2011 (6)

2010 (12)

2009 (10)


2008 (18)


2007 (16)


2006 (19)


2005 (16)


2004 (19)


 *Daniel Best, Alex Endert, Daniel Kidwell*
7 Key Challenges for Visualization in Cyber Network Defense (2014)
VizSec 2014 - DOI: 10.1145/2671491.2671497
What does it take to be a successful visualization in cyber security? This question has been explore ...

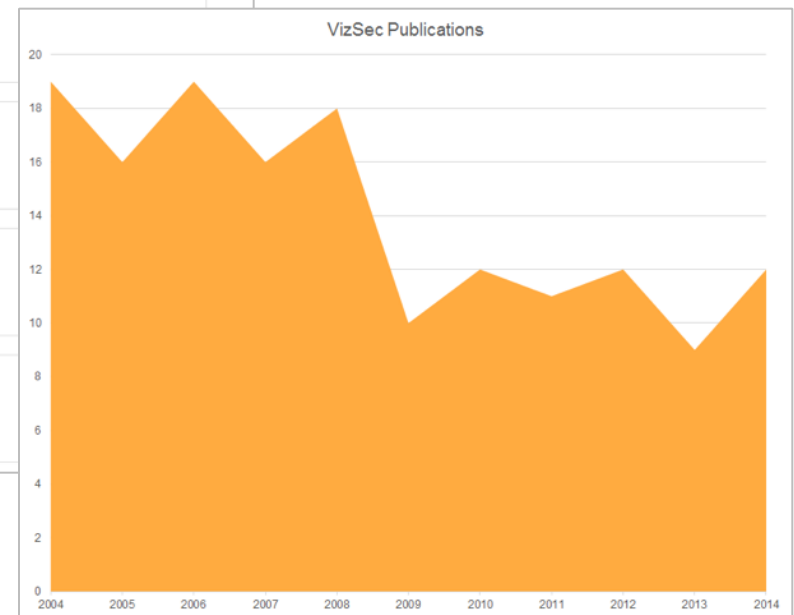
 *Christopher Humphries, Nicolas Prigent, Christophe Bidan, Frédéric Majorczyk*
CORGI: Combination, Organization and Reconstruction through Graphical Interactions (2014)
VizSec 2014 - DOI: 10.1145/2671491.2671494
In this article, we present CORGI, a security-oriented log visualization tool that allows security e ...

 *Tobias Wüchner, Alexander Pretschner, Martin Ochoa*
DAVAST: Data-centric Activity Visualization at the System Level (2014)
VizSec 2014 - DOI: 10.1145/2671491.2671499
Host-based intrusion detection systems need to be complemented by analysis tools that help understand ...

 *Alexander Long, Josh Saxe, Robert Gove*
Detecting Malware Samples with Similar Image Sets (2014)
VizSec 2014 - DOI: 10.1145/2671491.2671500
This paper proposes a method for identifying and visualizing similarity relationships between malwar ...

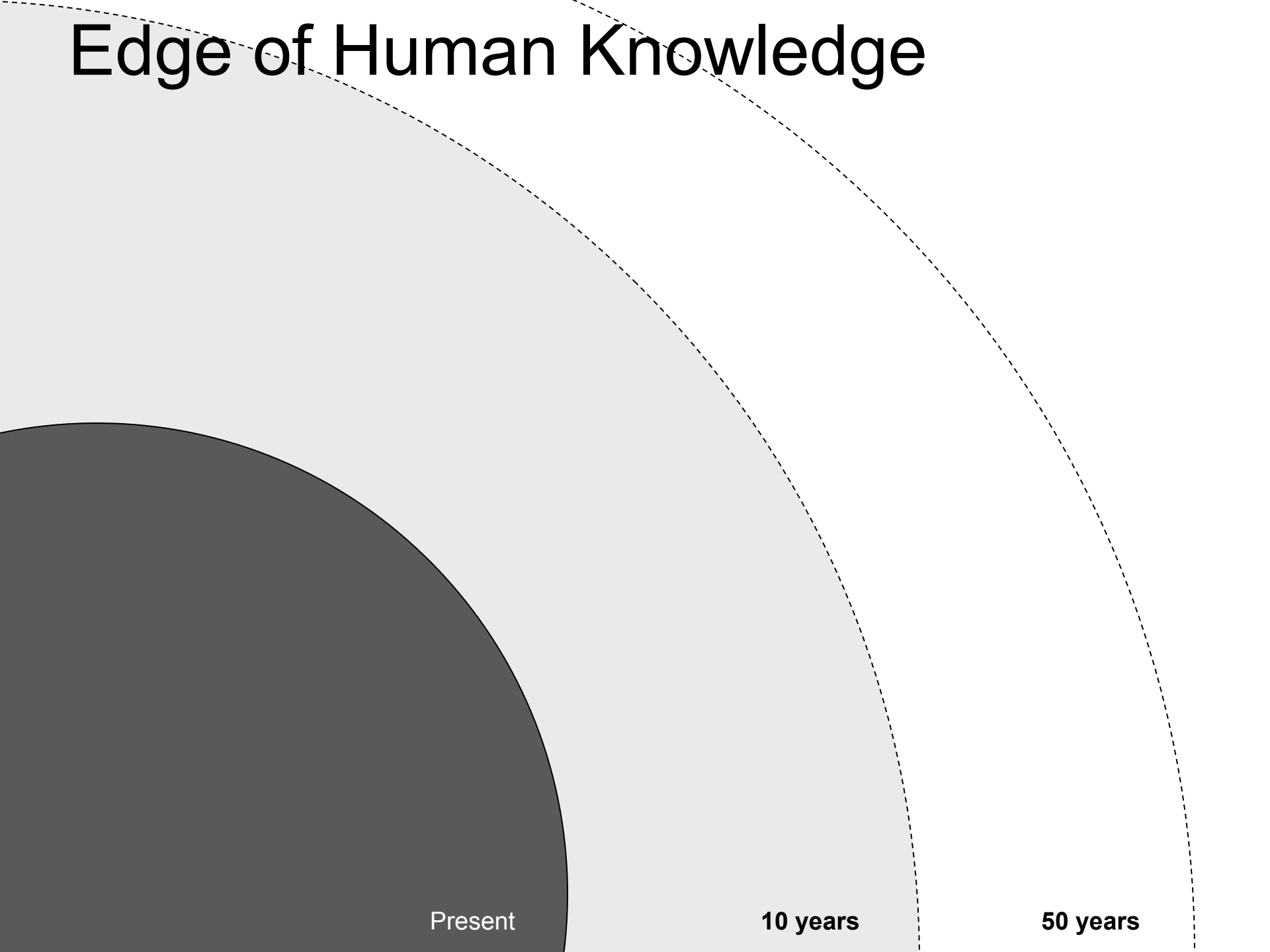
 *J. Joseph Fowler, Thienne Johnson, Paolo Simonetto, Michael Schneider, Carlos Acedo, Stephen Kobourov, Loukas Lazos*
IMap: Visualizing Network Activity over Internet Maps (2014)
VizSec 2014 - DOI: 10.1145/2671491.2671501
We propose a novel visualization, IMap, which enables the detection of security threats by visualizi ...

 *Simon Walton, Eamonn Maguire, Min Chen*
Multiple Queries with Conditional Attributes (QCATs) for Anomaly Detection and Visualization (2014)
VizSec 2014 - DOI: 10.1145/2671491.2671502
This paper describes a visual analytics method for visualizing the effects of multiple anomaly detec ...



<http://vizsec.dbvis.de/>

Edge of Human Knowledge

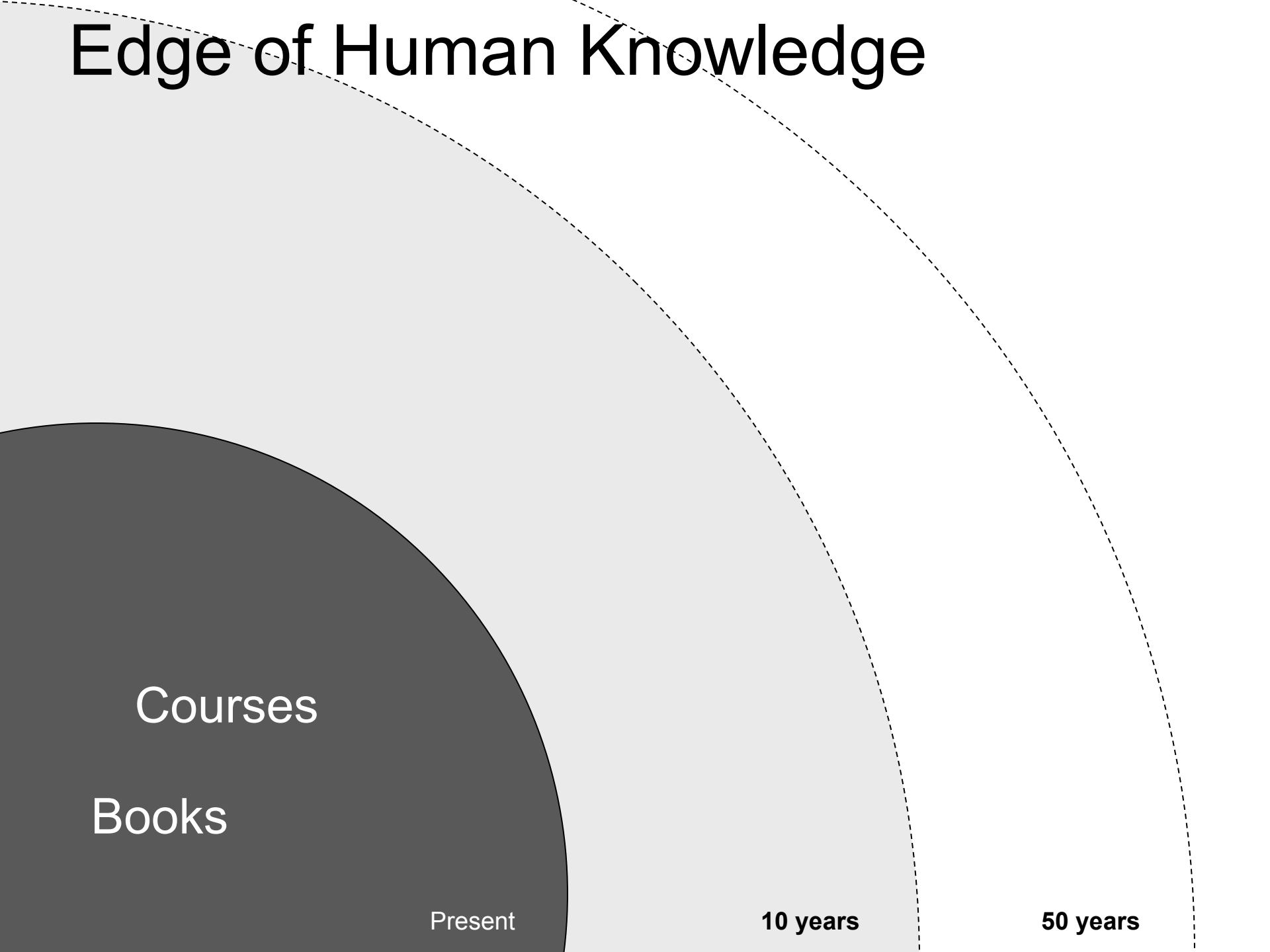


Present

10 years

50 years

Edge of Human Knowledge



Courses

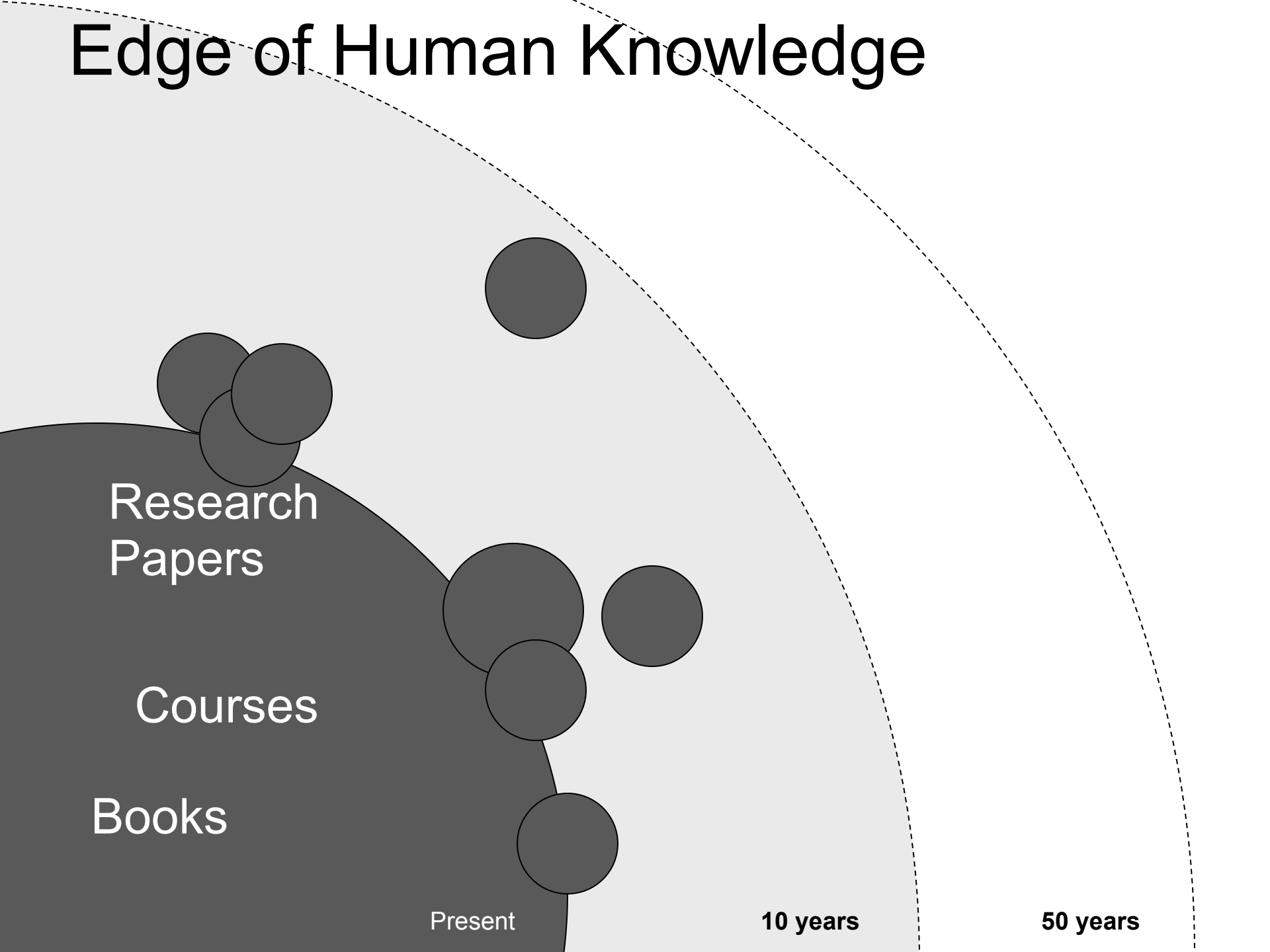
Books

Present

10 years

50 years

Edge of Human Knowledge



Research
Papers

Courses

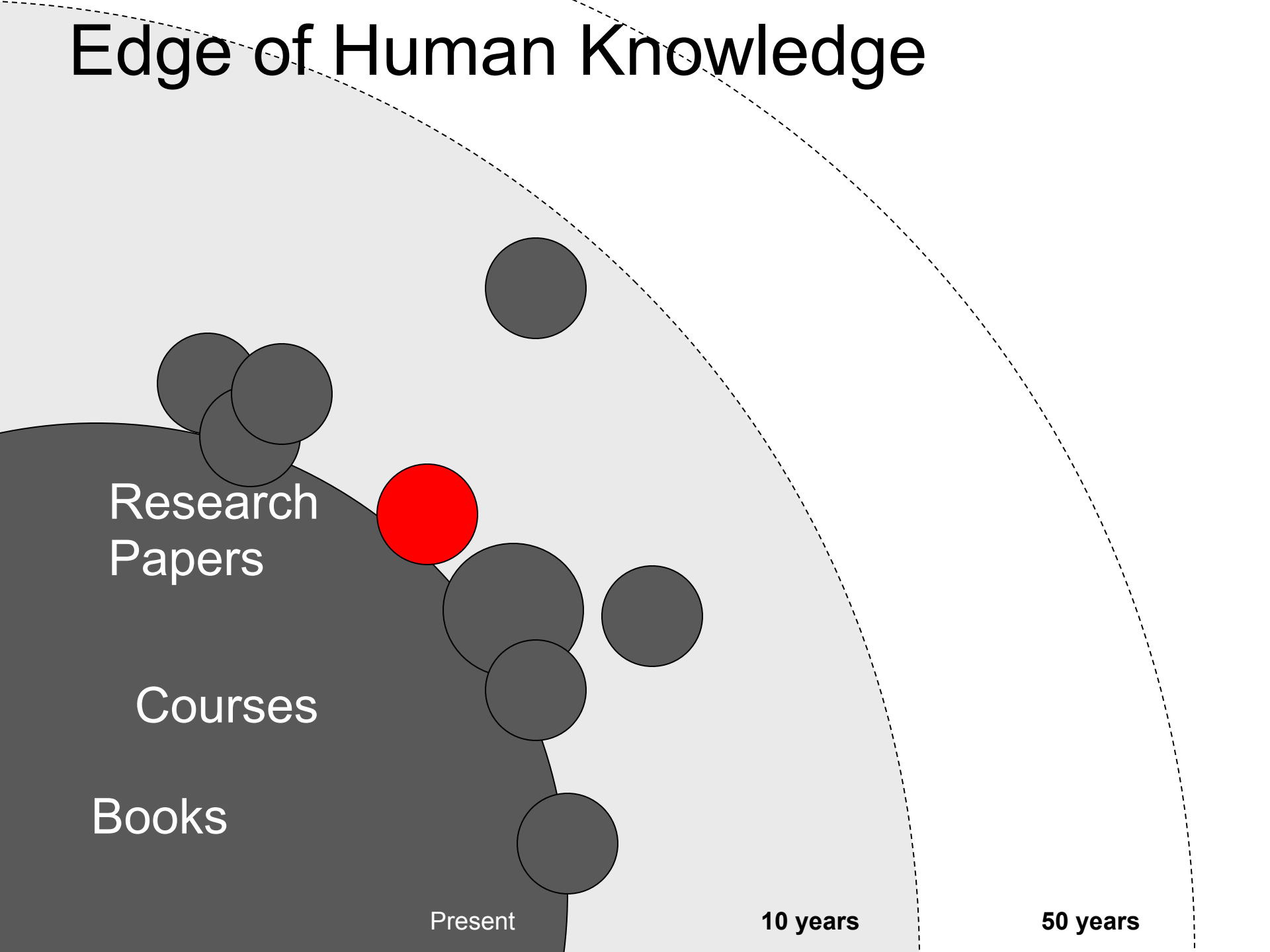
Books

Present

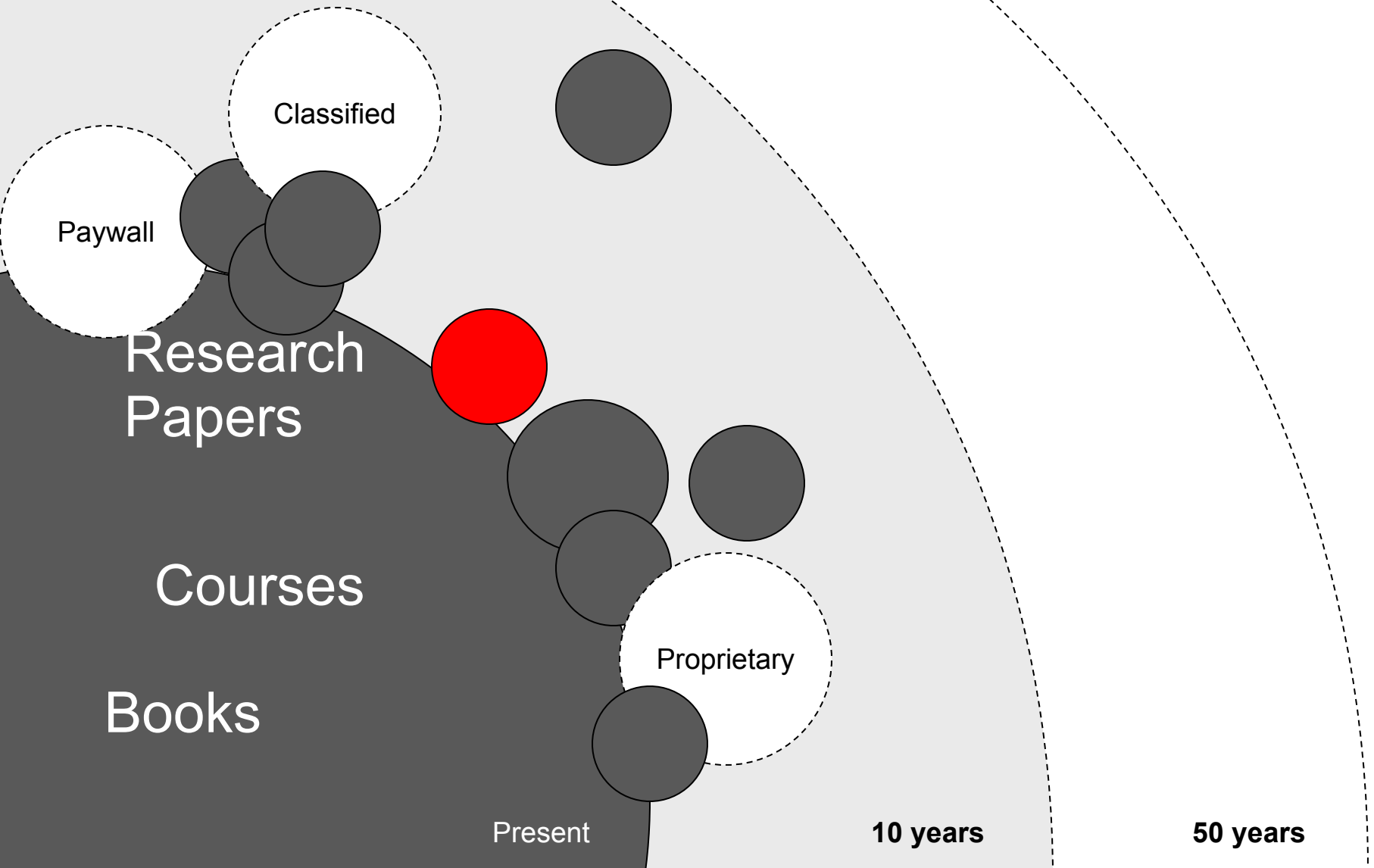
10 years

50 years

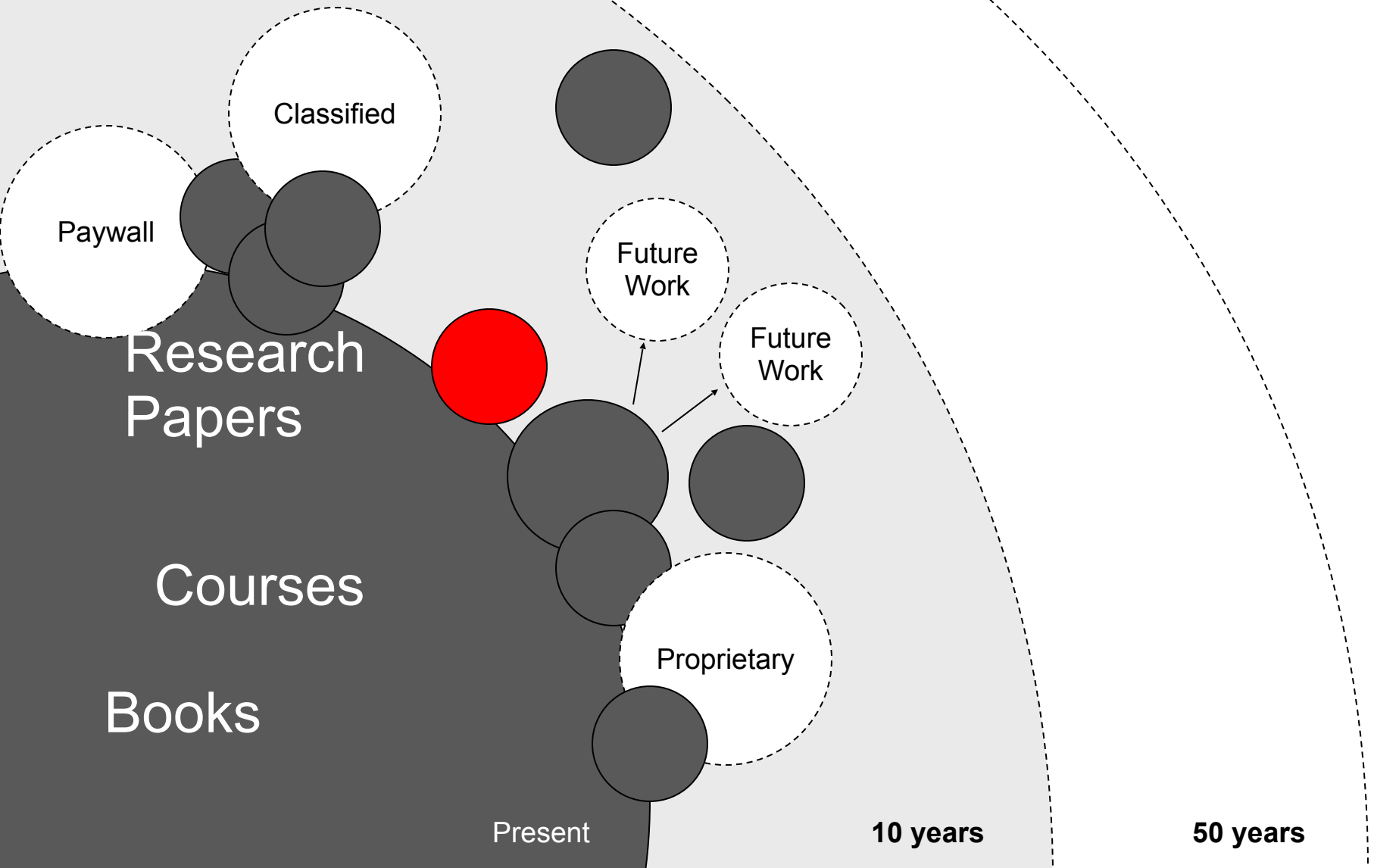
Edge of Human Knowledge



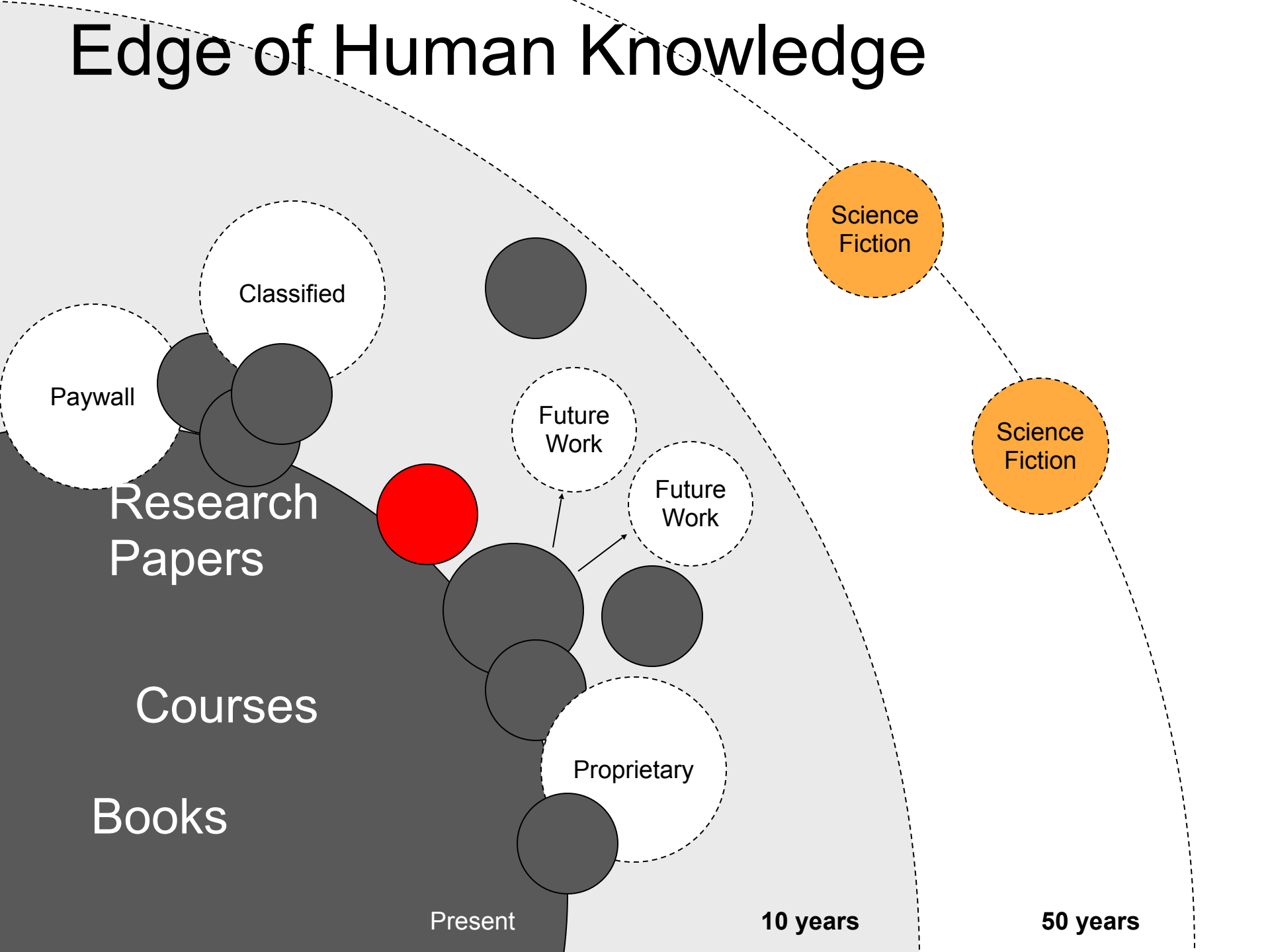
Edge of Human Knowledge



Edge of Human Knowledge



Edge of Human Knowledge



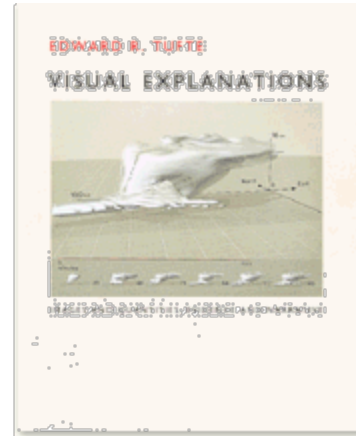
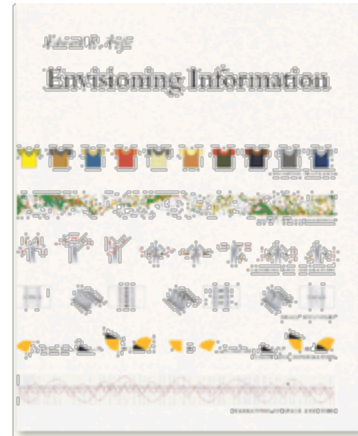
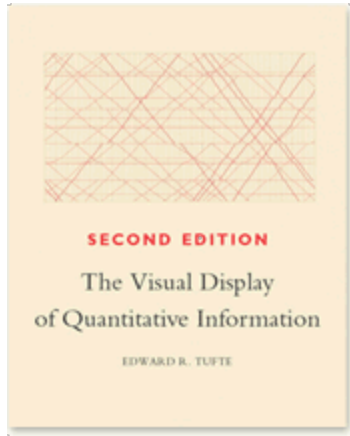


Past

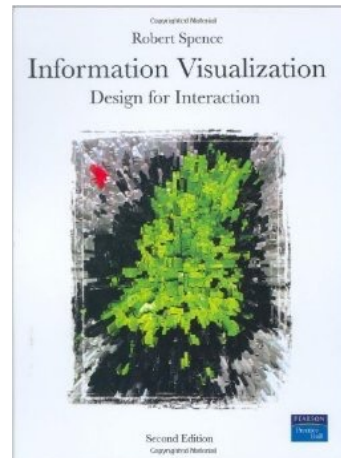
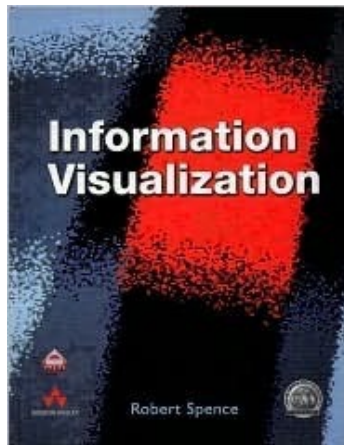
1996 - Shneiderman's Mantra

*Overview first,
zoom and filter,
then details-on demand.*

General Purpose Information Visualization



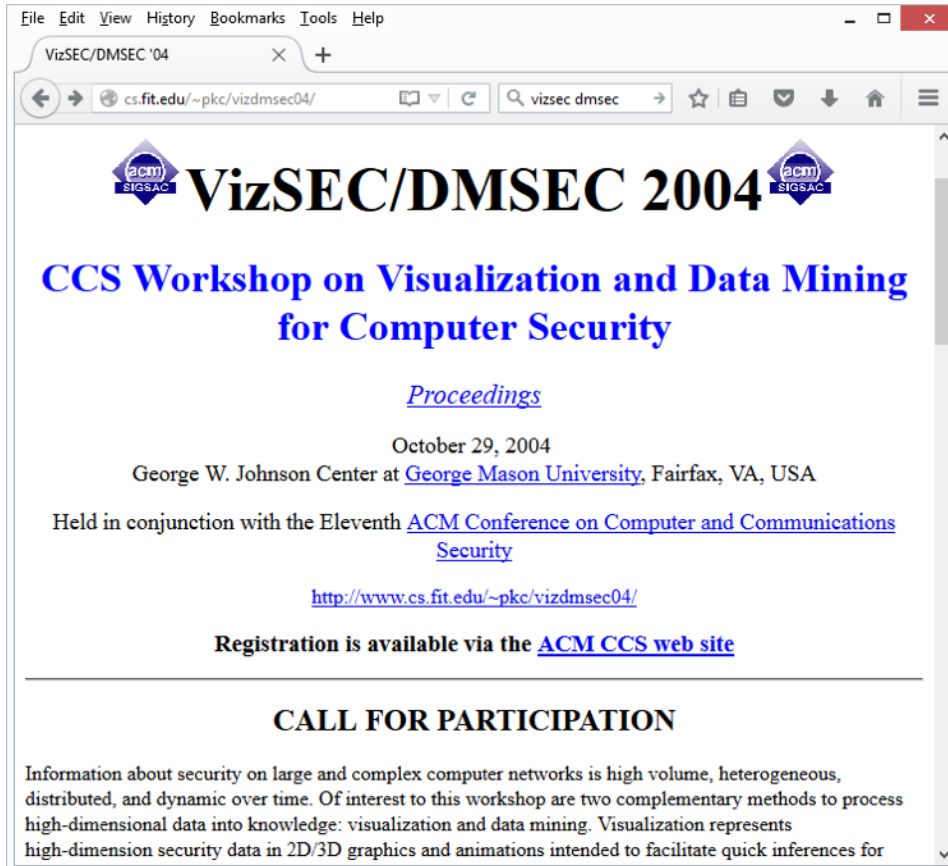
Tufte



Spence





VizSEC/DMSEC (2004)



File Edit View History Bookmarks Tools Help

VizSEC/DMSEC '04

cs.fit.edu/~pkc/vizdmsec04/ vizsec dmsec

 **VizSEC/DMSEC 2004** 

**CCS Workshop on Visualization and Data Mining
for Computer Security**

[Proceedings](#)

October 29, 2004
George W. Johnson Center at [George Mason University](#), Fairfax, VA, USA

Held in conjunction with the Eleventh [ACM Conference on Computer and Communications Security](#)

<http://www.cs.fit.edu/~pkc/vizdmsec04/>

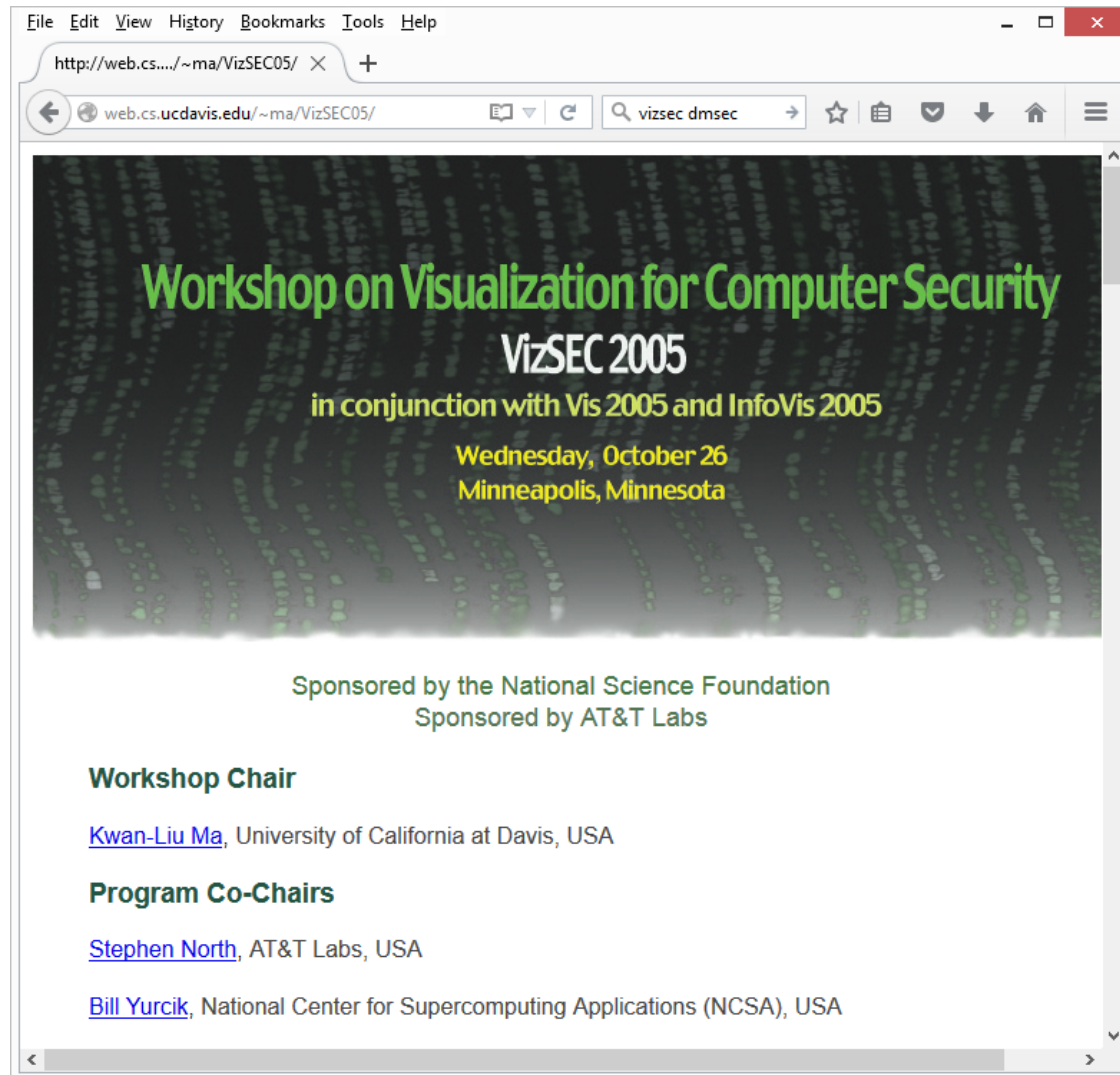
Registration is available via the [ACM CCS web site](#)

CALL FOR PARTICIPATION

Information about security on large and complex computer networks is high volume, heterogeneous, distributed, and dynamic over time. Of interest to this workshop are two complementary methods to process high-dimensional data into knowledge: visualization and data mining. Visualization represents high-dimension security data in 2D/3D graphics and animations intended to facilitate quick inferences for

- visualizing vulnerabilities
- visualizing IDS alarms (NIDS/HIDS)
- visualizing worm/virus propagation
- visualizing routing anomalies
- visualizing large volume computer network logs
- visual correlations of security events
- visualizing network traffic for security
- visualizing attacks in near-real-time
- security visualization at line speeds
- dynamic attack tree creation (graphic)
- forensic visualization
- feature selection
- feature construction
- incremental/online learning
- noise in the data
- skewed data distribution
- distributed mining
- correlating multiple models
- efficient processing of large amounts of data
- correlating alerts
- signature detection
- anomaly detection
- forensic analysis

VizSEC (2005)



The image shows a screenshot of a web browser window. The browser's address bar displays the URL `http://web.cs.ucsd.edu/~ma/VizSEC05/`. The page content features a large banner with a dark background and green, glowing text that reads "Workshop on Visualization for Computer Security" in a large font, followed by "VizSEC 2005" in a slightly smaller font. Below this, it states "in conjunction with Vis 2005 and InfoVis 2005" in a smaller font. The date and location, "Wednesday, October 26" and "Minneapolis, Minnesota", are listed in a yellow font. Further down, the page lists sponsors: "Sponsored by the National Science Foundation" and "Sponsored by AT&T Labs". The workshop chair is identified as "Kwan-Liu Ma, University of California at Davis, USA". The program co-chairs are "Stephen North, AT&T Labs, USA" and "Bill Yurcik, National Center for Supercomputing Applications (NCSA), USA". The browser interface includes a menu bar with "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The status bar at the bottom shows navigation arrows and a scrollbar.

File Edit View History Bookmarks Tools Help

http://web.cs.ucsd.edu/~ma/VizSEC05/ X +

web.cs.ucdavis.edu/~ma/VizSEC05/ vizsec dmsec

Workshop on Visualization for Computer Security

VizSEC 2005

in conjunction with Vis 2005 and InfoVis 2005

Wednesday, October 26
Minneapolis, Minnesota

Sponsored by the National Science Foundation
Sponsored by AT&T Labs

Workshop Chair

[Kwan-Liu Ma](#), University of California at Davis, USA

Program Co-Chairs

[Stephen North](#), AT&T Labs, USA

[Bill Yurcik](#), National Center for Supercomputing Applications (NCSA), USA

The "Dashboard"



Welcome, John Smith | [\[Log-out\]](#)

Global My Company Feeds CyberThreat Reports Settings

Crime Servers Map

Top Ranked Vulnerabilities In the Wild

#	Vulnerability	CVE	Patch
1	MSIE CFunctionPointer Memory Corruption	CVE-2009-0075	10-Feb-2009
2	PDF collab.getIcon() Remote Code Execution	CVE-2009-0927	09-Apr-2009
3	PDF Util.Printf() Stack Overflow	CVE-2008-2992	04-Nov-2008
4	PDF collab.collectEmailInfo() Memory Corruption	CVE-2007-5659	06-May-2008
5	DirectX DirectShow ActiveX Heap Overflow	CVE-2008-0015	11-Aug-2009
6	MS Access Snapshot Viewer ActiveX	CVE-2008-2463	12-Aug-2008
7	MDAC RDS.Dataspace ActiveX	CVE-2006-0003	11-Apr-2006
8	MS OWC Spreadsheet ActiveX	CVE-2009-1136	11-Aug-2009
9	PDF Doc.media.newPlayer Use-After-Free	CVE-2009-4324	12-Jan-2010
10	Java JRE getSoundBank Stack Based Overflow	CVE-2009-3867	04-Nov-2009

Online Threats Statistics

Chart: Exploit Kits Distribution

CyberThreat Level

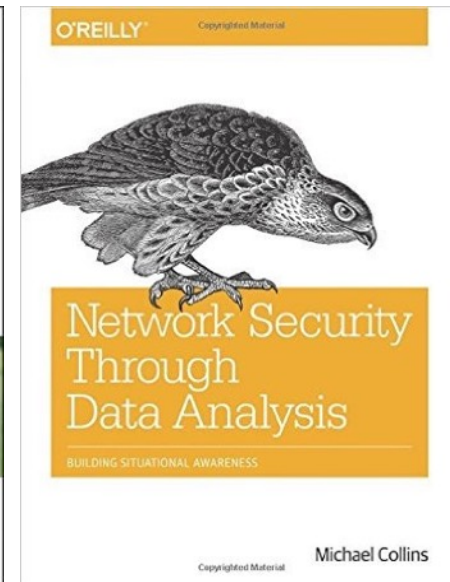
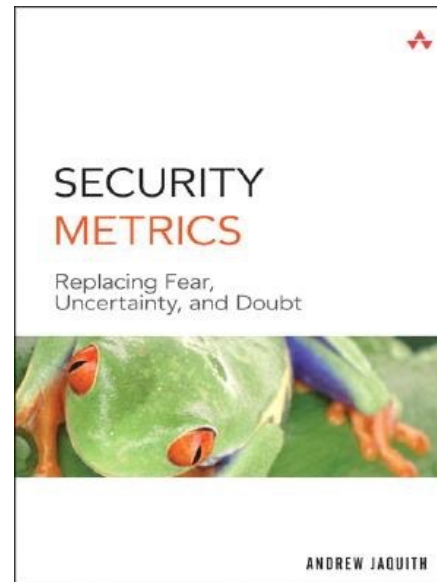
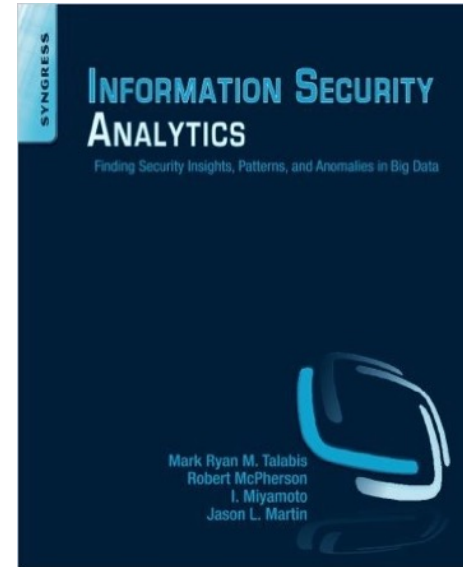
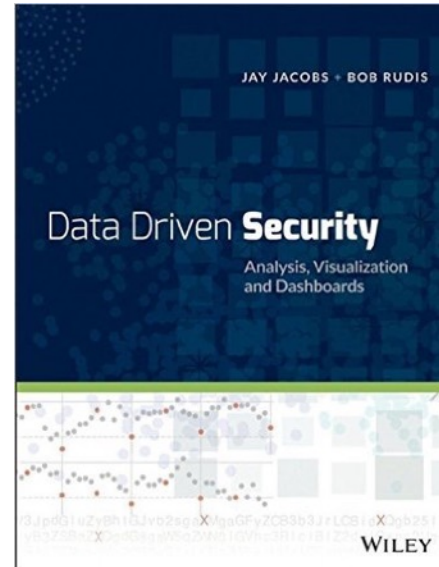
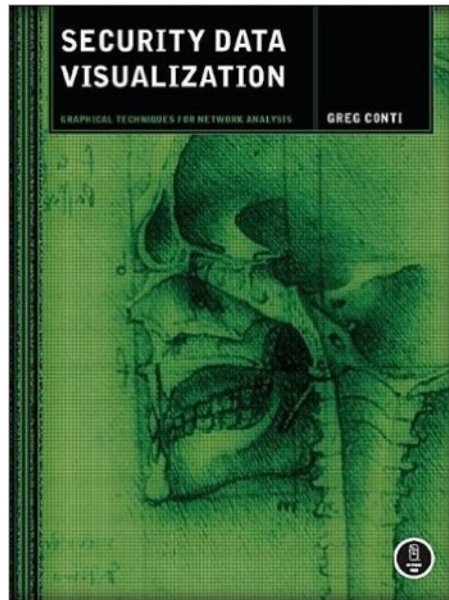
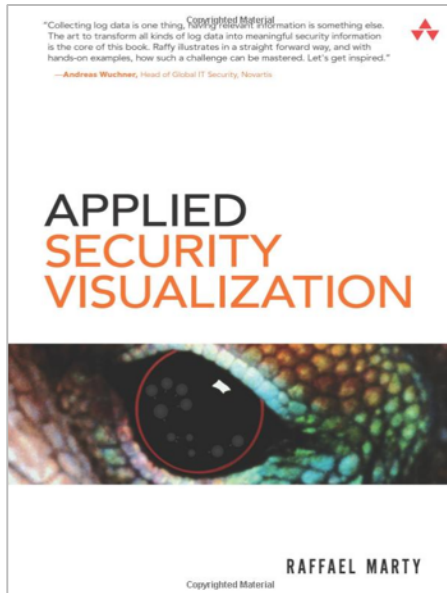
65%

CyberThreat Level Trend

Period: 24h 1w 1m 6m

Time	Level (%)
12:00	14%
16:00	10%
20:00	65%
0:00	68%
4:00	45%
8:00	28%

Security Visualization and Enabler Books Emerge...



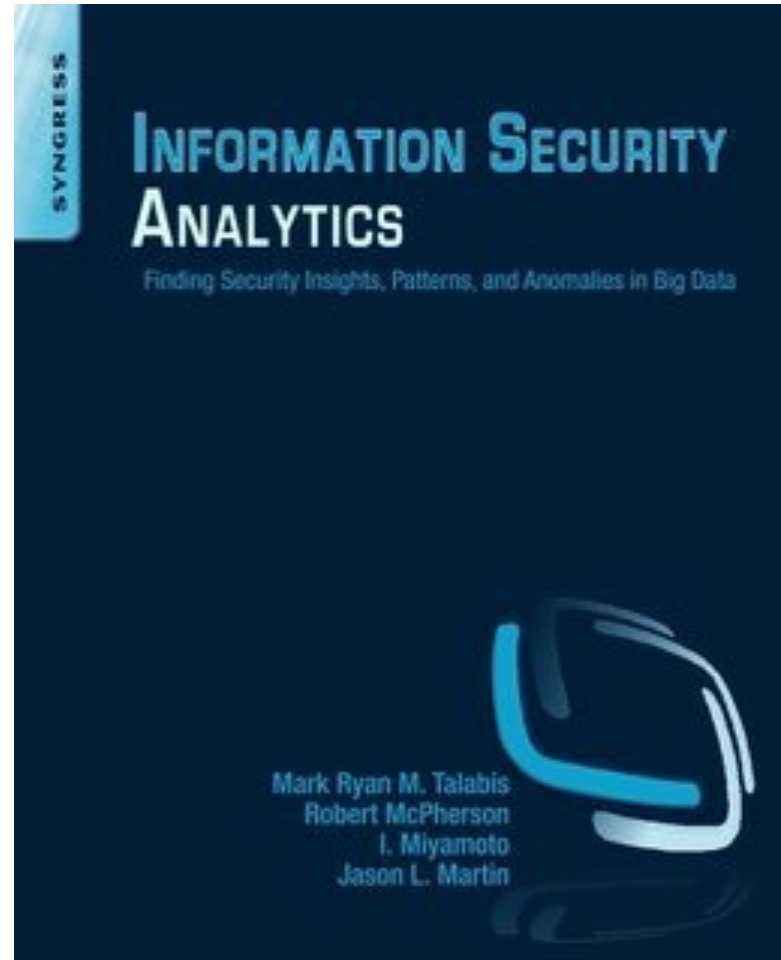
the perfect time
is when you turn
the present into
what you want it
to be.

Anna Levine

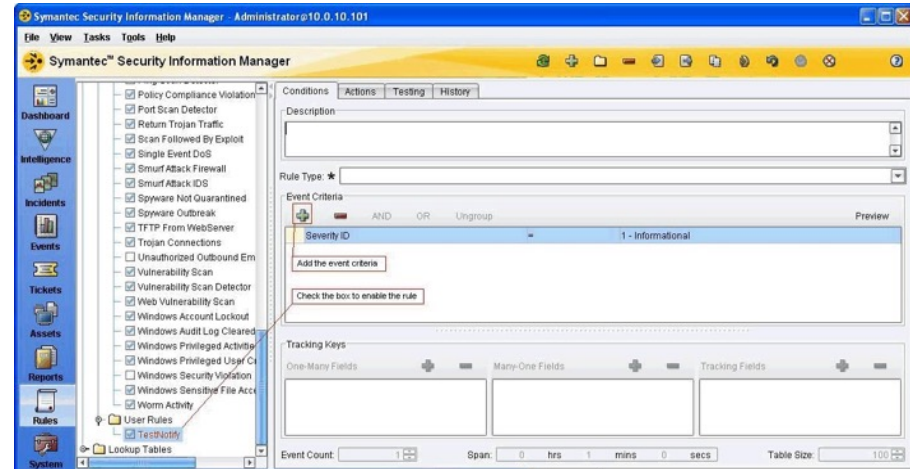
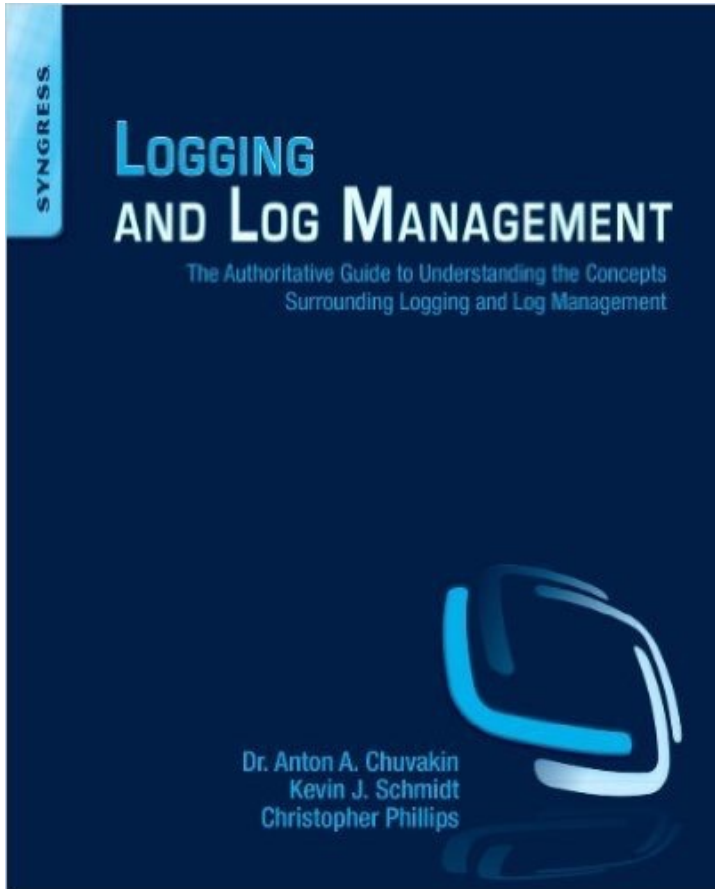
meetville.com

Present

Analytics



Diverse Data Flows



- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
- Forensic analysis

The "Dashboard"



Welcome, John Smith | [\[Log-out\]](#)

Global My Company Feeds CyberThreat Reports Settings

Crime Servers Map

Top Ranked Vulnerabilities In the Wild

#	Vulnerability	CVE	Patch
1	MSIE CFunctionPointer Memory Corruption	CVE-2009-0075	10-Feb-2009
2	PDF collab.getIcon() Remote Code Execution	CVE-2009-0927	09-Apr-2009
3	PDF Util.Printf() Stack Overflow	CVE-2008-2992	04-Nov-2008
4	PDF collab.collectEmailInfo() Memory Corruption	CVE-2007-5659	06-May-2008
5	DirectX DirectShow ActiveX Heap Overflow	CVE-2008-0015	11-Aug-2009
6	MS Access Snapshot Viewer ActiveX	CVE-2008-2463	12-Aug-2008
7	MDAC RDS.Dataspace ActiveX	CVE-2006-0003	11-Apr-2006
8	MS OWC Spreadsheet ActiveX	CVE-2009-1136	11-Aug-2009
9	PDF Doc.media.newPlayer Use-After-Free	CVE-2009-4324	12-Jan-2010
10	Java JRE getSoundBank Stack Based Overflow	CVE-2009-3867	04-Nov-2009

Online Threats Statistics

Chart: Exploit Kits Distribution

CyberThreat Level

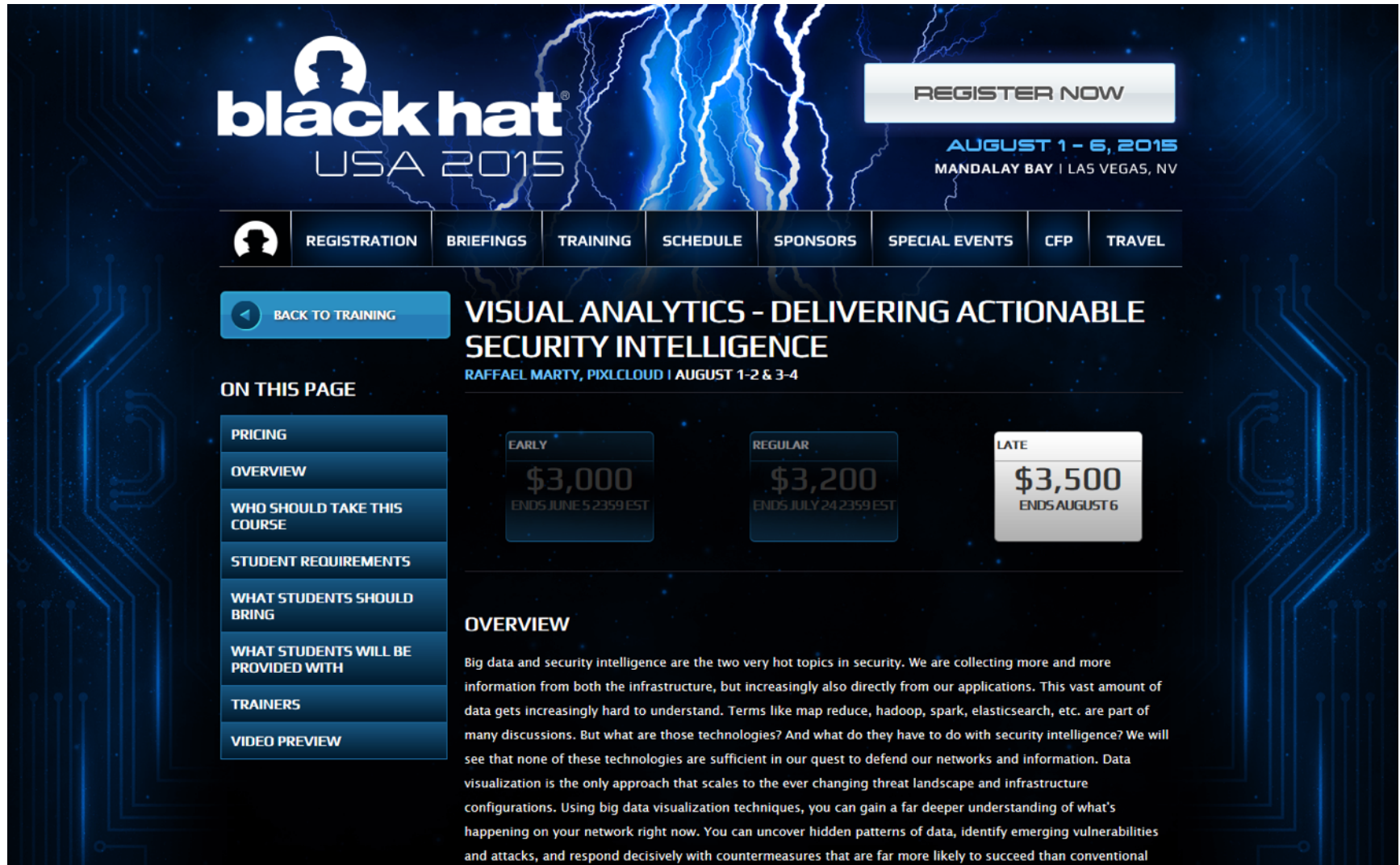
65%

CyberThreat Level Trend

Period: 24h 1w 1m 6m

Time	Level (%)
12:00	14%
16:00	10%
20:00	65%
0:00	68%
4:00	45%
8:00	28%

Training



The image shows a webpage for Black Hat USA 2015 training. The header features the Black Hat logo and event details: "REGISTER NOW", "AUGUST 1 - 6, 2015", and "MANDALAY BAY | LAS VEGAS, NV". A navigation bar includes links for "REGISTRATION", "BRIEFINGS", "TRAINING", "SCHEDULE", "SPONSORS", "SPECIAL EVENTS", "CFP", and "TRAVEL". The main content area is titled "VISUAL ANALYTICS - DELIVERING ACTIONABLE SECURITY INTELLIGENCE" by Raffael Marty from Pixlcloud, scheduled for August 1-2 & 3-4. A sidebar on the left lists navigation options: "PRICING", "OVERVIEW", "WHO SHOULD TAKE THIS COURSE", "STUDENT REQUIREMENTS", "WHAT STUDENTS SHOULD BRING", "WHAT STUDENTS WILL BE PROVIDED WITH", "TRAINERS", and "VIDEO PREVIEW". The pricing section shows three options: Early at \$3,000 (ends June 5), Regular at \$3,200 (ends July 24), and Late at \$3,500 (ends August 6). The overview text discusses the challenges of big data and security intelligence, emphasizing the need for data visualization to understand and defend against threats.

black hat[®]

USA 2015

REGISTER NOW

AUGUST 1 - 6, 2015
MANDALAY BAY | LAS VEGAS, NV

REGISTRATION BRIEFINGS TRAINING SCHEDULE SPONSORS SPECIAL EVENTS CFP TRAVEL

[← BACK TO TRAINING](#)

VISUAL ANALYTICS - DELIVERING ACTIONABLE SECURITY INTELLIGENCE

RAFFAEL MARTY, PIXL CLOUD | AUGUST 1-2 & 3-4

ON THIS PAGE

- PRICING
- OVERVIEW
- WHO SHOULD TAKE THIS COURSE
- STUDENT REQUIREMENTS
- WHAT STUDENTS SHOULD BRING
- WHAT STUDENTS WILL BE PROVIDED WITH
- TRAINERS
- VIDEO PREVIEW

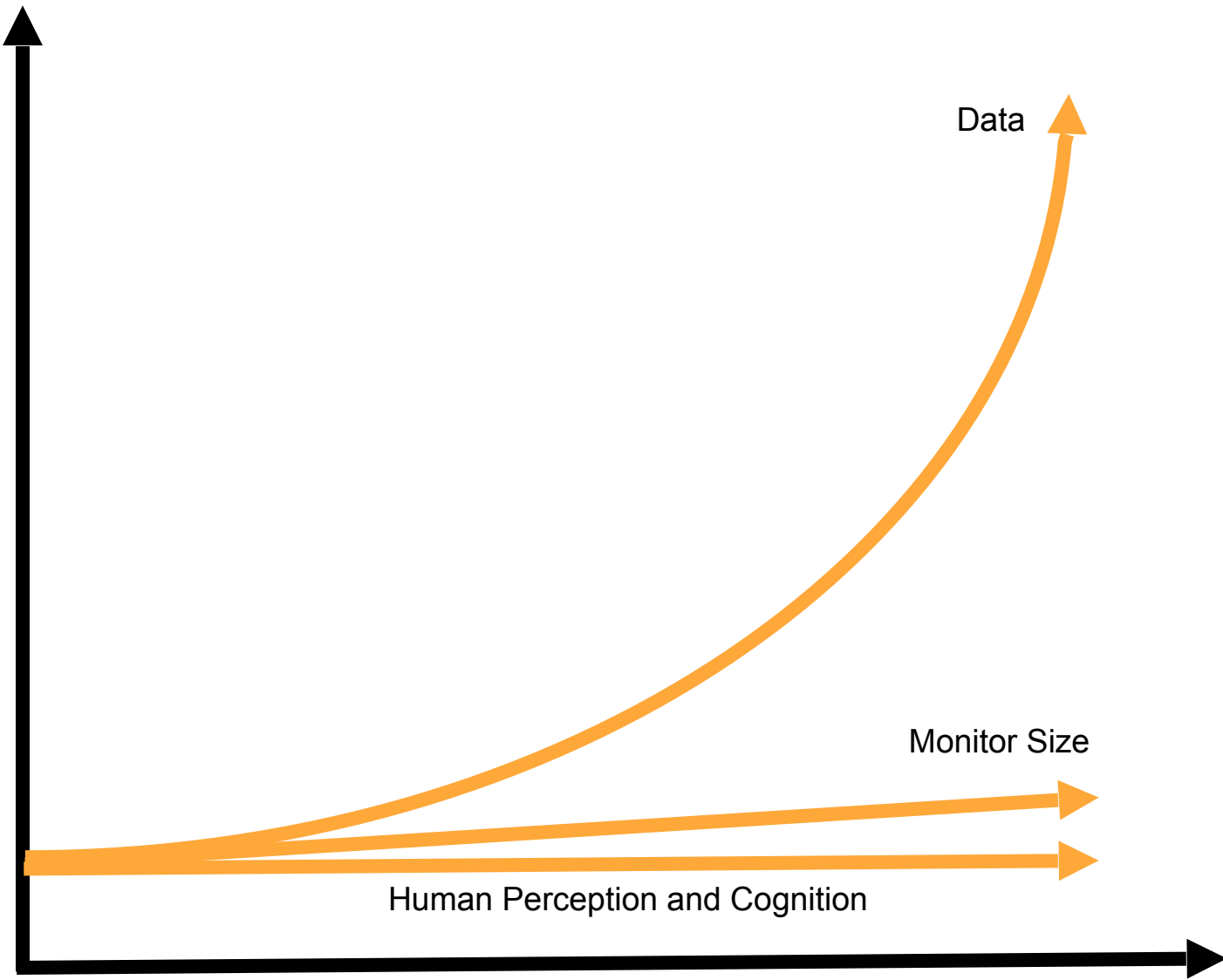
EARLY	REGULAR	LATE
\$3,000	\$3,200	\$3,500
ENDS JUNE 5 2359 EST	ENDS JULY 24 2359 EST	ENDS AUGUST 6

OVERVIEW

Big data and security intelligence are the two very hot topics in security. We are collecting more and more information from both the infrastructure, but increasingly also directly from our applications. This vast amount of data gets increasingly hard to understand. Terms like map reduce, hadoop, spark, elasticsearch, etc. are part of many discussions. But what are those technologies? And what do they have to do with security intelligence? We will see that none of these technologies are sufficient in our quest to defend our networks and information. Data visualization is the only approach that scales to the ever changing threat landscape and infrastructure configurations. Using big data visualization techniques, you can gain a far deeper understanding of what's happening on your network right now. You can uncover hidden patterns of data, identify emerging vulnerabilities and attacks, and respond decisively with countermeasures that are far more likely to succeed than conventional



Future



Time

Data

Monitor Size

Human Perception and Cognition

The "Dashboard"



Welcome, John Smith | [\[Log-out\]](#)

Global My Company Feeds CyberThreat Reports Settings

Crime Servers Map

Top Ranked Vulnerabilities In the Wild

#	Vulnerability	CVE	Patch
1	MSIE CFunctionPointer Memory Corruption	CVE-2009-0075	10-Feb-2009
2	PDF collab.getIcon() Remote Code Execution	CVE-2009-0927	09-Apr-2009
3	PDF Util.Printf() Stack Overflow	CVE-2008-2992	04-Nov-2008
4	PDF collab.collectEmailInfo() Memory Corruption	CVE-2007-5659	06-May-2008
5	DirectX DirectShow ActiveX Heap Overflow	CVE-2008-0015	11-Aug-2009
6	MS Access Snapshot Viewer ActiveX	CVE-2008-2463	12-Aug-2008
7	MDAC RDS.Dataspace ActiveX	CVE-2006-0003	11-Apr-2006
8	MS OWC Spreadsheet ActiveX	CVE-2009-1136	11-Aug-2009
9	PDF Doc.media.newPlayer Use-After-Free	CVE-2009-4324	12-Jan-2010
10	Java JRE getSoundBank Stack Based Overflow	CVE-2009-3867	04-Nov-2009

Online Threats Statistics

Chart: Exploit Kits Distribution

Exploit Kit	Percentage
Phoenix	~25%
NeoSploit	~25%
YES	~15%
NULLED	~10%
Fragus	~10%
Liberty	~10%
Eleonore	~5%

CyberThreat Level

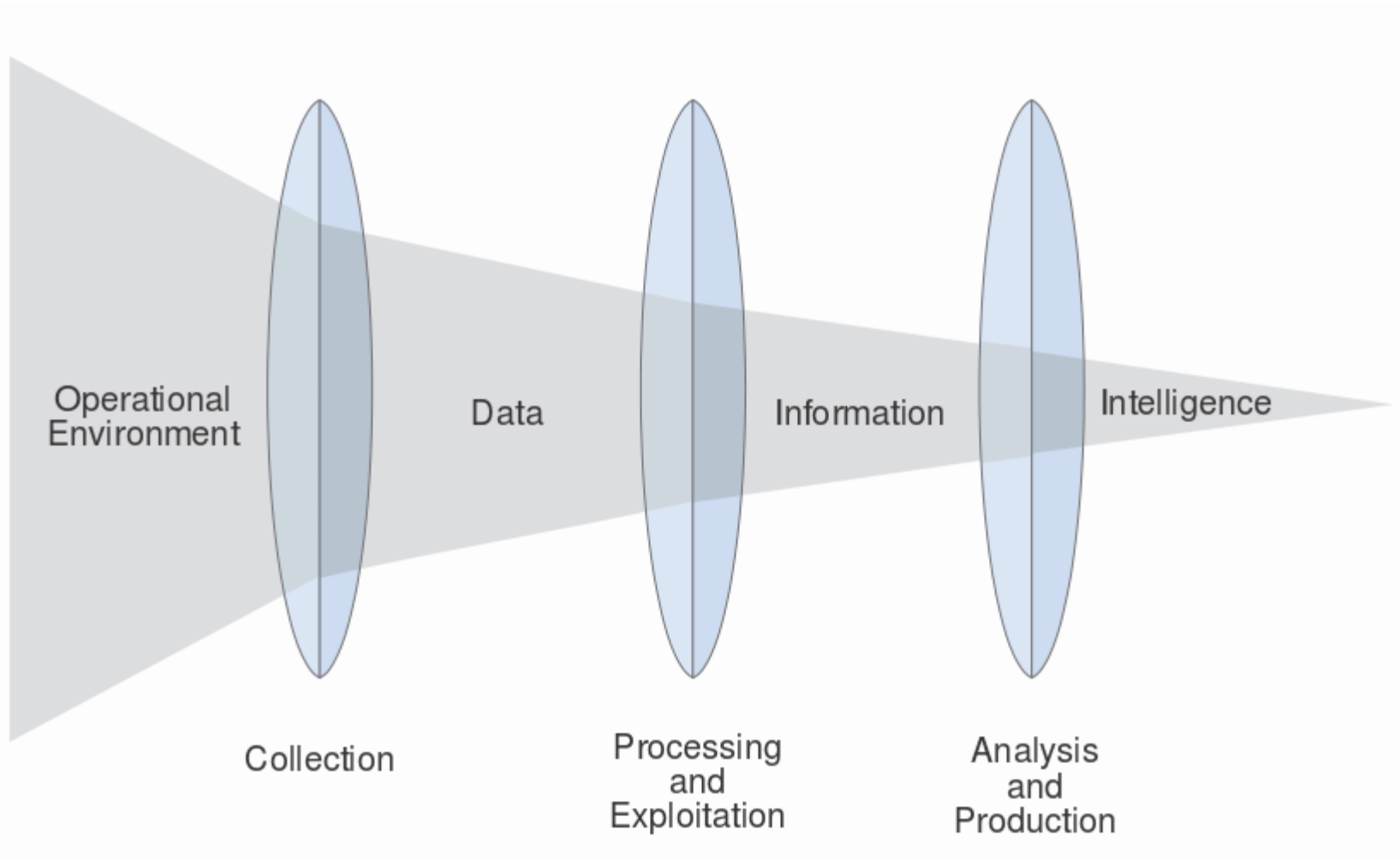
65%

CyberThreat Level Trend

Period: 24h 1w 1m 6m

Time	Level (%)
12:00	14%
16:00	10%
20:00	65%
0:00	68%
4:00	45%
8:00	28%

Relationship of Data, Information, and Intelligence



Expressing Confidence in Analytic Judgments

Low

- Uncorroborated information from good or marginal sources
- Many assumptions
- Mostly weak logical inferences, minimal methods application
- Glaring intelligence gaps exist

Terms/Expressions

- Possible
- Could, may, might
- Cannot judge, unclear

Moderate

- Partially corroborated information from good sources
- Several assumptions
- Mix of strong and weak inferences and methods
- Minimum intelligence gaps exist

Terms/Expressions

- Likely, unlikely
- Probable, improbable
- Anticipate, appear

High

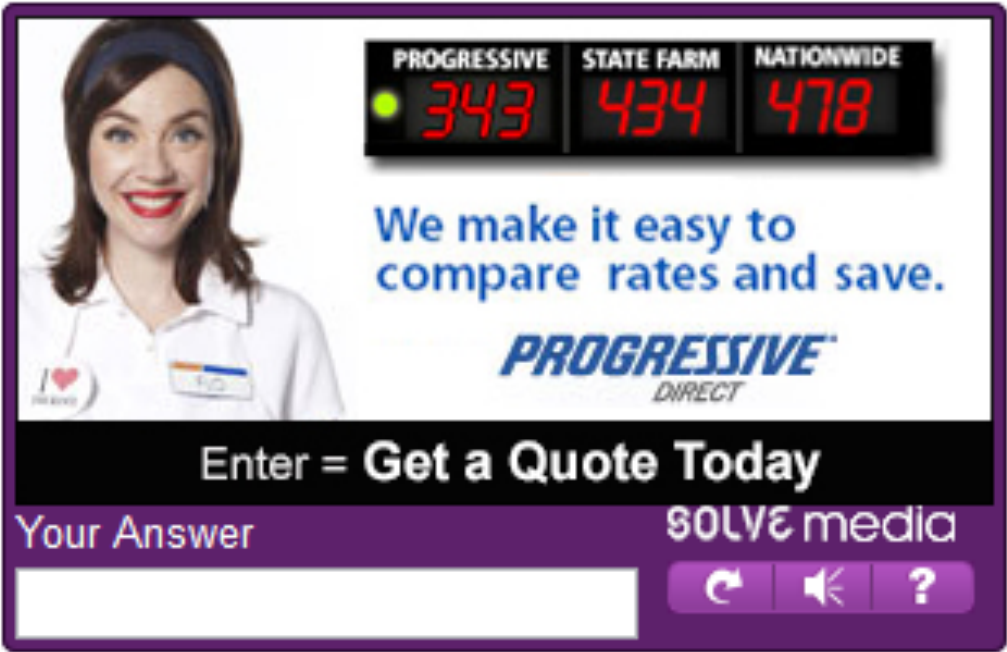
- Well-corroborated information from proven sources
- Minimal assumptions
- Strong logical inferences and methods
- No or minor intelligence gaps exist

Terms/Expressions

- Will, will not
- Almost certainly, remote
- Highly likely, highly unlikely
- Expect, assert, affirm

Don't Use Your Powers for #DarkPatterns

[Click here if you do not see a captcha](#)



The image shows a screenshot of a Progressive Direct advertisement. On the left is a woman in a white polo shirt with a name tag. On the right, a black digital display shows rates for Progressive (343), State Farm (434), and Nationwide (478). Below the display is the text "We make it easy to compare rates and save." and the Progressive Direct logo. A black banner at the bottom of the ad says "Enter = Get a Quote Today".

PROGRESSIVE STATE FARM NATIONWIDE
343 434 478

We make it easy to compare rates and save.

PROGRESSIVE
DIRECT

Enter = **Get a Quote Today**

Your Answer solve media

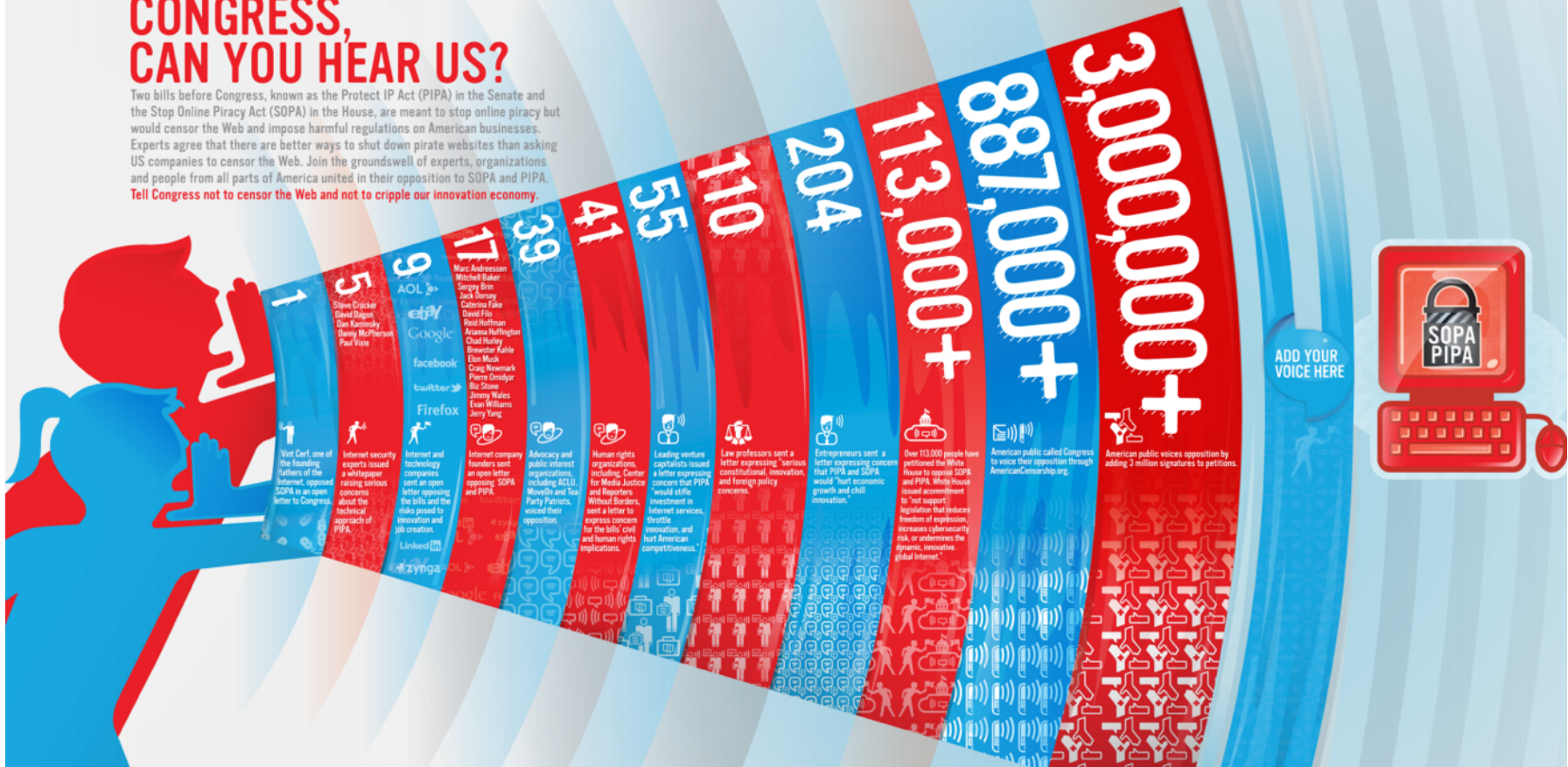
↻ 🔊 ?

Not a bot!!

Advocacy

CONGRESS, CAN YOU HEAR US?

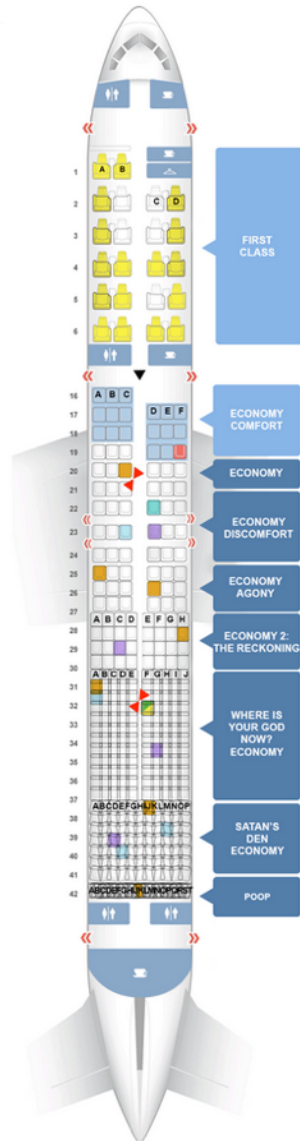
Two bills before Congress, known as the Protect IP Act (PIPA) in the Senate and the Stop Online Piracy Act (SOPA) in the House, are meant to stop online piracy but would censor the Web and impose harmful regulations on American businesses. Experts agree that there are better ways to shut down pirate websites than asking US companies to censor the Web. Join the groundswell of experts, organizations and people from all parts of America united in their opposition to SOPA and PIPA. Tell Congress not to censor the Web and not to cripple our innovation economy.












ADD YOUR VOICE HERE



Social Good



-  Passenger judging you
-  Stewardess who won't let you use the front bathroom
-  Screaming baby
-  Child kicking or banging on your headrest while trying to use the in-flight entertainment
-  Passenger using knee defender
-  Passenger leaning so far back she is in your lap
-  Barefoot foot fungus passenger with feet in your space
-  Passenger stealing your armrest while eating tuna fish and a boiled egg
-  Arguments on the verge of becoming all out brawls

Public Education

Standard Form 86
 Revised December 2010
 U.S. Office of Personnel Management
 5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
 OMB No. 3206 0005

PERSONS COMPLETING THIS FORM SHOULD BEGIN WITH THE QUESTIONS BELOW AFTER CAREFULLY READING THE PRECEDING INSTRUCTIONS.

I have read the instructions and I understand that if I withhold, misrepresent, or falsify information on this form, I am subject to the penalties for inaccurate or false statement (per U. S. Criminal Code, Title 18, section 1001), denial or revocation of a security clearance, and/or removal and debarment from Federal Service. YES NO

Section 1 - Full Name

Provide your full name. If you have only initials in your name, provide them and indicate "Initial only". If you do not have a middle name, indicate "No Middle Name". If you are a "Jr.," "Sr.," etc. enter this under Suffix.

Last name	First name	Middle name	Suffix
-----------	------------	-------------	--------

Section 2 - Date of Birth

Provide your date of birth.
(Month/Day/Year)

Section 3 - Place of Birth

Provide your place of birth.

City	County	State	Country <i>(Required)</i>
------	--------	-------	---------------------------

Section 4 - Social Security Number

Provide your U.S. Social Security Number.

Not applicable

Section 5 - Other Names Used

Have you used any other names? YES NO *(If NO, proceed to Section 6)*

Complete the following if you have responded 'Yes' to having used other names.

Provide your other name(s) used and the period of time you used it/them [for example: your maiden name(s), name(s) by a former marriage, former name(s), alias(es), or nickname(es)]. If you have only initials in your name(s), provide them and indicate "Initial only." If you do not have a middle name (s), indicate "No Middle Name" (NMN). If you are a "Jr.," "Sr.," etc. enter this under Suffix.

#1 Last name	First name	Middle name	Suffix
From <i>(Month/Year)</i>	To <i>(Month/Year)</i>	<input type="checkbox"/> Present	Maiden name?
<input type="checkbox"/> Est.	<input type="checkbox"/> Est.	<input type="checkbox"/> YES <input type="checkbox"/> NO	Provide the reason(s) why the name changed

What is the Secret Ingredient?



“The First Law of Intrusion Detection: That Which You Can’t See, You Can’t Detect.” - Anup Ghosh

Chasing the Invisible Man...




Fight for Visibility

File Edit View History Bookmarks Tools Help


top Washington Post: Breakin... X +

https://www.washingtonpost.com Search

Sections Politics Opinions Sports Local National World Sign In Subscribe




UNMUTE
CLOSE



The Washington Post

Oct 23, 2015 Edition: U.S. & World | Regional



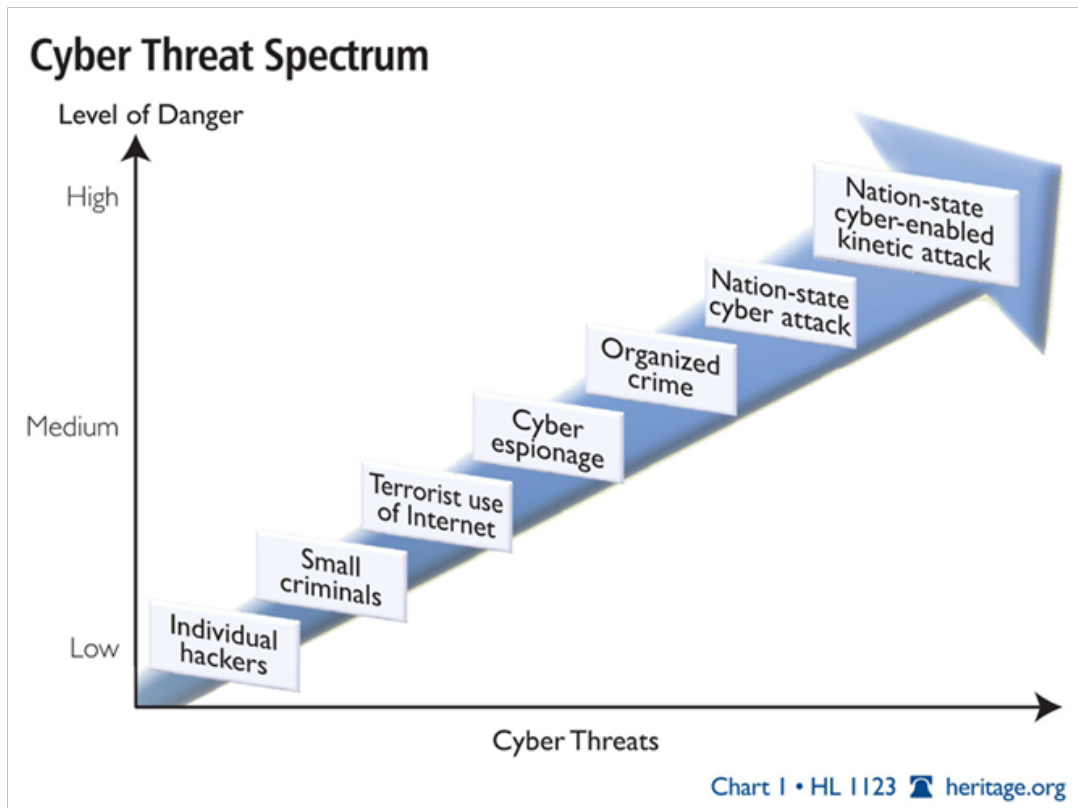
https://adclick.g.doubleclick.net/aclk?sa=L&ai=Bou6fwRcqVqXsH4SMML_ZhugGwozykAgAA...b-3671346551221509&adurl=https://ad.doubleclick.net/ddm/clk/297109790;124172743;k

Fight for Visibility

The image shows a screenshot of a web browser displaying a Washington Post article. The browser's address bar shows the URL <https://www.washingtonpost.com>. The page features a navigation bar with sections like Politics, Opinions, Sports, Local, National, and World, along with Sign In and Subscribe buttons. A video player is embedded in the article, showing a chef in a kitchen. A red-bordered box is overlaid on the video player, containing the URL <https://adclick.g.doubleclick.net/aclick?sa=L&ai=Bou6fwR>. Below the video player, there are advertisements for FAGE yogurt and The Washington Post logo. The page footer includes the date Oct 23, 2015, and the edition U.S. & World | Regional. The browser's status bar at the bottom shows a long URL: https://adclick.g.doubleclick.net/aclick?sa=L&ai=Bou6fwRcqvqXsH4SMML_ZhugGwozykAgAA...b-3671346551221509&adurl=https://ad.doubleclick.net/ddm/clk/297109790;124172743;v

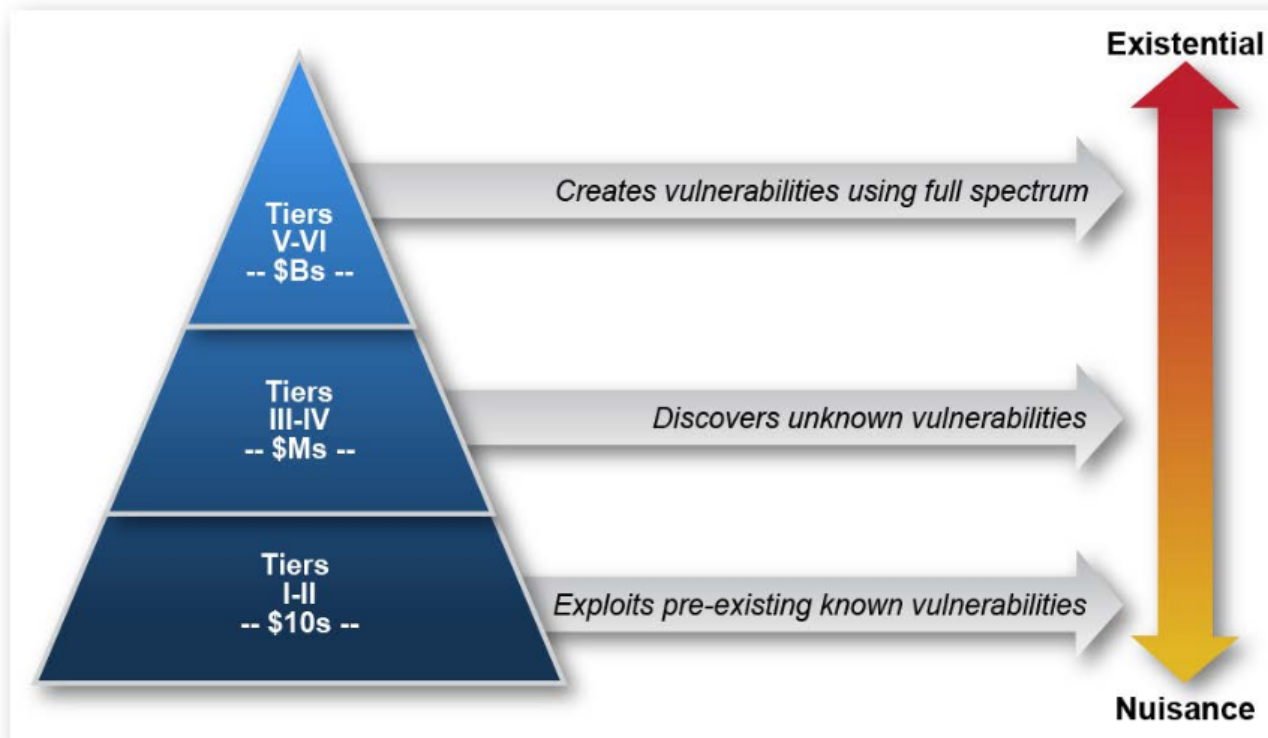
Role of an Adversary





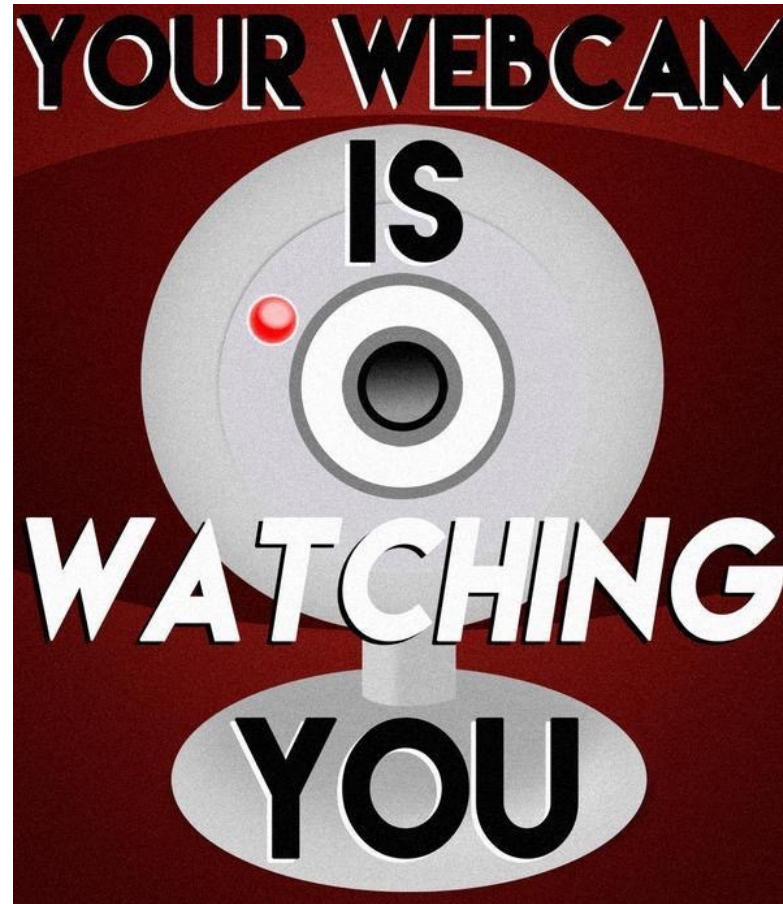
We used to be fighting individuals . . .
now we are defending ourselves against nation-states

Three Tiers

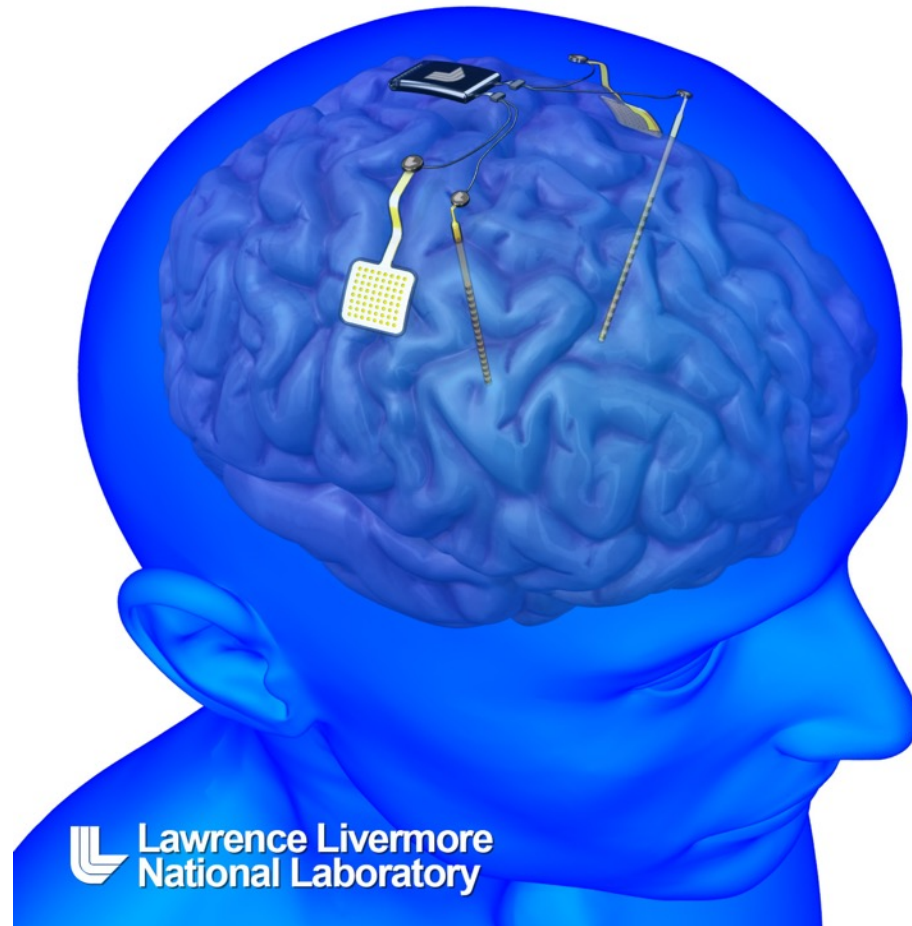


See Defense Science Board, "Resilient Military Systems and the Advanced Cyber Threat," JAN 2013

Privacy



Neural Interfaces



On Demand Web-based Tools

The screenshot displays the binvis.io web interface. On the left, a memory dump is visualized as a heatmap where colors represent different byte classes: black for 0x00, green for low values, blue for ASCII, red for high values, and white for 0xff. On the right, the raw memory data is shown in hex and ASCII format. The hex dump starts at address 00191b0 and ends at 00192e0. The ASCII dump shows fragments of XML and other text, including "http://n s.adobe.com/xap/ 1.0/.<?x packet b egin="..", ". id="W 5M0MpCeh iHzreSzN Tczkc9d", "> <x:xm pmeta xm lns:x="a dobe:ns: meta/" x :xmpTk=" Adobe XM P Core 5 .6-c014 79.15679 7, 2014/ 08/20-09 :53:02 "> <rdf:RD F xmlns:", and "8BIM...".

binvis.io

binvis.io

“Big Data” and “The Cloud”



IPv6



Moving Target Defense



Deception



Members of the 23rd lift a "tank." (Rick Beyer/Hatcher Graduate Library)

Scales of Time



Humans in the Loop



10. The computer decides everything, acts autonomously, ignoring the human
9. informs the human only if it, the computer, decides to
8. informs the human only if asked
7. executes automatically, then necessarily informs the human
6. allows the human a restricted time to veto before automatic execution
5. executes that suggestion if the human approves
4. suggests one alternative
3. narrows the selection down to a few
2. the computer offers a complete set of decision/action alternatives
1. the computer offers no assistance: human must take all decisions and actions

“Levels of Automation of Decision and Action Selection” from Raja Parasuraman, Thomas Sheridan, and Christopher Wickens, “A Model for Types and Levels of Human Interaction with Automation,” IEEE Transactions on Systems, Man and Cybernetics, Vol. 30, No. 3, May 2000.

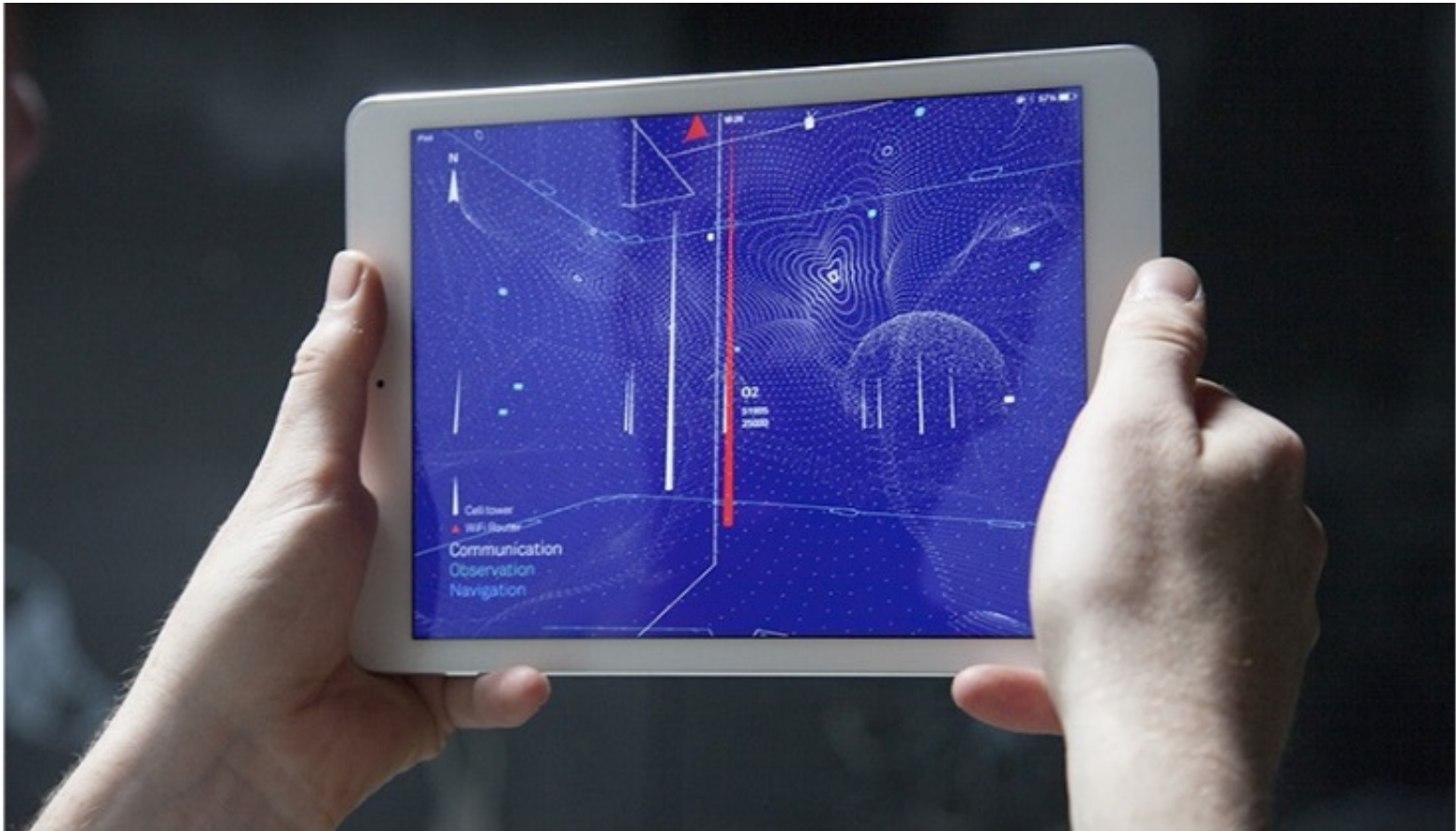
Sensors



Virtual Reality

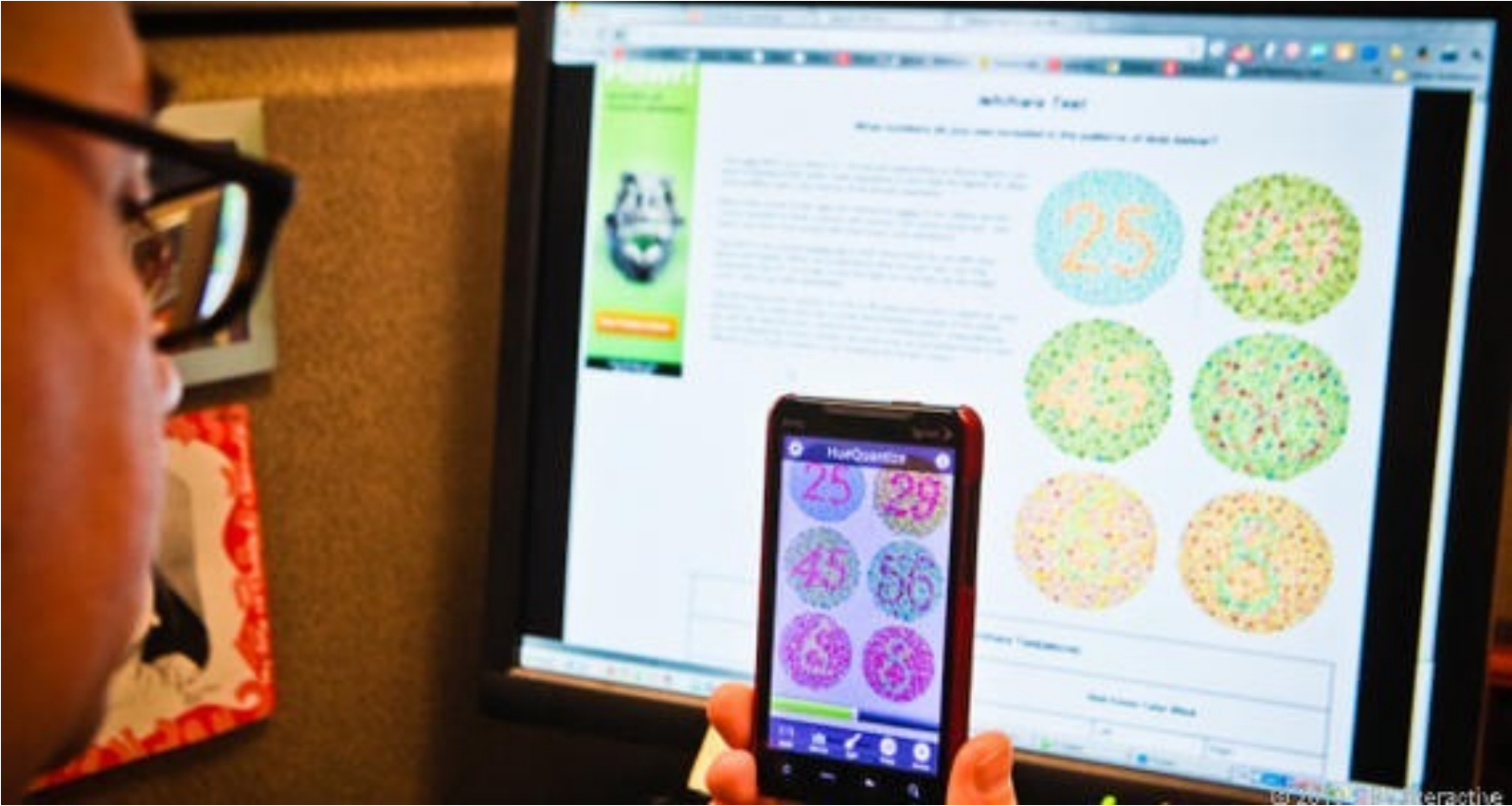


Augmented Reality



Architecture of Radio

Mobile

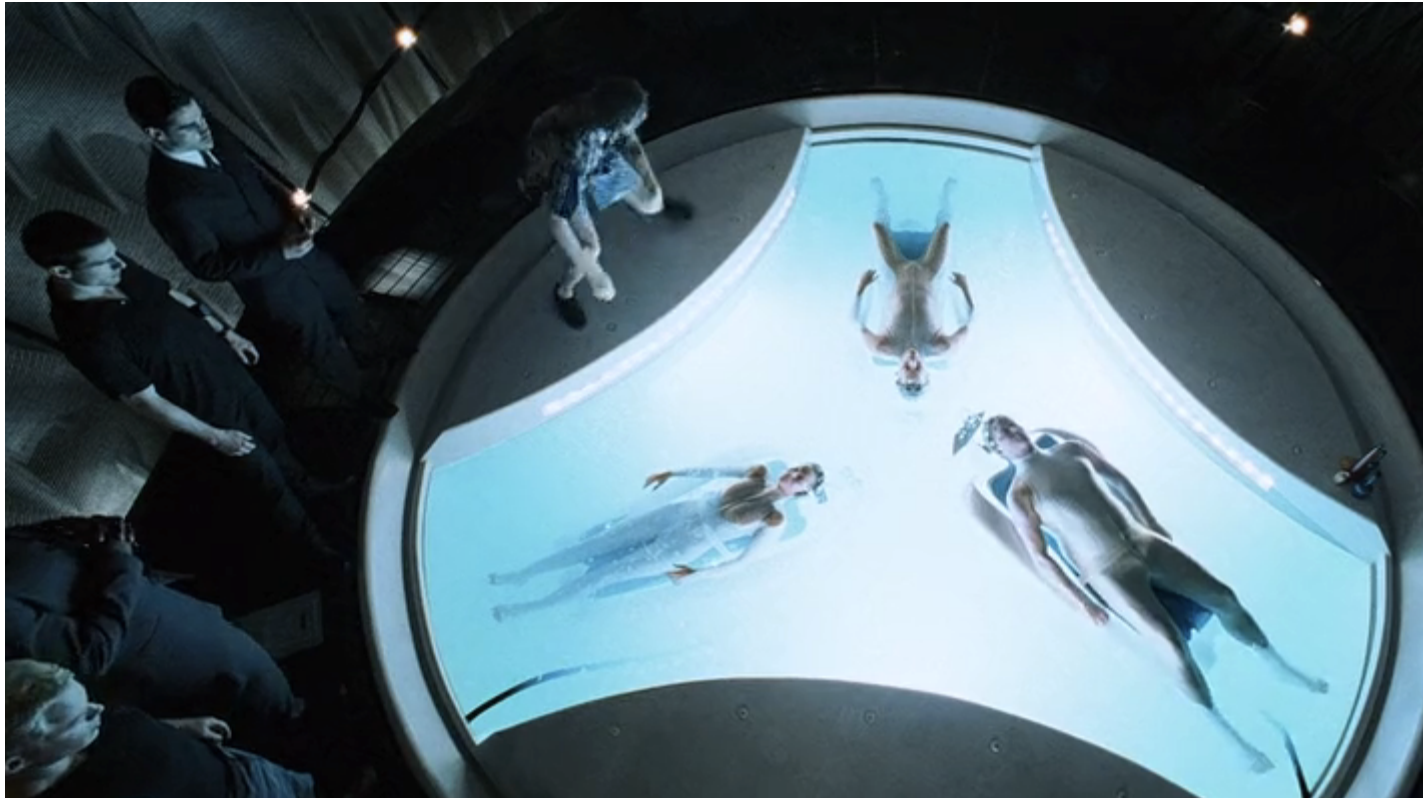


DanKam

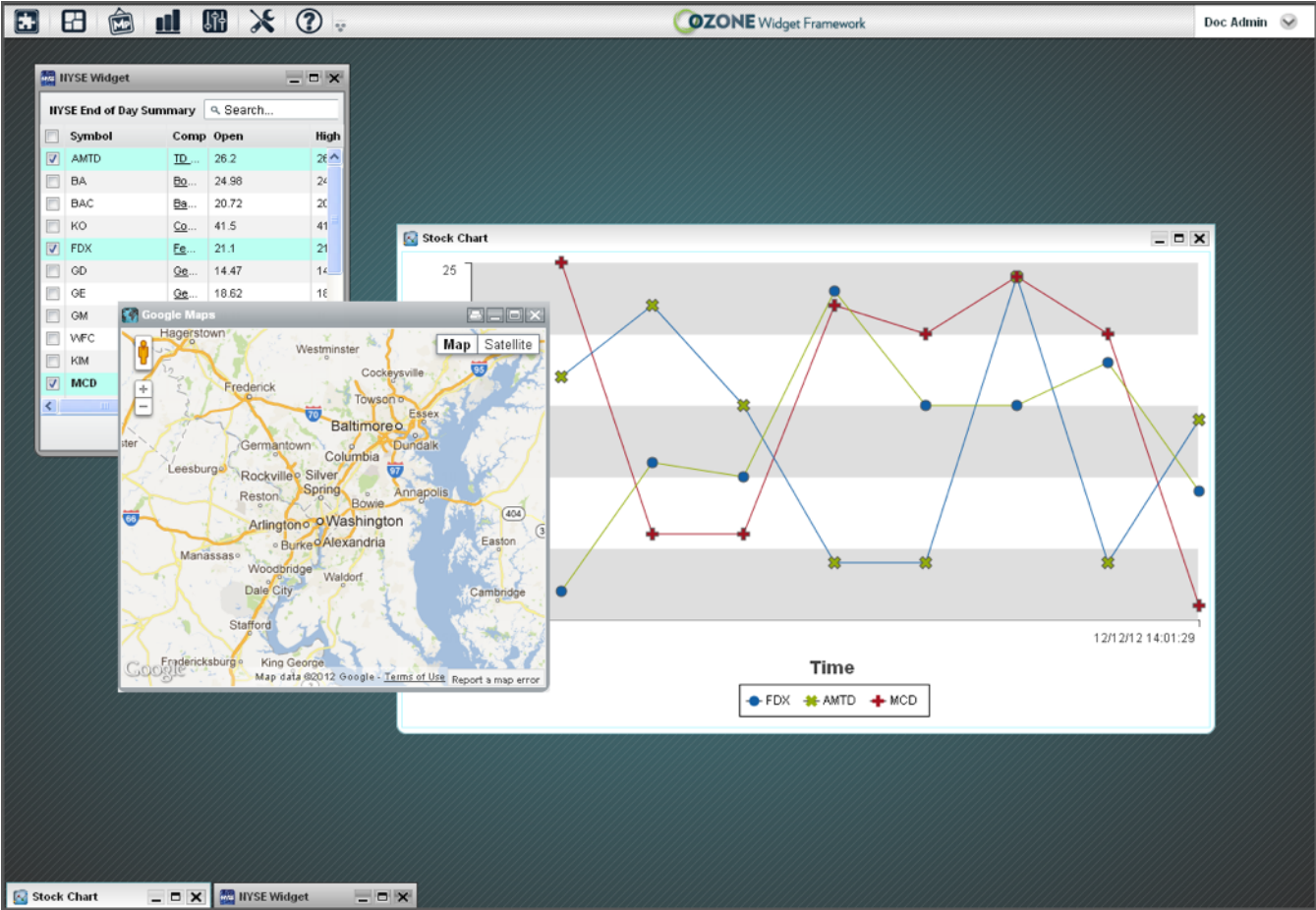
Internet of Things



Predictive



User Defined Operating Picture



Operator Requirements



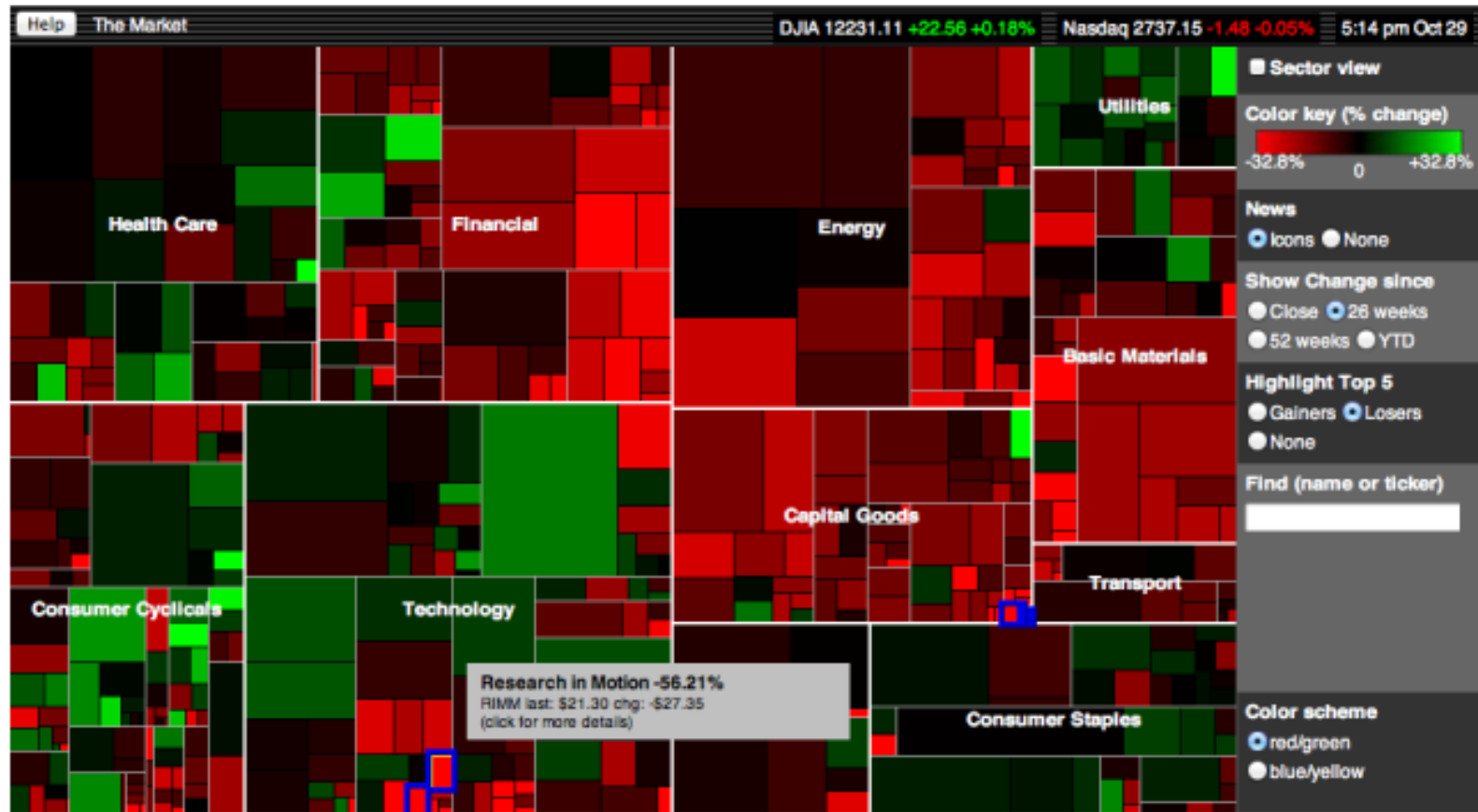
Partnering



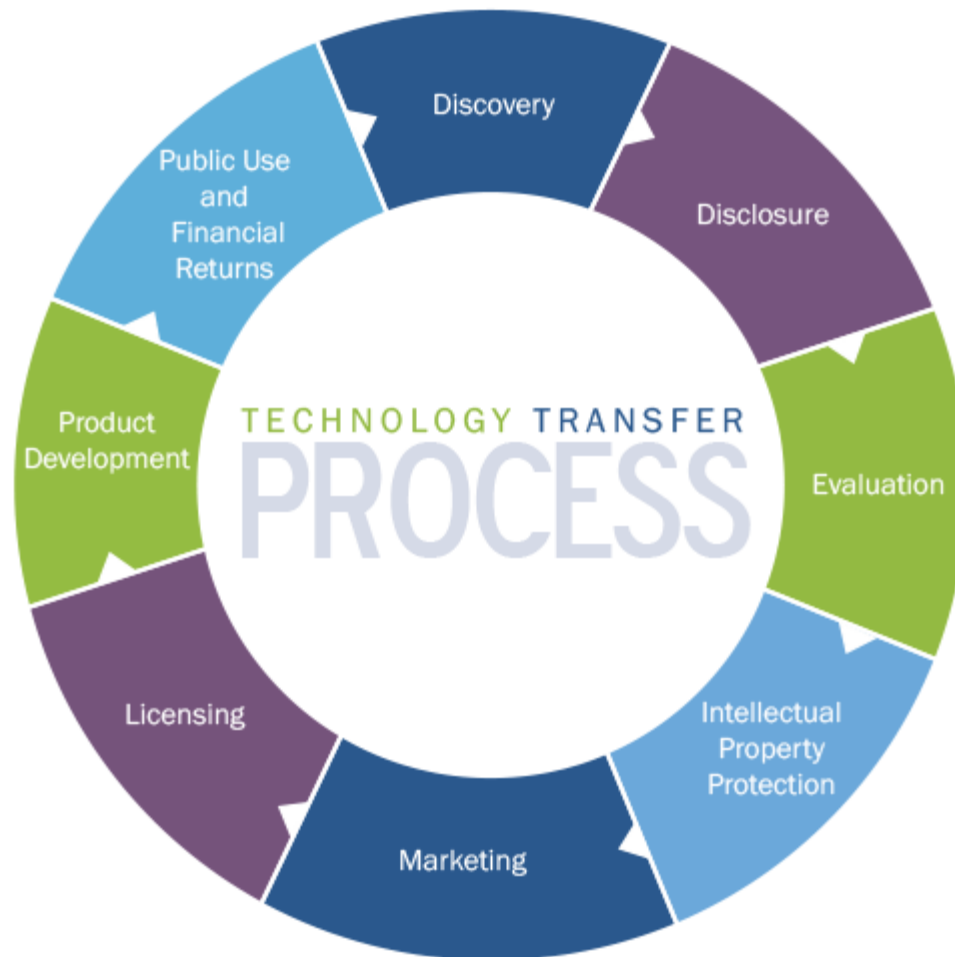
Adoption and Commercial Utilization

Map of the Market

SmartMoneySelect Upgrade [here](#) to access the Market Map 1000 and search 1,000 companies with enhanced capabilities.



Tech Transfer



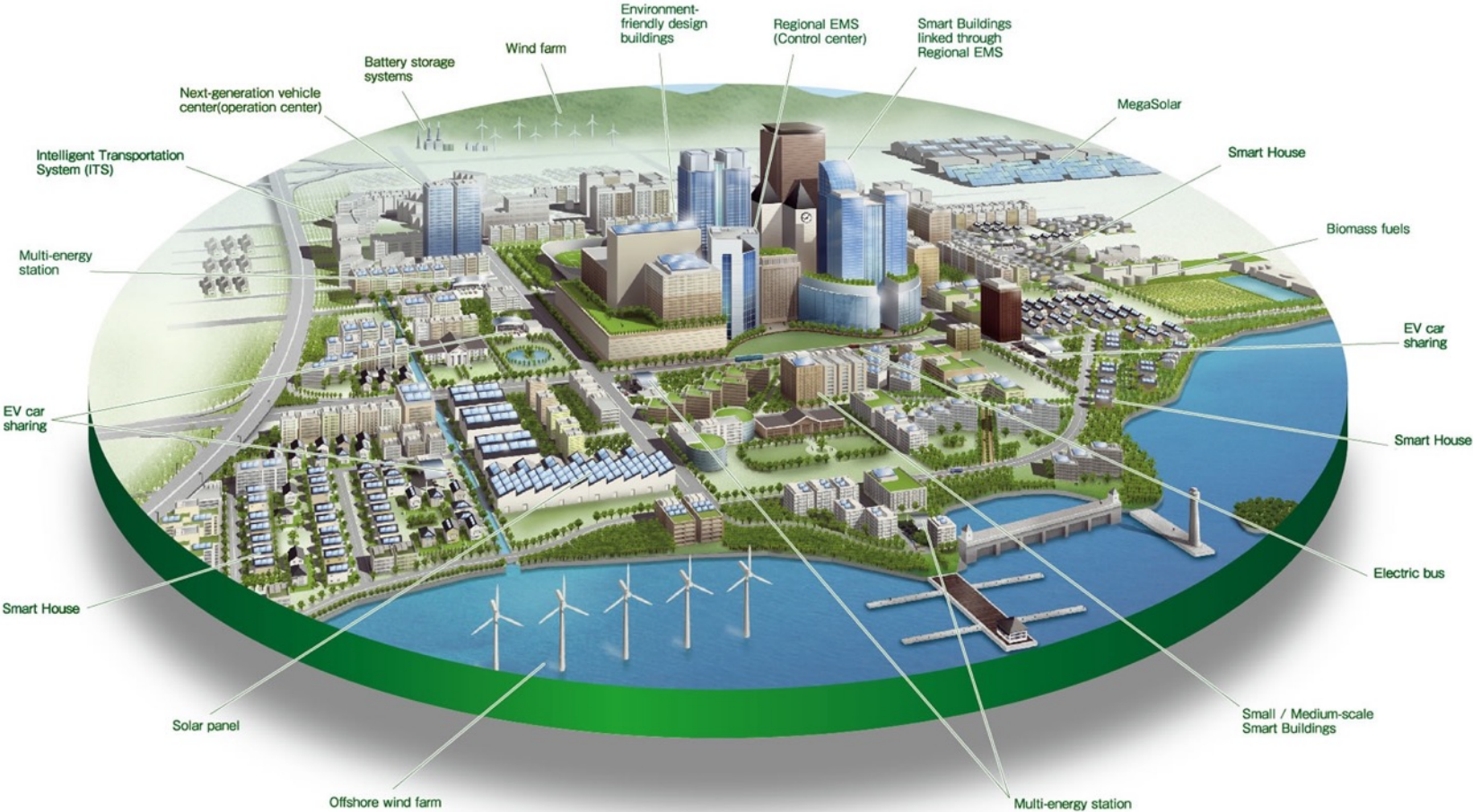
Risk Analysis

		LIKELIHOOD					
		A	B	C	D	E	
		Practically Impossible	Not likely to occur	Could occur or I've heard of it before	It is known to occur or "it has before"	Common or occurs frequently	
C O N S E Q U E N C E S	1	First Aid Injury	Low	Low	Medium	Medium	High
	2	Medical treatment injury	Low	Medium	Medium	High	Extreme
	3	Lost Time Injury less than 7 days	Medium	Medium	High	Extreme	Extreme
	4	LTI > 7 days PTD or fatality	Medium	High	Extreme	Extreme	Extreme
	5	Multiple PTD or fatalities	High	High	Extreme	Extreme	Extreme
		Low – Monitor and manage					
		Medium – Monitor and maintain strict measures					
		High – Review and introduce additional controls to lower the level of risk					
		Extreme – Do not proceed – Immediately introduce further control measures to lower the risk. Re assess before proceeding					

Compliance



Smart Cities



Smart Cities



Times are Changing...

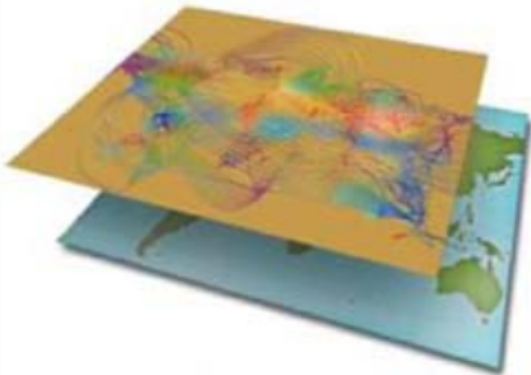


Cyber, Cyber, Everywhere

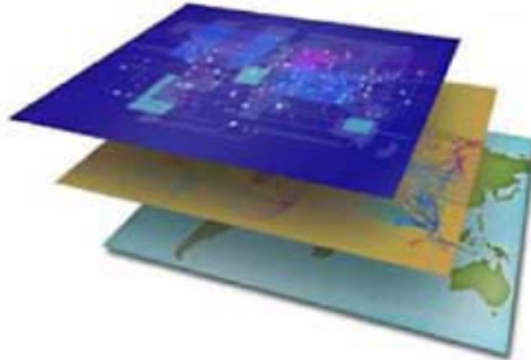


“Layers of Cyberspace”

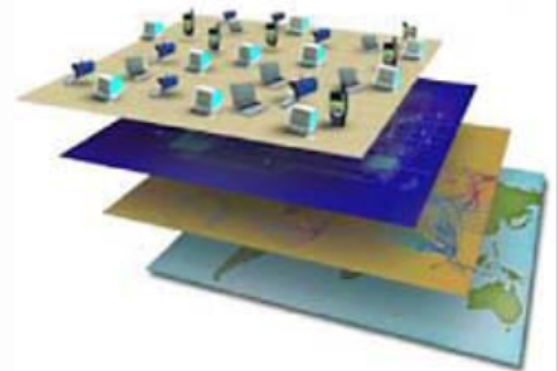
Physical Network Layer



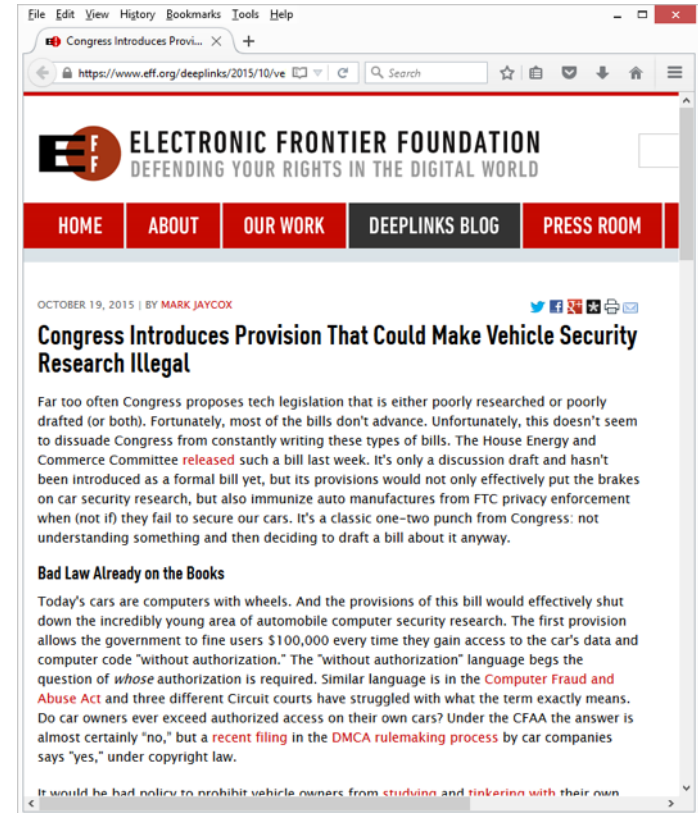
Logical Network Layer



Cyber-Persona Layer



War on General Purpose Computing



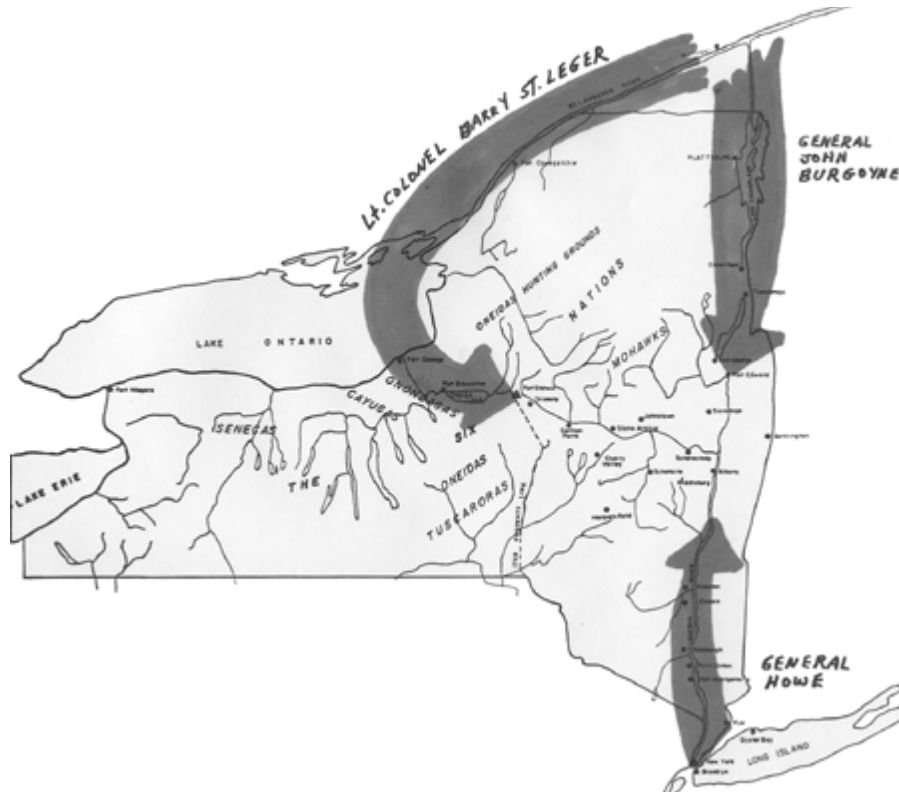
(Human && Machine) >> (Human || Machine)



Parting Thoughts

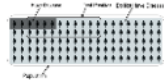


Think in Terms of Research Campaigns



- Long Term
- Inform decision makers
- Communicate with different audiences
- Research vision

Marketplace of Ideas



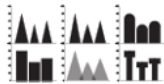
Improving Bayesian Reasoning: The Effects of Phrasing, Visualization, and Spatial Ability

Alvitta Ottley, Evan M. Peck, Lane Harrison, Daniel Afergan, Caroline Ziemkiewicz, Holly A. Taylor, Paul K. J. Han, Remco Chang
IEEE Transactions on Visualization and Computer Graphics (Proc. InfoVis), 2015



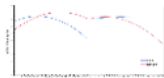
BRAAHMS: A Novel Adaptive Musical Interface Based on Users' Cognitive State

Beste F. Yuksel, Daniel Afergan, Evan M Peck, Garth Griffin, Lane Harrison, Nick W.B. Chen, Remco Chang and Robert J.K. Jacob
New Interfaces for Musical Expression (NIME), 2015



An Evaluation of The Impact of Visual Embellishments In Bar Charts

Drew Skau, Lane Harrison, Robert Kosara
Computer Graphics Forum (Proc. EuroVis), 2015



Infographic Aesthetics: Designing for the First Impression

Lane Harrison, Katharina Reinecke, Remco Chang
Proc. ACM Human Factors in Computing Systems (CHI), 2015



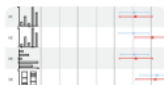
Ranking Visualizations of Correlation Using Weber's Law

Lane Harrison, Fumeng Yang, Steven Franconeri, Remco Chang
IEEE Transactions on Visualization and Computer Graphics (Proc. InfoVis), 2014



Visualization Evaluation for Cyber Security: Trends and Future Directions

Diane Staheli, Tamara Yu, Jordan Crouser, Suresh Damodaran, Kevin Nam, David O'Gwynn, Sean McKenna, Lane Harrison
Proceedings of the Eleventh International Symposium on Visualization for Cyber Security (VizSec), 2014



Influencing Visual Judgment through Affective Priming

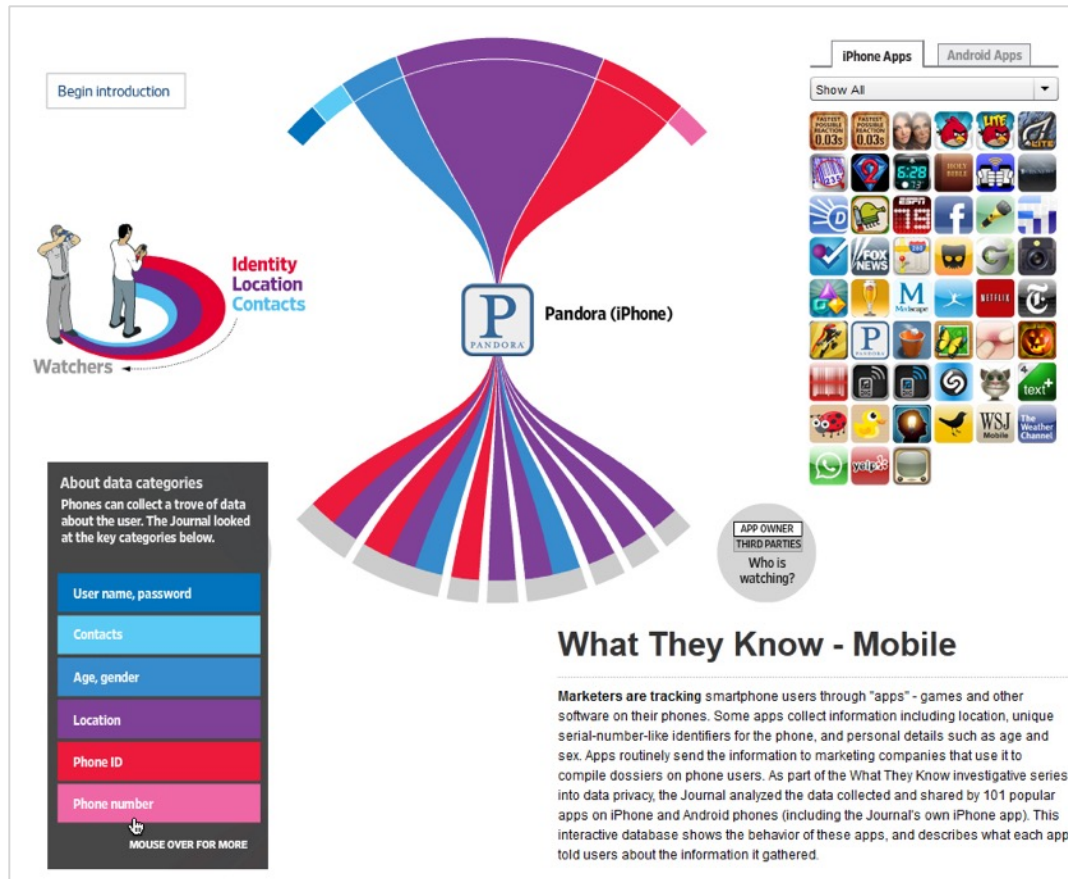
Lane Harrison, Drew Skau, Steven Franconeri, Aidong Lu, Remco Chang
Proc. ACM Human Factors in Computing Systems (CHI), 2013



The adaptive user: Priming to improve interaction

Alvitta Ottley, Evan M Peck, Lane Harrison, Remco Chang
ACM CHI 2013 Workshop on Many People Many Eyes, 2013

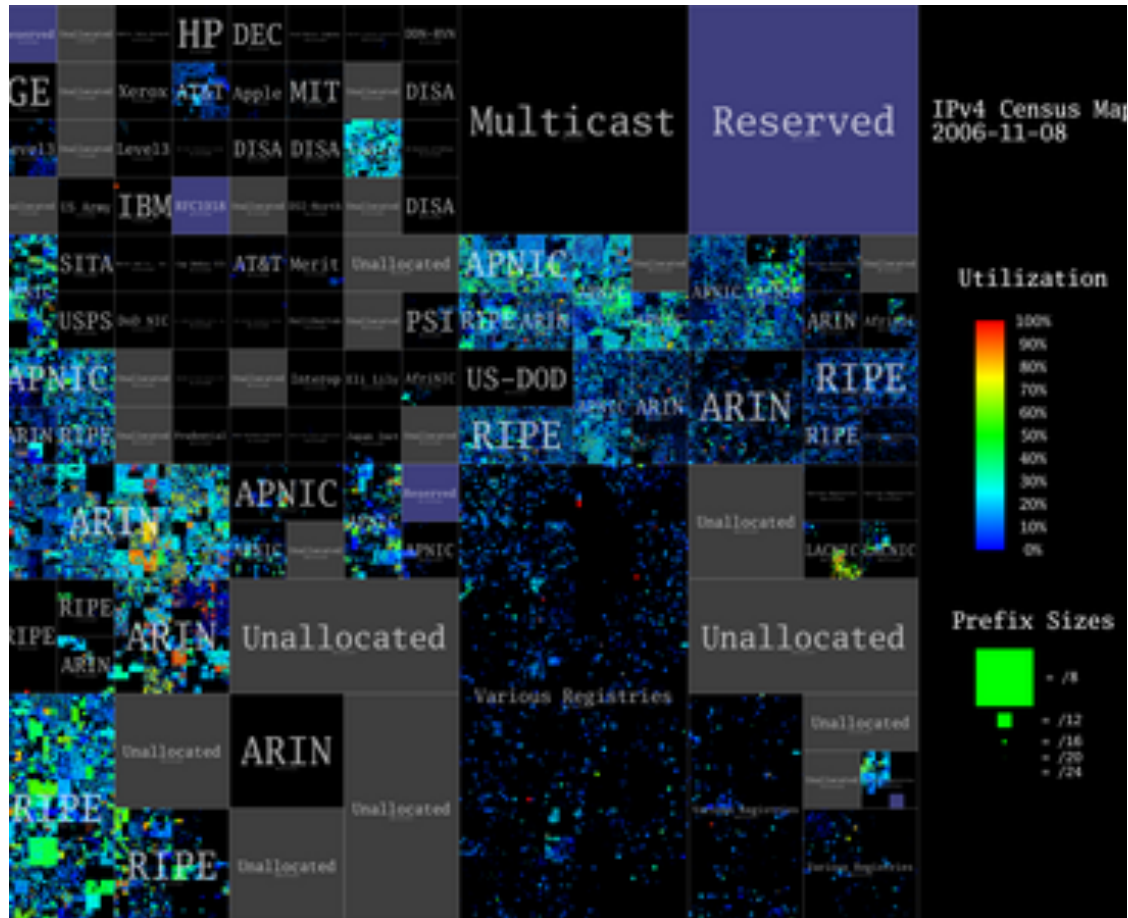
Engage/Support the Media



Challenge Assumptions

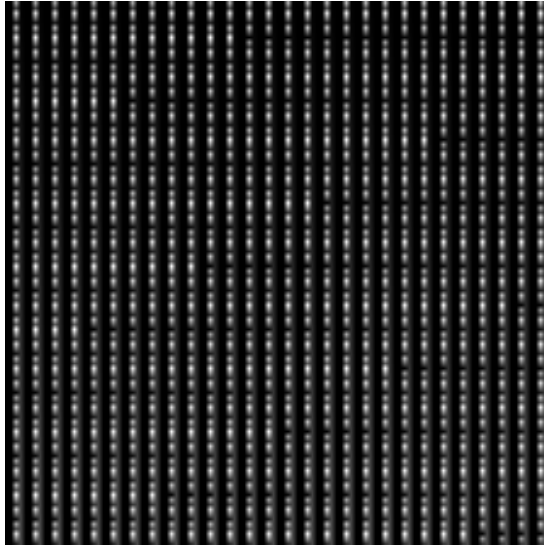


Think Big



Cooperative Association for Internet Data Analysis (CAIDA)
2007 IPv4 Census Map (two-month ping sweep)

Think Small



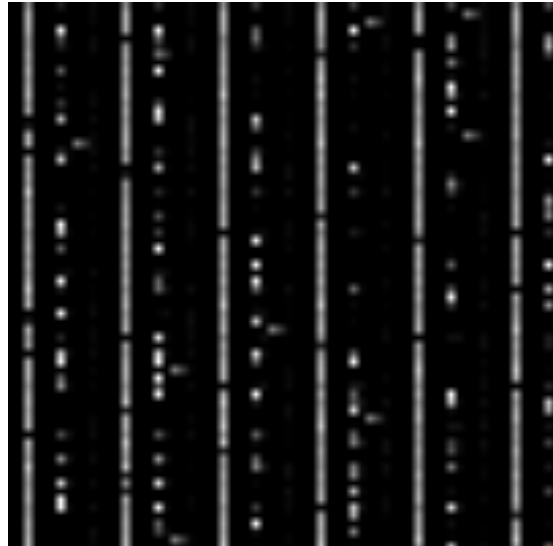
Microsoft Word 2003 .doc



Firefox Process Memory



Windows .dll

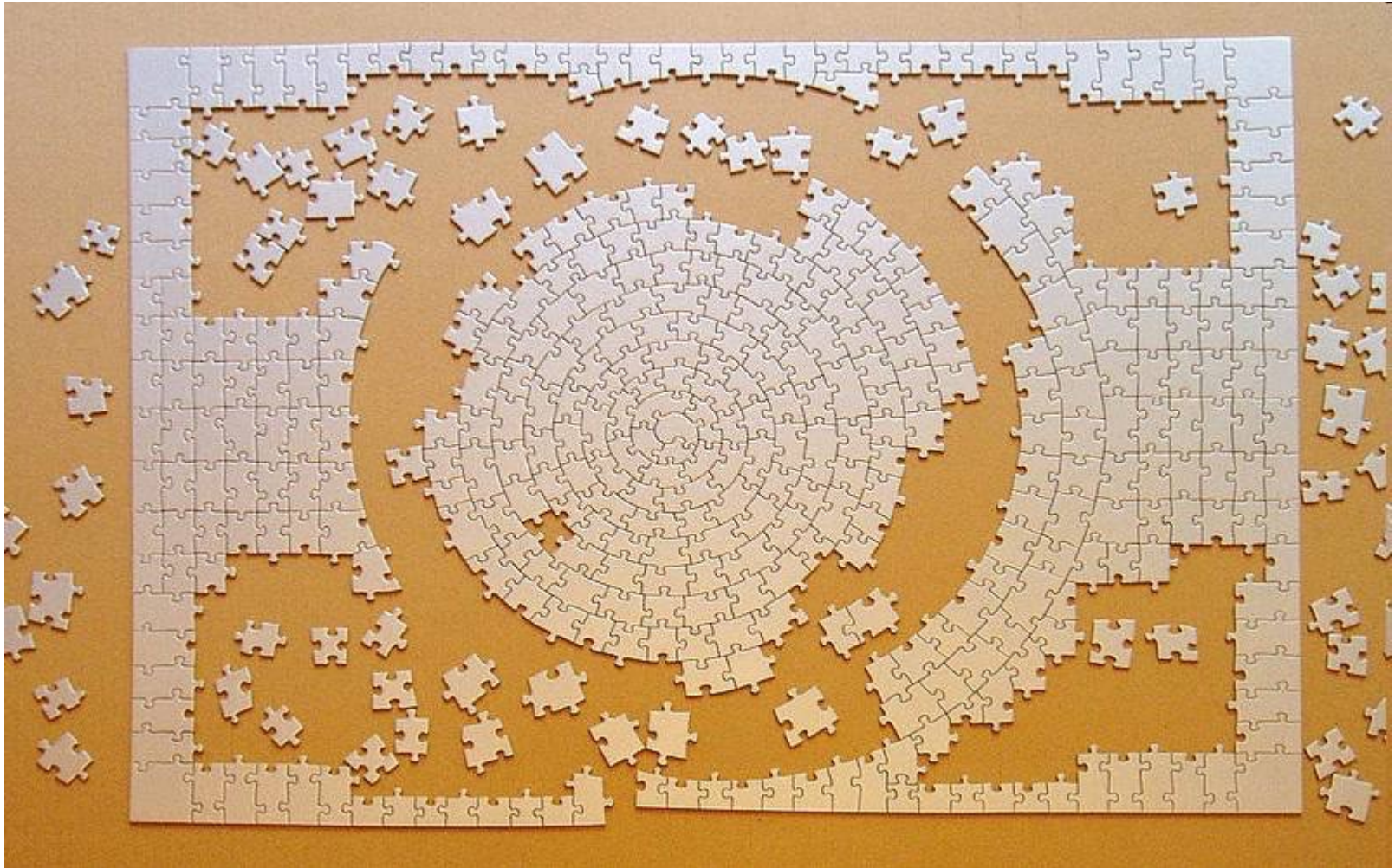


Neverwinter Nights Database

Irritate Software, Hardware, Protocols, and People



Detect Patterns



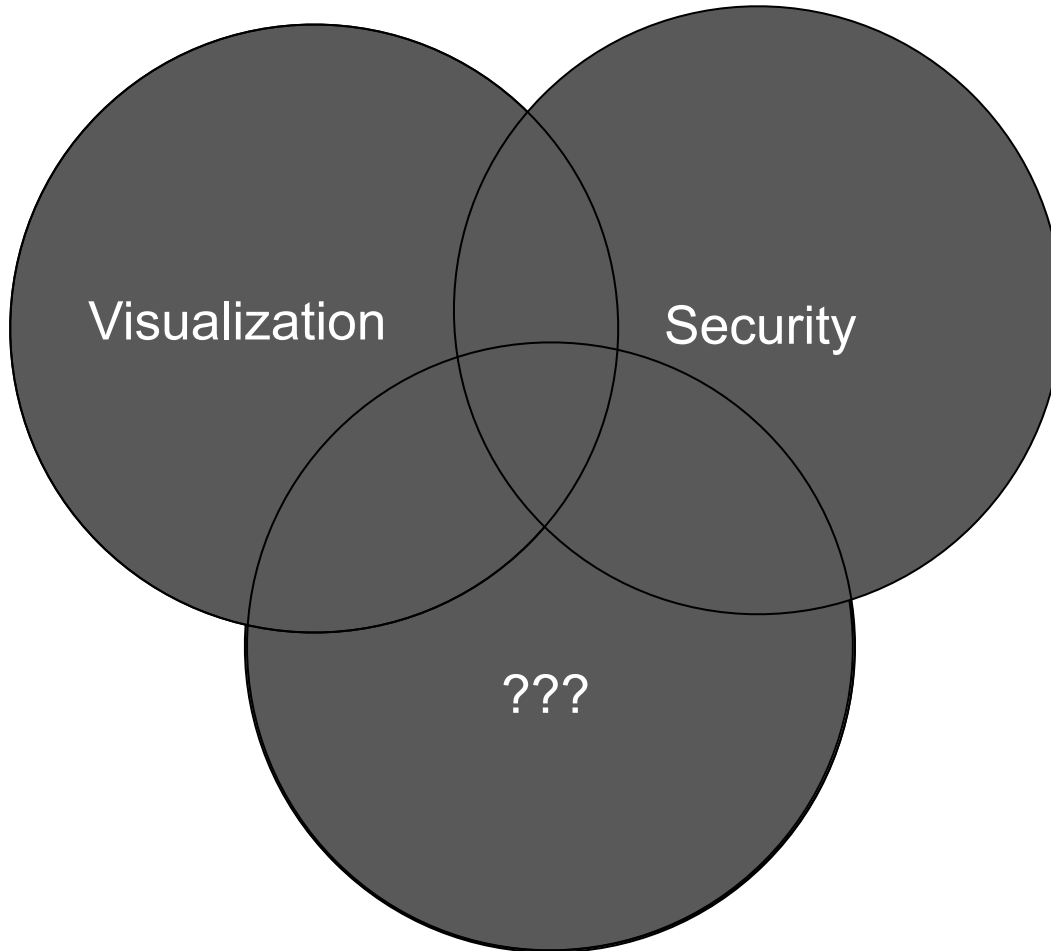
Detect Patterns



\$500,000 Worth of Bitcoins Stolen	276
Ask Amir Taaki About Bitcoin	741
Friday's Big Swings, Mostly Down, Illustrate Bitcoin Value Volatility	469
Bitcoin Used For the Narcotics Trade	535
AMD Betting Future On the GPGPU	181
Increased Power Usage Leads to Mistaken Pot Busts for Bitcoin Miners	411
Mint It Yourself With a Browser-Based Bitcoin Miner	490
BitCoin, the Most Dangerous Project Ever?	858
Google Engineer Releases Open Source Bitcoin Client	280
Online-Only Currency BitCoin Reaches Dollar Parity	517
2011	2010
WikiLeaks, Money, and Ron Paul	565
Bitcoin Releases Version 0.3	491

<http://slashdot.org/index2.pl?fhfilter=bitcoin>

Look at the Intersection of Your Interest Areas



- Robots
- Software Defined Radio
- Cyber Operations
- Malware
- Deception
- Privacy
- Social Engineering
- Insider Threat
- ...
- <What are you passionate about?>

What Makes You Mad

The image shows a screenshot of a weather website interface. On the left, the weather for West Point, NY (10996) is displayed as 'Cloudy' with a temperature of 68°F. A 'Right Now for' section includes a 'Save Location' link and language/metric options. A 'Weather for your life' section has a dropdown menu. A 'VIDEO' section features a 'Your Local Forecast' video thumbnail and a 'Today's Highlights' list with links to news items like 'We now have Tropical Storm Fay' and 'Ask Cantore: What Causes Fog?'. A 'STORM WATCH' section is also visible. On the right, a large advertisement for Stoli Blakberi vodka is shown, featuring a bottle flying through the air and a couple clinking glasses. The ad includes a countdown timer showing 01:27:49 and the text 'UNTIL YOUR NIGHT BEGINS' and 'START IT OFF WITH THE NEW Stoli Blakberi'. A 'CLOSE [X]' button is overlaid on the ad. At the bottom of the ad, it says 'CHOOSE RESPONSIBILITY. STOLI BLAKBERI VODKA'.

Flying Vodka Bottles

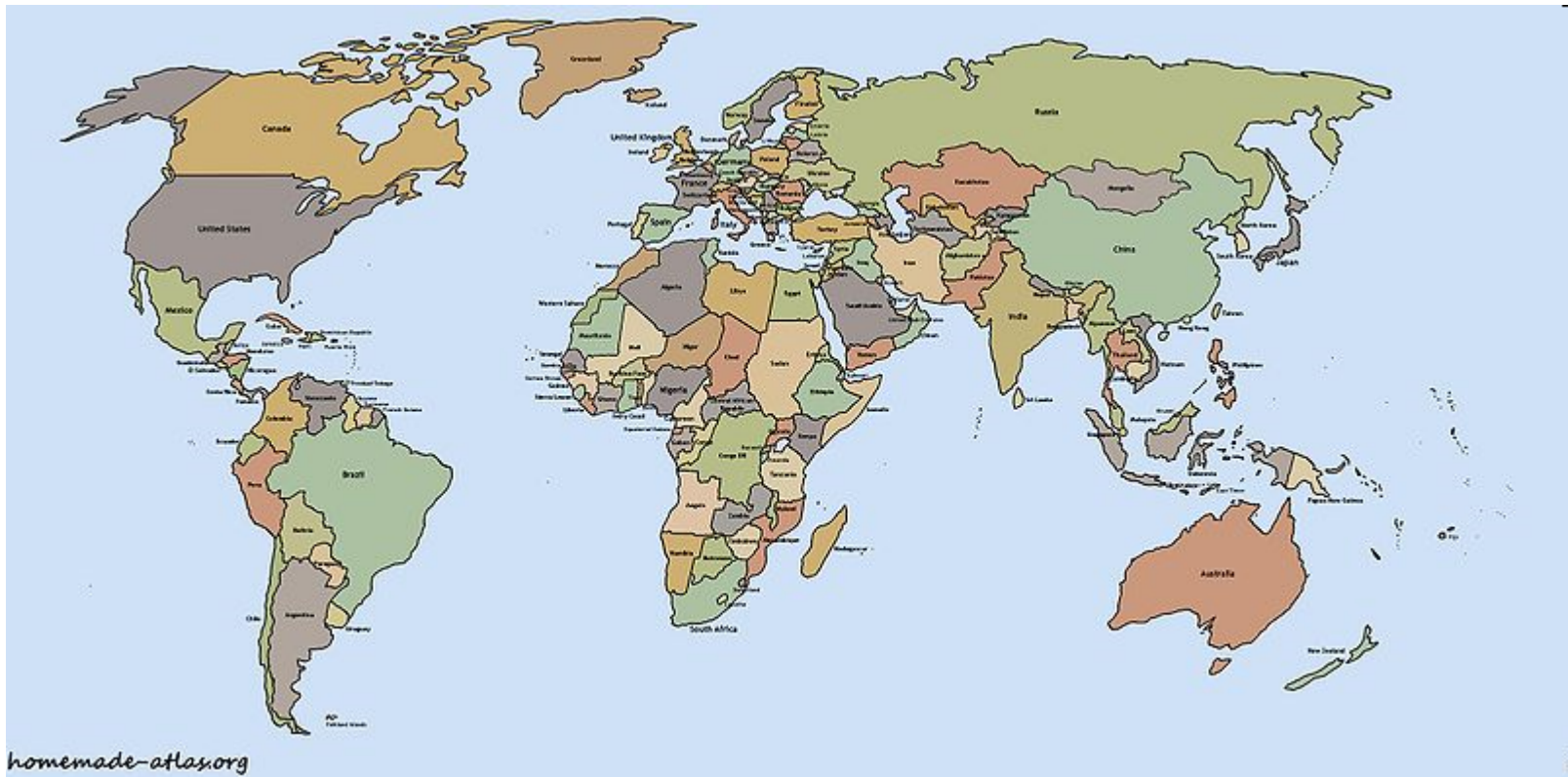
What Can Possibly Go Wrong



Pretty Pictures



Think Like a Nation-State



Look in Cracks, Crevices, Under Rocks, and Other Dark Places



VizSec 2015

Chicago, Illinois, USA
October 25, 2015



Enjoy the Golden Age of Visualization :)



Questions???