



# **THE EVOLVING DYNAMICS OF CYBER RISK: WHAT BEHAVIORAL ECONOMICS CAN TEACH US ABOUT CYBER LIABILITY AND RELATED EMERGING RISKS**

**MICHAEL SOLOMON, FCAS, MAAA, CERA**

**BEN GOODMAN, CRISC**

**UNDERWRITING COLLABORATION SEMINAR**

**CHICAGO, IL**

**MARCH 6, 2017**



# Antitrust Notice

- **The Casualty Actuarial Society is committed to adhering strictly to the letter and spirit of the antitrust laws. Seminars conducted under the auspices of the CAS are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.**
- **Under no circumstances shall CAS seminars be used as a means for competing companies or firms to reach any understanding – expressed or implied – that restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition.**
- **It is the responsibility of all seminar participants to be aware of antitrust regulations, to prevent any written or verbal discussions that appear to violate these laws, and to adhere in every respect to the CAS antitrust compliance policy.**



# Introduction to Session

- Learning Objectives

- Understanding emerging risk in the cyber space
- The Dark Web
  - Deconstructing “emerging risk”
  - Cognitive/perceptual “blind spots” and how those may impact decision making
  - Applications/implications for insurance
    - Capacity
    - SIRs/Deductibles
- Rethinking emerging risk in the cyber arena



# Introduction to Michael Solomon

- FCAS, MAAA, CERA
- 1<sup>st</sup> Prize, Society of Actuaries/ Casualty Actuarial Society Joint Risk Section Cybersecurity call for Essays
- 1<sup>st</sup> Prize, Professionally Speaking Toastmasters public speaking competition
- CAMAR Vice President
- Member, Committee for P&C focused ERM Seminars
- Member, CAS/ CIA/ SOA Impairment Project Oversight Group



# Introduction to Ben Goodman

- Founder & CEO, 4A Security & Compliance
- CRISC Worldwide Achievement Award
- Faculty Member, Drexel LeBow College of Business, Corporate & Executive Education
- Member, Cybersecurity Advisory Board, Pace University Seidenberg School of Computer Science
- Member, CAS Cyber Risk Task Force
- Member, SOA Cybersecurity Insurance: Modeling and Pricing Project Oversight Group





## COMMON EXPERIENCE OF THE INTERNET “NETWORK EFFECT”





## CASTING A NET ACROSS THE “SURFACE WEB”



Google



Google Search

I'm Feeling Lucky



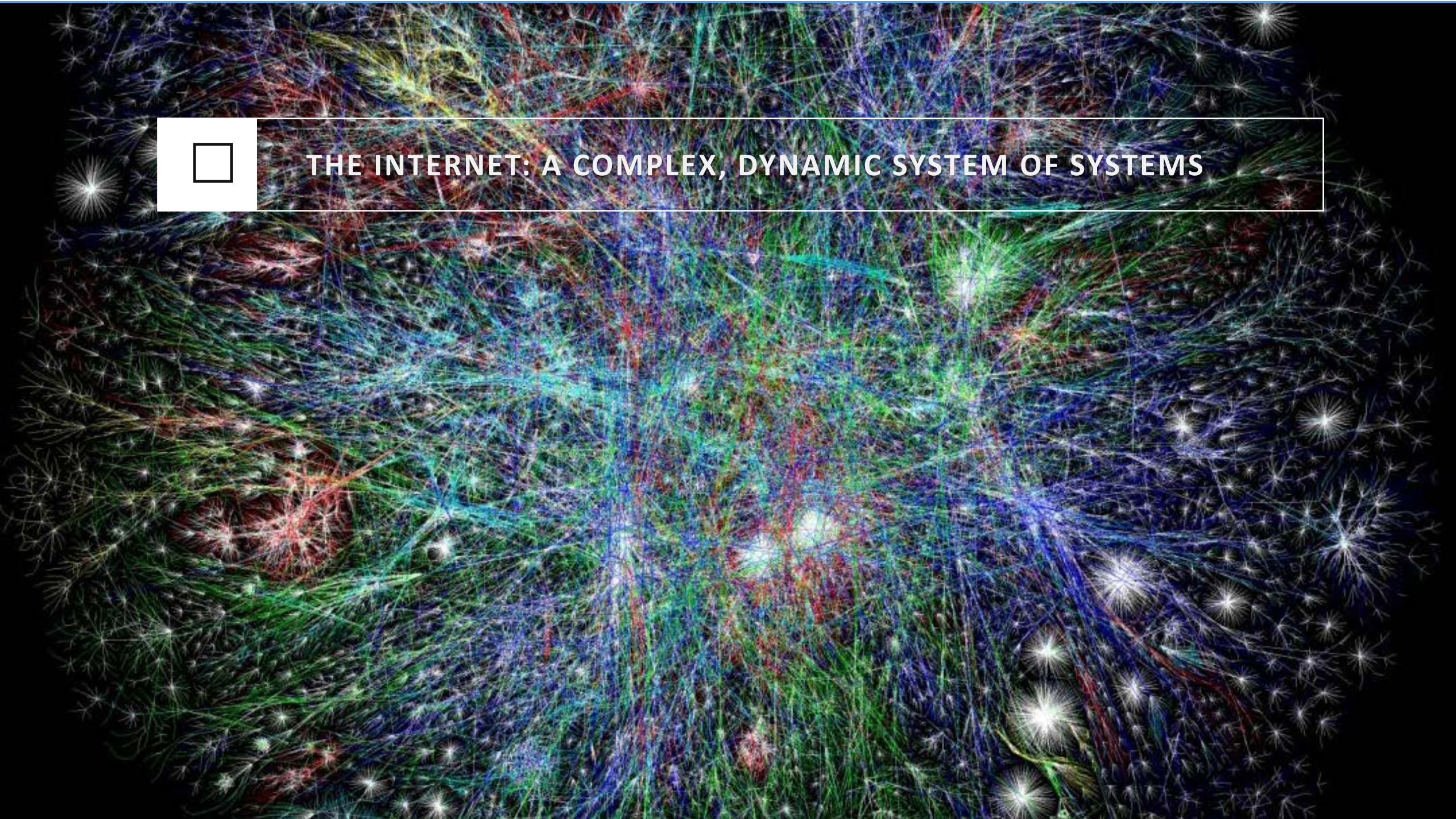
## WE INTERACT WITH THE “SURFACE WEB”

The screenshot shows the Amazon.com homepage in a browser window. The browser's address bar displays "amazon.com". The page features a dark navigation bar with the Amazon logo, a search bar, and links for "style code LIVE", "WATCH & SHOP NOW", "Account & Lists", "Orders", "Try Prime", and "Cart". Below the navigation bar is a large banner for "Back to Business" with the text "Save on work supplies" and an image of office supplies. The main content area is divided into several sections: "Welcome" with a "Sign in securely" button, "Popular departments" featuring "Kindle" and "Amazon Video", "Style Code Live" with a photo of a man and a woman, and an advertisement for "Enjoy family TV fun with Prime Video monthly" with a "Get started" button and the Amazon logo. At the bottom, a "Deal of the day" section is partially visible.





# THE INTERNET: A COMPLEX, DYNAMIC SYSTEM OF SYSTEMS





# B2B SOFTWARE AS A SERVICE

The screenshot shows the Epicor website homepage. At the top, there is a navigation bar with 'Partners' and 'Customers' links. The main hero banner features a large graphic of a stylized 'E' and the headline 'See How Epicor Gets Distributors Set for Growth' with a 'Learn More' button. Below this is a section for 'Industry-focused Applications' with icons for Distribution, Manufacturing, Retail, Services, Automotive Aftermarket, and LBM. The 'Featured Content' section includes four cards: 'Cloud', 'Business Growth Strategies', 'Retail Resource Center', and 'Videos'. At the bottom, the 'Our Customers' section displays logos for various companies including Rexel, Energizer, ACE, JeldWen, and North American Lumber.

ERP | Retail Software | C x +  
epicor.com/default.aspx

## See How Epicor Gets Distributors Set for Growth

Learn More

grow business ☁ not software™

### Industry-focused Applications

- Distribution
- Manufacturing
- Retail
- Services
- Automotive Aftermarket
- LBM

### Featured Content

- Cloud**  
Cloud eliminates barriers to implementing or upgrading software and allows businesses to focus on core business operations.  
More >
- Business Growth Strategies**  
Learn how to perfect your business growth plans with Epicor.  
More >
- Retail Resource Center**  
Explore how retailers can streamline processes, integrate channels, and inspire customers.  
More >
- Videos**  
Explore the library of customer videos to learn industry knowledge from your peers.  
More >

### Our Customers

- REXEL
- Energizer
- ACE
- JELD WEN
- North American Lumber



## THE MEANS OF PRODUCTION HAS CHANGED





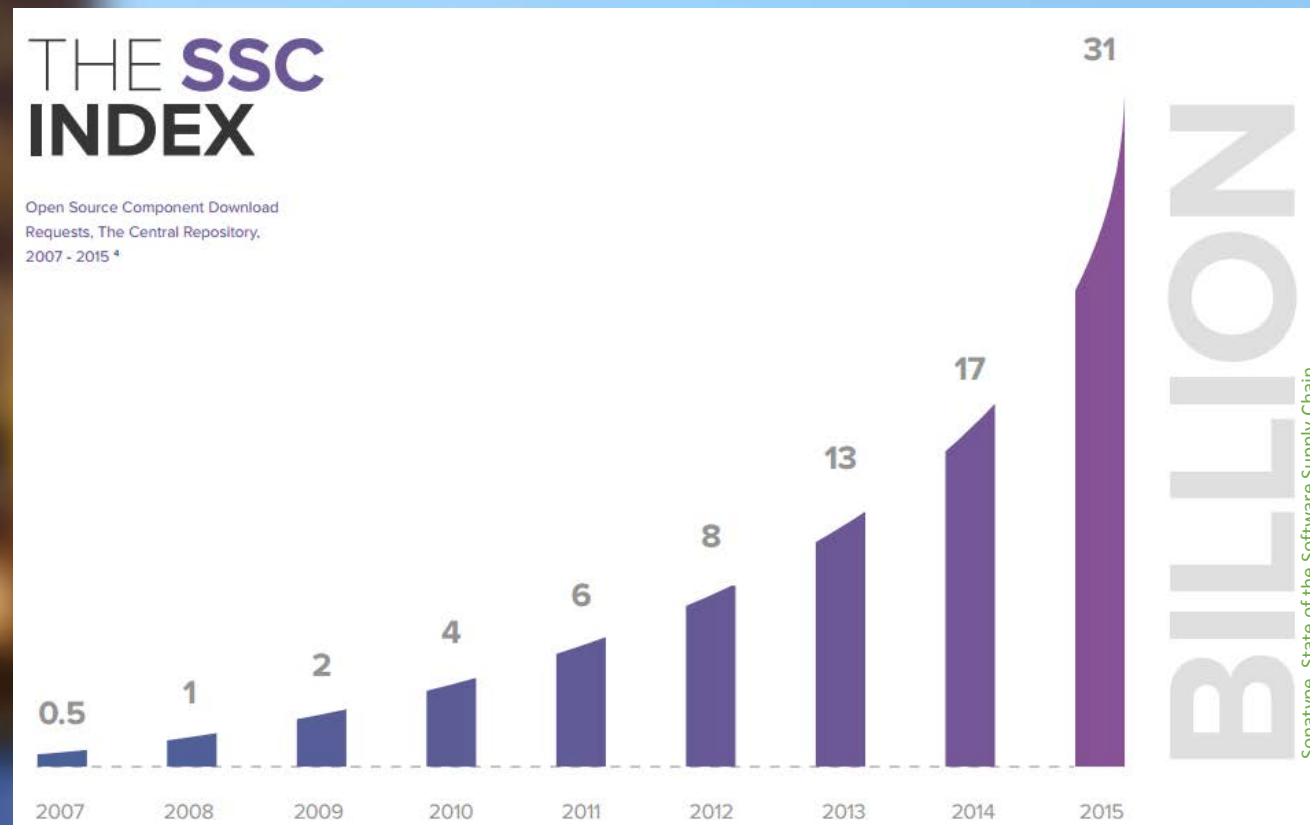
## THE MEANS OF PRODUCTION HAS CHANGED





## THE SOFTWARE SUPPLY CHAIN HAS CHANGED

31B Component Downloads by 10M Developers Worldwide

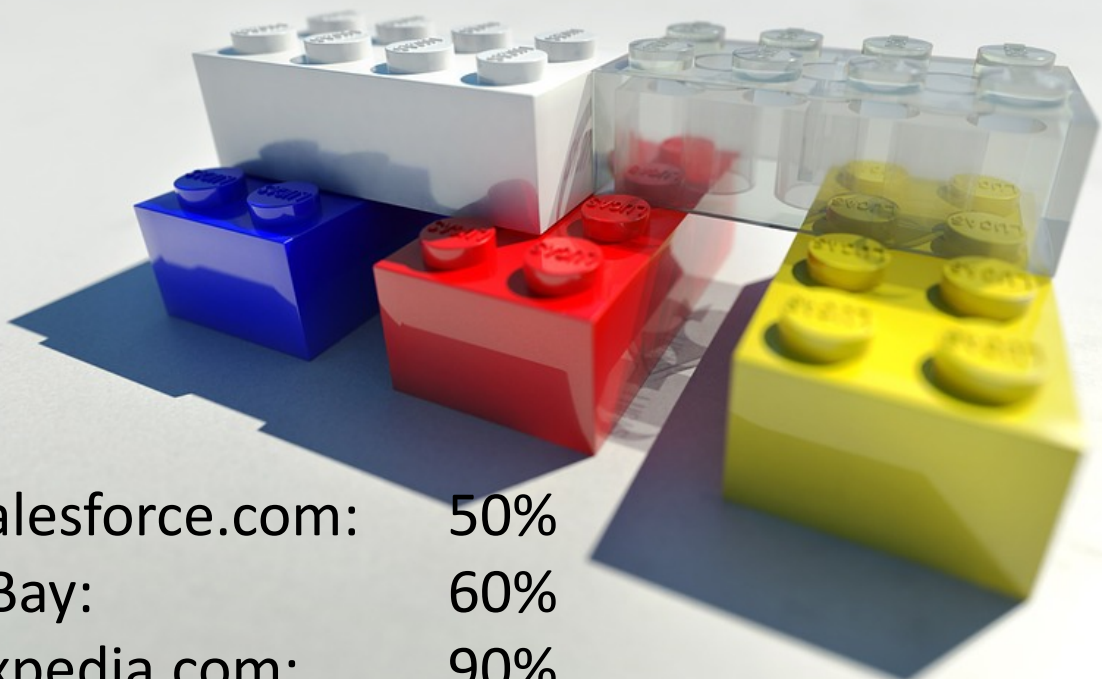




## BUSINESS MODELS DEPEND ON OTHER NETWORK PARTICIPANTS

Application programming interface (API) are a major revenue source

### % of Revenue Generated Through APIs

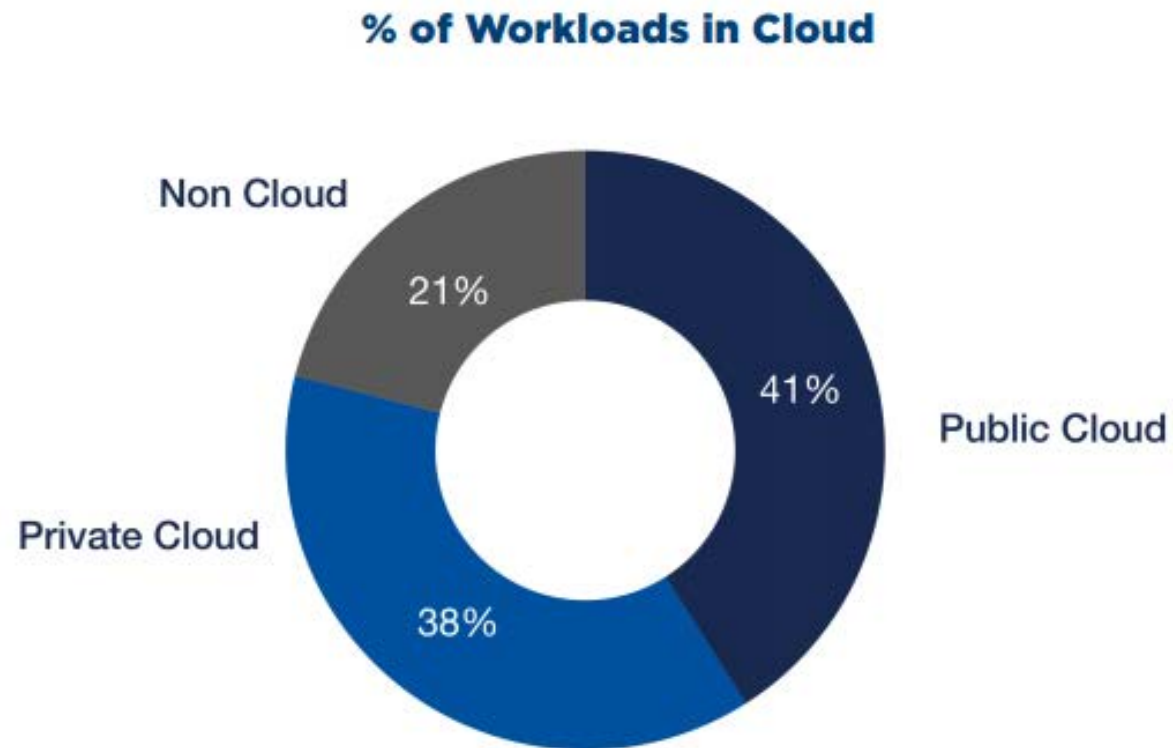


Salesforce.com:	50%
eBay:	60%
Expedia.com:	90%

Viewed February 17, 2017, Harvard Business Review  
<https://hbr.org/2015/01/the-strategic-value-of-apis>



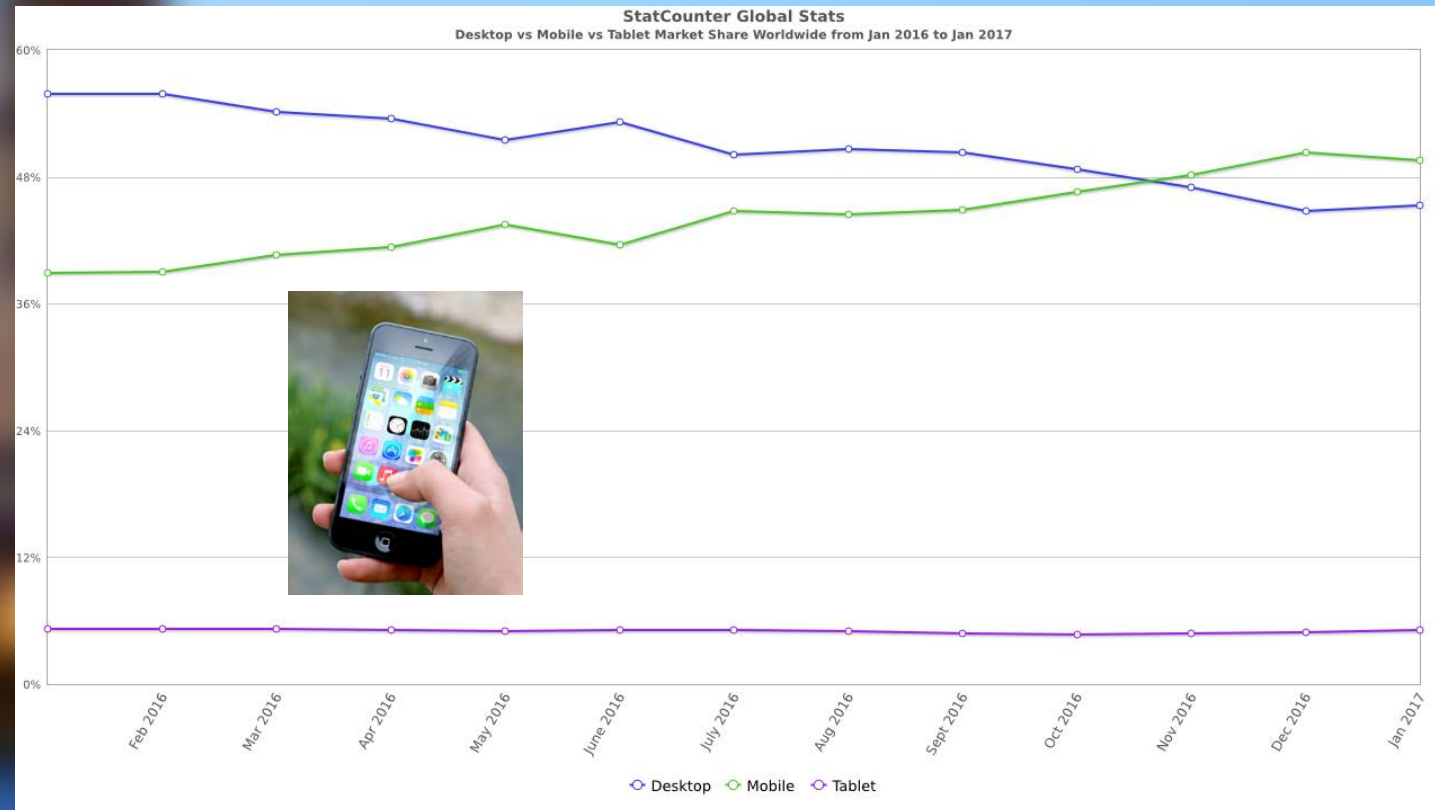
## IT INFRASTRUCTURE IS MOVING TO THE CLOUD



Source: RightScale 2017 State of the Cloud Report



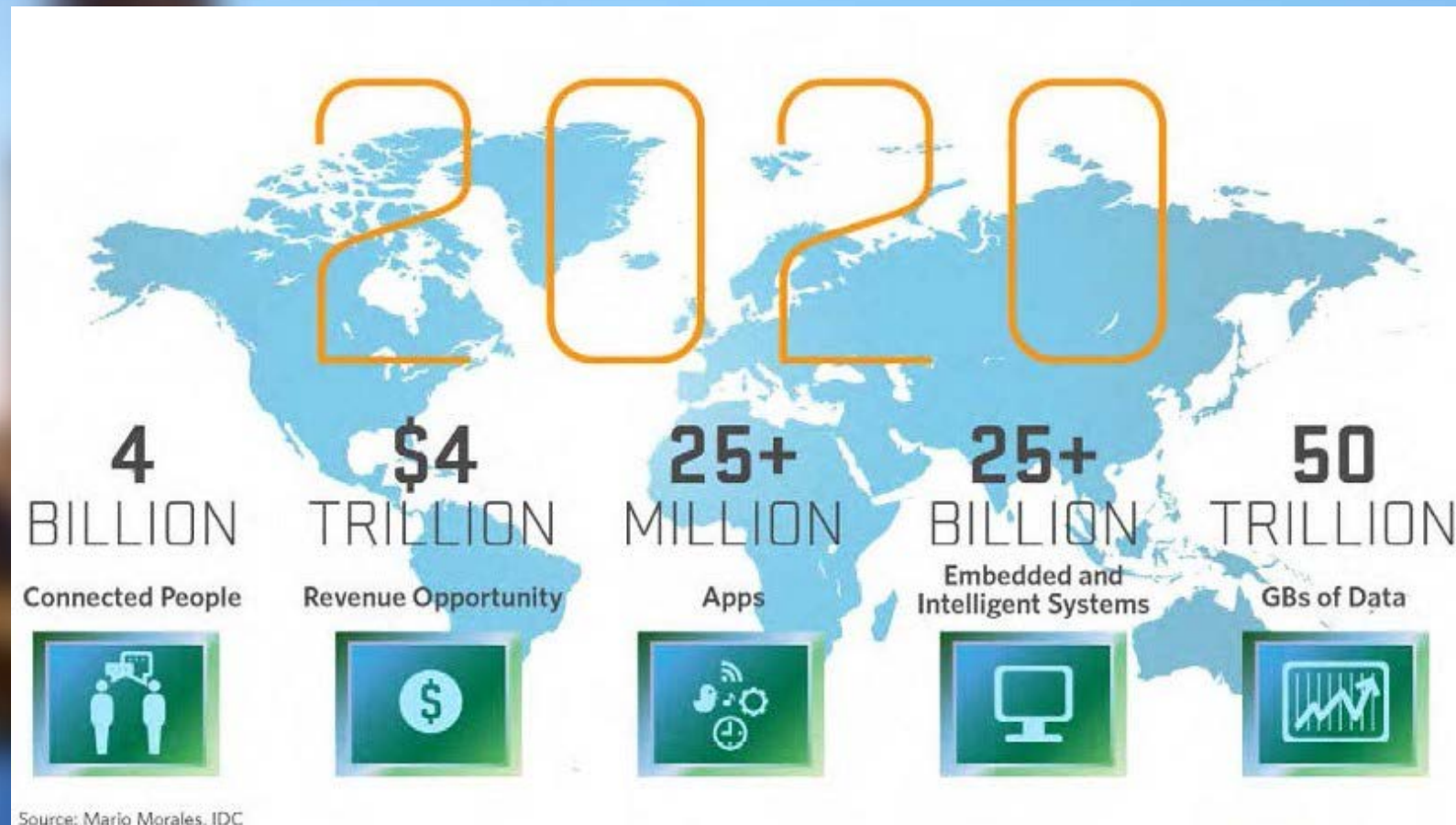
## MORE MOBILE THAN PC USERS





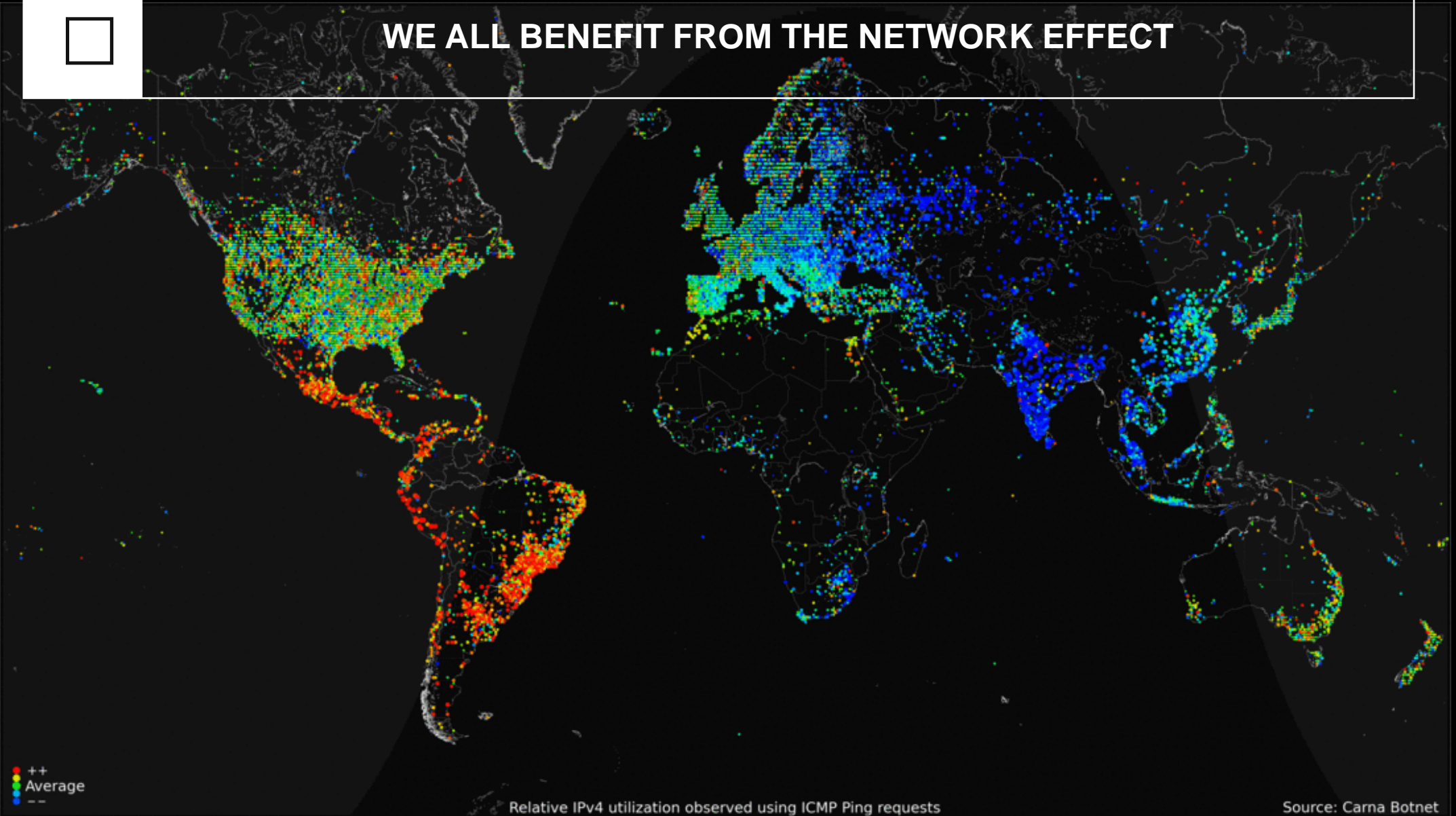


## THE INTERNET OF THINGS CHANGES THE GAME AGAIN



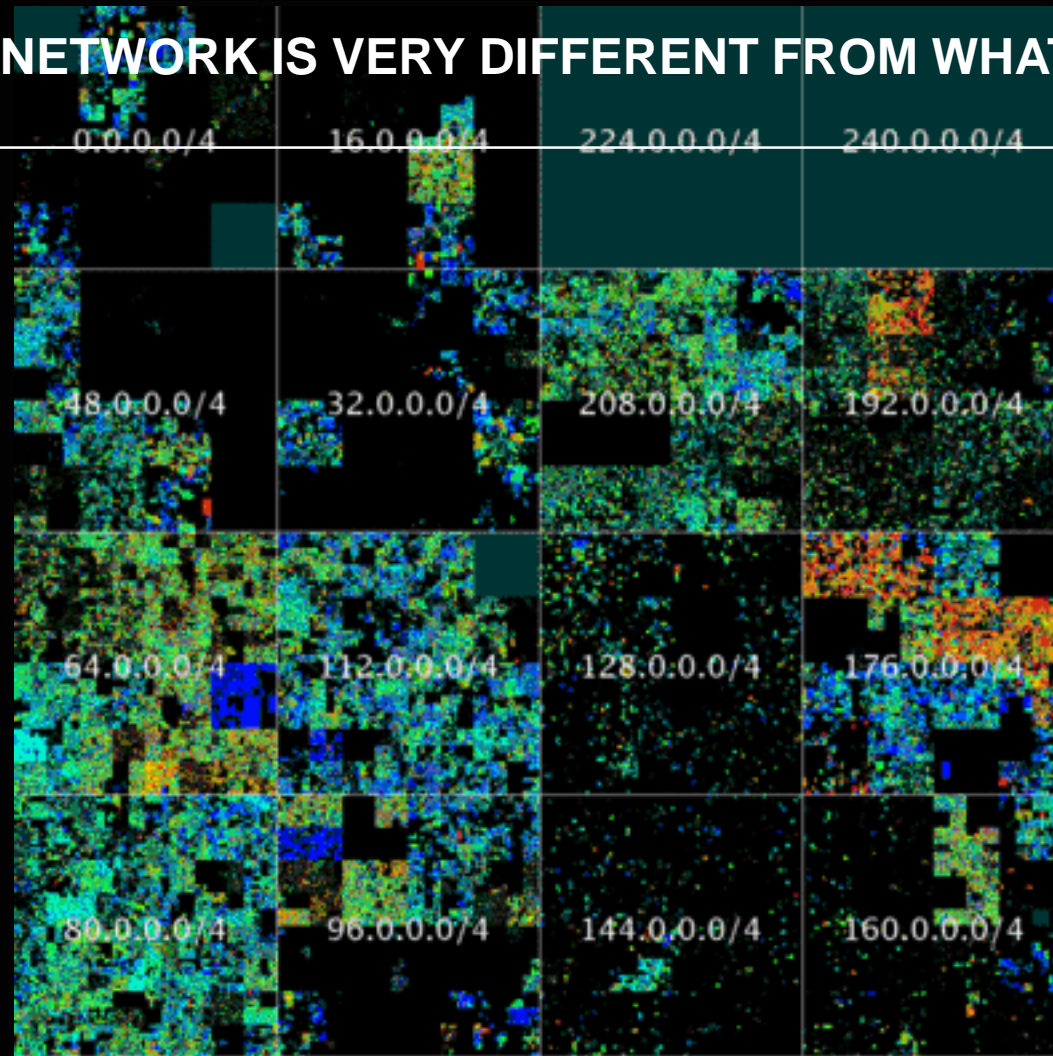


# WE ALL BENEFIT FROM THE NETWORK EFFECT





# THE NETWORK IS VERY DIFFERENT FROM WHAT WE IMAGINE

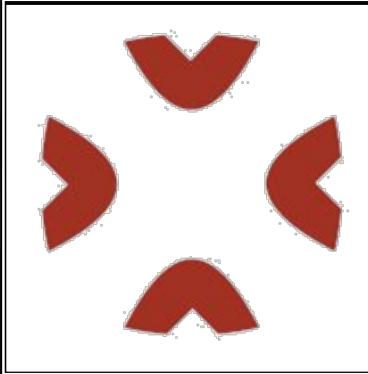


++  
Average  
--

16:00 Los Angeles  
19:00 New York

01:00 Amsterdam  
04:00 Moscow

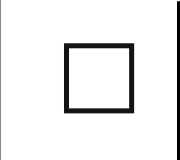
08:00 Shanghai  
10:00 Sydney



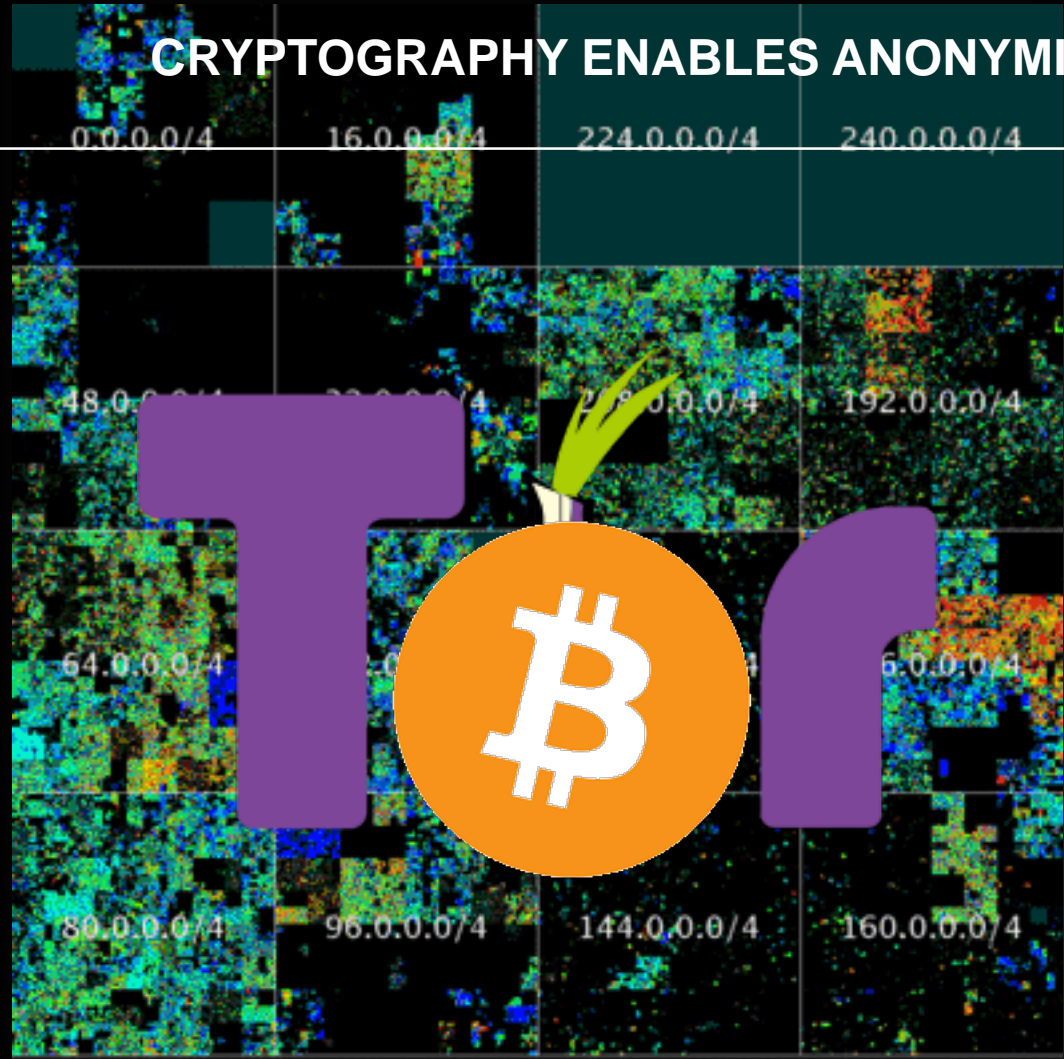
**THE NETWORK CO-EXISTS WITH**

**THE DEEP WEB AND THE DARK WEB**



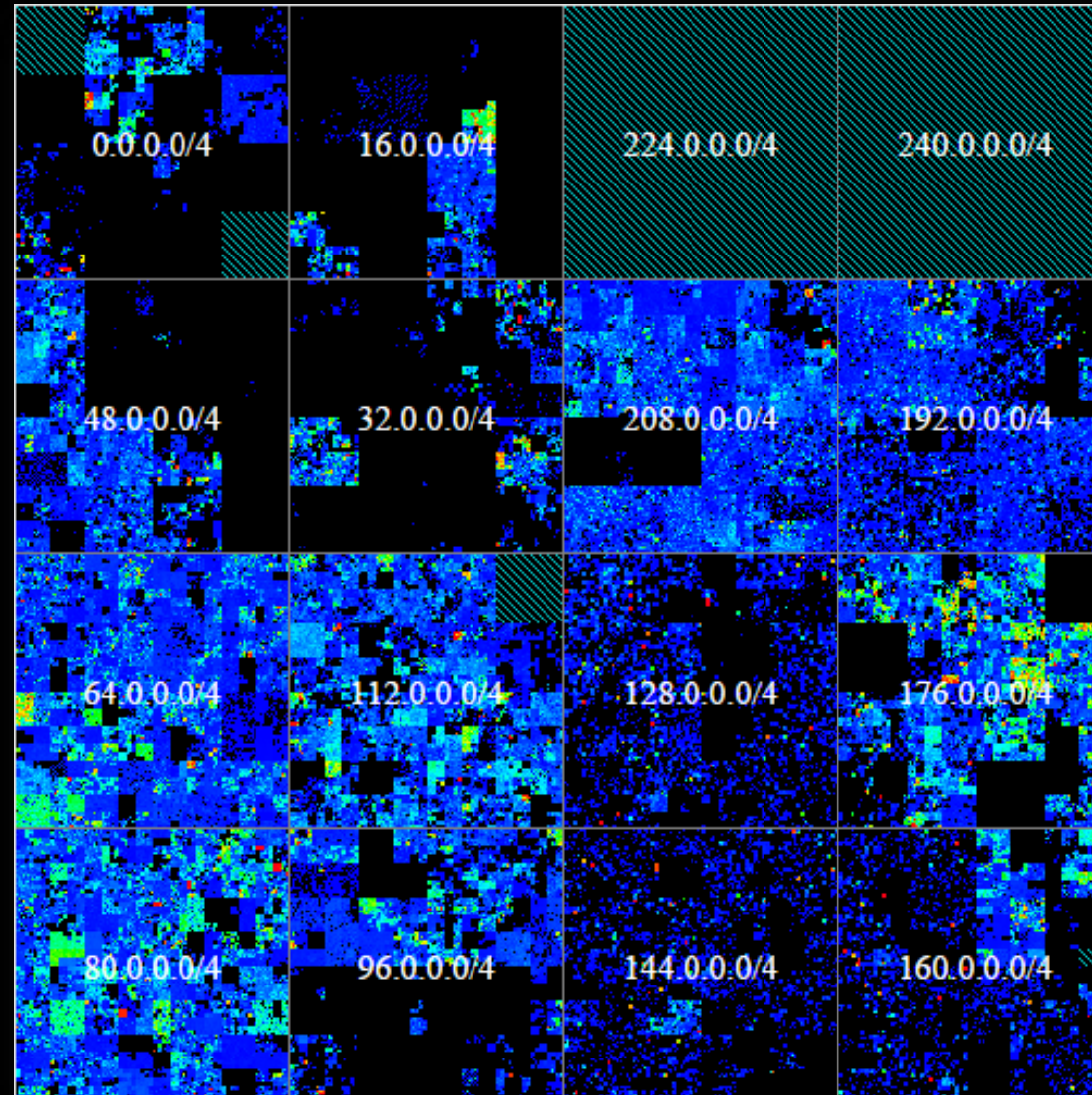


# CRYPTOGRAPHY ENABLES ANONYMITY



++ 16:00 Los Angeles 01:00 Amsterdam 08:00 Shanghai  
Average 19:00 New York 04:00 Moscow 10:00 Sydney  
--

Relative IPv4 utilization observed using ICMP Ping requests Source: Carna Botnet









# TOR-ANONYMOUS WEB SURFING ON THE DARKNET

View Tor Network

Refresh Zoom In Zoom Out Zoom To Fit Help Close

Server

- whistlersmother
- tutzing
- desync
- chaoscomputercl...
- charlesbabbage
- freetux4ever
- Tonga
- madrid2
- jalopy
- croeso
- bettyboop
- myrnaloy
- tormentor
- b4tz
- tor26
- lefkada
- k0w
- mytornodefig
- communicator
- BostonUCompSci
- anonymusbalserc
- dizum
- pcpoint
- terpion
- cweiske
- sasquatch
- adeia
- inap1

Connection	Status
so19charismax,sasquatch,bellerophon...	Open
h760662,desync,1df060248c02d8	Open
Webdust,MARSSolutions,Foe8uD2	Closed
gtisc,spoon,recursion	Closed
209.237.230.67:80	Retry...
209.237.230.67:80	Retry...

gtisc (Online)

Location: US

IP Address: 199.77.130.14

Platform: Tor 0.1.1.23 on Linux i686

Bandwidth: 1211 KB/s

Uptime: 18 hours 26 mins 16 secs



## SEARCHING FOR HIDDEN SERVICES ON THE DARKNET

# **nionCity**

*Enabling search and global access to Tor's onionsites*

[ [FAQ](#) ]

[ [Security](#) ]

[ [Legal](#) ]

Media mentions! [Naked Security](#) [FreedomHacker](#) [Digital News Asia](#)





## HIDDEN WIKI LINKS TO HIDDEN SERVICES

<http://6w6vcynl6dumn67c.onion/> – Tor Market Board – Anonymous Marketplace Forums

<http://wvk32thojln4gpp4.onion/> – Project Evil

<http://5mvm7cg6bgklfjtp.onion/> – Discounted electronics goods

<http://lw4ipk5choakk5ze.onion/raw/evbLewgkDSVkifzv8zAo/> – Unfriendlysolution – Legit hitman service

<http://nr6juudpp4as4gjjg.onion/torgirls.html> – Tor Girls

<http://tuu66yxvmn3of7l.onion/> – UK Guns and Ammo

<http://nr6juudpp4as4gjjg.onion/torguns.htm> – Used Tor Guns

<http://ucx7bkbi2dtia36r.onion/> – Amazon Business

<http://nr6juudpp4as4gjjg.onion/tor.html> – Tor Technology

<http://hbetshipq5yhhrsd.onion/> – Hidden BetCoin

<http://cstoreav7i44h2lr.onion/> – CStore Carded Store

<http://tfwdi3izigllure.onion/> – Apples 4 Bitcoin

<http://e2qizoerj4d6ldif.onion/> – Carded Store

<http://jvrnuue4bvbfiby.onion/> – Data-Bay

<http://bgkitnugq5ef2cpi.onion/> – Hackintosh

<http://vlp4uw5ui22jlg7.onion/> – EuroArms

<http://b4vqxw2j36wf2bqa.onion/> – Advantage Products

<http://ybp4oezfkhk24hxmb.onion/> – Hitman Network

<http://yth5q7zdmqlycbc.onion/> – Old Man Fixer's Fixing Services

<http://qizriixqwmeq4p5b.onion/> – Tor Web Developer

<http://vfqnd6mieccqyit.onion/> – UK Passports

<http://en35tuzqmn4lofbk.onion/> – US Fake ID Store

<http://xfnwyig7olydpdq5r.onion/> – USA Citizenship



## C2C CRIME AS A SERVICE

### TOP- DDOS Service (Support)

Order a ddos attack! Removable poster competition!

#### MENU

Home

Reviews

Rates

Methods of payment

Contacts



#### ▣ Rates

- ✓ 1:00, \$ 5
- ✓ 24-from \$ 40
- ✓ 1 week - from \$ 260
- ✓ 1 month - from \$ 900
- ✓ This is the minimum price. Prices depend on the line of targets.

#### ▣ Discounts:

- ✓ 1 week - 5%
- ✓ 2 weeks - 7%
- ✓ 3 weeks - 10%
- ✓ 1 month or more - 15%
- ✓ Also, when ordering from two sites also discounts.



## C2C CRIME AS A SERVICE

### Malware Drop Services for Sale

Главная Новости Настройки Баланс Задачи FAQ Выход

### Задачи

Новая задача

Путь до exe

Страна

Количество  заказа - 1000.

Стоимость

- Mix world
- Australia
- Canada
- Germany
- Mexico
- Netherlands
- Russian Federation
- Ukraine
- United Kingdom
- United States

□ TO C2C CRIME AS A SERVICE

# Botnet Services for Point-and-Click Users

**BHGroup full botnet setup A to Z**

\*\*\* This listing is non-refundable \*\*\* please read the description completely before buying the listing. this service is not recommended for low budget individuals. currently there is so such a service in deep web nor clearnet ! what is this service : this listing is for individuals who are interested to own a botnet for a lot of reasons. this service will help you to choose best b...

Sold by **BHGroup** - 12 sold since Dec 18, 2015 **Vendor Level 5** **Trust Level 5**

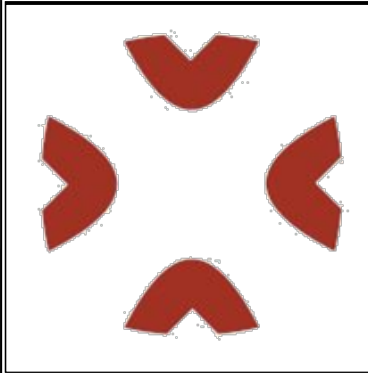
	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 20.00

Qty:  **Buy Now** **Queue**

0.0289 BTC / 2.7380 XMR

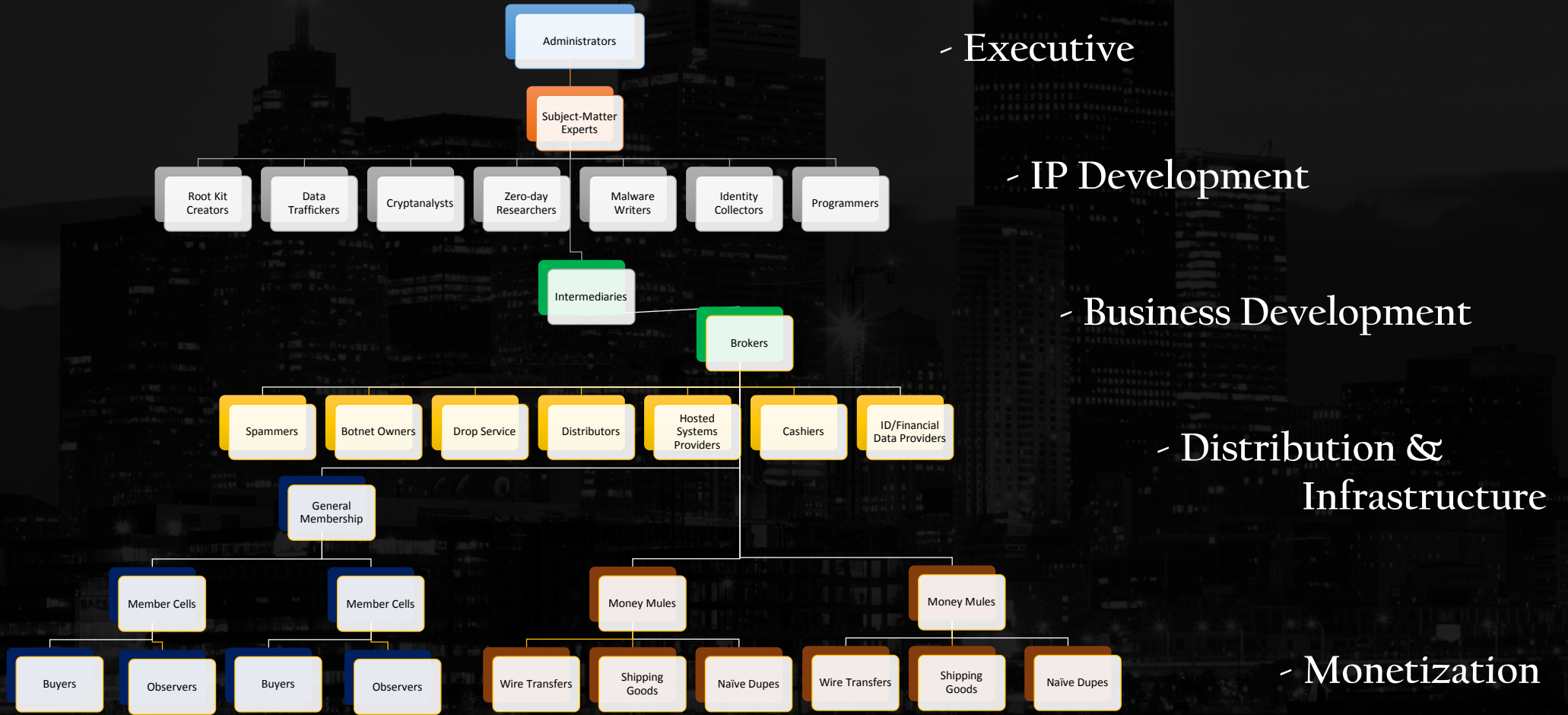


# MAPPING THE ORGANIZATION

**DARKNET**



# Black Market Organizational Structure







## DARK NET MARKET SIZE EXAMPLE



56,226  
465,222  
61,291



Members



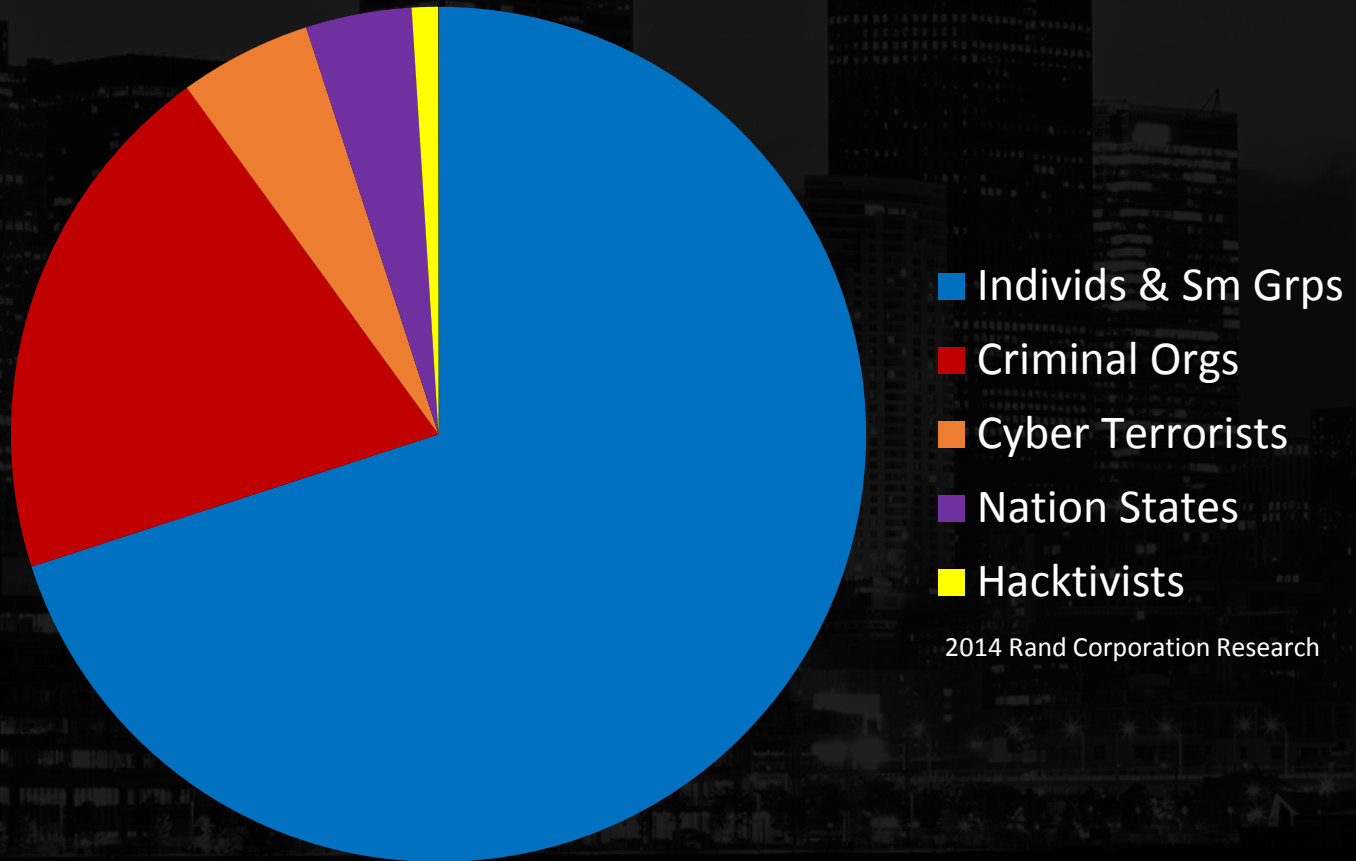
Messages



Discussions



## DARK NET ACTORS



2014 Rand Corporation Research



## Ransomware Attack

- Immediate impact to health and safety
- Aging IT infrastructure
- Limited IT resources
- Other IT resource allocation priorities
- Large aggregation of valuable data





## Mirai DDoS Attack

- IoT-based Distributed Denial of Service Attack
- Cameras, baby monitors, printers, routers...
- 1.2 terabits/second (largest attack in Internet history)
- Millions of users lost access to sites in US, Europe and around the world
- Lasted ~12 hours
- 14,000 internet domains dropped Dyn
- DDoS attacks have increased 7,900% in size since 2005
- Mirai code released into the wild



## APT Attack – Dridex

- Instructions to steal \$951M via SWIFT Network
- Five transactions worth \$101M succeeded, 30 transactions blocked
- Loss stopped by misspelling of transfer request, not security alerts
- \$81 Million loss



# ASYMETRIC INFORMATION

## SECURITY INSIDERS TEND TO DWELL ON WORST CASE SCENARIOS



- “Cyber-criminals’ annual profit exceeds \$1 trillion”<sup>1</sup>
- “Medical records sell for 50 times more on the dark web than stolen credit cards”<sup>2</sup>
- “Average cost per breach is \$221 per record”<sup>3</sup>

## Victims Under-report


- Fear of law suits
- Fear of reputational damage
- Response costs
- Law enforcement delays
- Loss data represents a competitive advantage

1. Edward Amaroso, AT&T CISO Testimony before congress, 2014
2. Numerous sources
3. Ponemon Cost of a Data Breach Study



# Emerging Risk





“We also know there are known unknowns; that is to say, we know there are some things we do not know.  
But there are also unknown unknowns – the ones we don't know we don't know.”

United States Secretary of Defense, Donald Rumsfeld  
Press Briefing, February 12, 2002





# Category 1~ Framing the Problem

- Things we don't know... but we're aware of it!
  - Emerging Risk as an "information gap"
  - Solutions:
    - Ask others
    - Fill in the data points, gaps



## Category 2~ Framing the Problem

- Things we don't know... and we're unaware of it!
  - Much more difficult
  - NOT merely an information gap that can be filled
  - Emergent nature presents specific challenges and limitations



# Category 2~ A Closer Look

(Things we don't know... and we're unaware of it!)

- Emerging risk~ “A novel manifestation of risk, of a type that has not been experienced before” (Locklear, 2011)
  - Pure- never experienced before, at all, by anyone
    - example: nanotechnology, fracking, genetically modified crops
  - Hybrid- blends together known risk types in new ways (combinations) to produce outcomes that haven't been experienced before
    - Example: Zoonotic disease + global warming = (zika?)
    - Example: Overstressed power grids + greater dependence on telecommunications + {X Factor} = ???



# Challenges of Emerging Risk

- 'Relational Complexity': Growing difficulty in determining relationships among causal factors, making risk more 'opaque'
  - Richardson, Cilliers & Lissack (2001)
    - Under these conditions, causes and effects no longer have simple, linear connections
    - It's more difficult to ascertain interactions between elements
    - Implication: Challenges for appropriately pricing and structuring insurance where "cause" (i.e.- "trigger, for insurance) is not always apparent





# Challenges of Emerging Risk

- Amplification/Cascade potential: Seemingly simple root causes can trigger events which cascade through a network and are amplified to produce an extreme event
  - Example: August 2003 mega-power outage
    - Ohio, Maryland, New York, Toronto
    - Overstressed lines failed in Ohio after contacting overgrown tree limbs (Holbrook, 2010)
    - Expected outcome was a minor, local outage
  - Implication: Appropriate pricing for insurance, as well as capacity, are challenged when a seemingly minor event is amplified



# Challenges of Emerging Risk

- Emerging risk is often opaque, clouded within a complex web of causal factors, until it escalates into an extreme event
  - In an environment of great complexity, emerging risk may remain “hidden” (latent)
  - Modern structures, like the “Internet of Things” provide rich environments for this period of latency
  - Implication: Insurance/risk management need to use different tools
    - Environmental scanning can help identify early “signals of change” (Ashley & Morrison, 1997) which if overlooked, ignored or downplayed, can allow emerging risk to continue along its development trajectory



# Challenges of Emerging Risk

- May involve rapid and widespread deployment of new/novel technology/modalities
- By the time an issue is identified, the problem is already extensive



# "Classic" Example of Emerging Risk

- Asbestos ("Emerged" risk)
  - Naturally occurring, used as far back as ancient Greece
  - Industrial revolution, insulator for furnaces
  - Subsequently used far and wide
  - Then problems grew apparent (1960's)
  - Extensive litigation, ongoing abatement problems
  - Classic illustration of unexpected impact for insurers
  - NOTE: Hind-sight is 20/20!







# Challenges of Emerging Risk

- Lack of historical data OR data that is not entirely relevant
  - The capabilities of traditional risk management tools (quantitative, predictive) are being stretched when applied to emerging risk
    - Traditional modeling does not “fit” the challenges of “unknown-unknowns”
    - Implications: In order to optimize approaches, including insurance, “non traditional” tools may be needed
      - Environmental scanning, systems thinking





## Our “Human” Challenges

- Tendency to focus within the “comfort zone”
  - Risks that are well known, well understood
  - Lots of data available for analysis
  - “Pure” risks that either happen, or don’t (e.g.- fire), with no up-side potential
- We tend to heavily value corroborating factual information and discount outliers, non-conforming information



# More “human” challenges

- Recent movie “Everest”
- Roberto, M. A. (2002). Lessons from Everest: The interaction of cognitive bias, psychological safety, and system complexity. *California Management Review*, 45(1), 136-158.



# "Human" challenges- Lessons from the movie 'Everest'

- **Commitment escalation-** continuing to invest resources, commitment to a course of action that increasingly appears questionable at best (Staw, 1987)
  - Led climbers to ignore rules and place themselves in increasing danger
- **Recency bias-** tendency to focus on more recent events
  - Hindered the judgment of the expedition leaders who had experienced good weather on Everest during the prior recent years, causing them to underestimate the severity of the storm despite historical data that showed the conditions on May 10, 1996 were anything but abnormal.



# More “human” challenges

- Groupthink

- Defective decision making that occurs when conformity pressures of a group lead to faulty decisions, made in an effort to preserve group harmony.

- Defective ‘groupthink’ decision making is characterized by the following attributes: poor information searching; selective bias in information processing; incomplete surveying of objectives and alternatives; failure to re-examine choices and rejected alternatives; and failure to develop contingency plans (Janis & Manning, 1977, p. 132).

- “a disease of insufficient search for information, alternatives and modes of failure” (McCauley, 1998, p. 144)



# Something to Consider: Lessons from the Black Swan (Taleb, 2007)

- Extreme outlier (unpredictable)
- Thought not to exist (improbable)
- Outside the boundaries of “normal” expectations
- It can't be... therefore it isn't



# Some Cyber Losses

Breach	Cause	Cost (Ground Up)	Cost (Insured)
Epsilon	Spear-Phishing <sup>i</sup>	Up to \$4 billion <sup>ii</sup>	No coverage in place
Home Depot	Vendor Cybersecurity Failure and Microsoft Windows security failure	\$ billions <sup>iii</sup>	\$100 million
Wendy's	Unknown	\$ billions <sup>iv</sup>	Unknown
Veterans Administration	Computer/ External Hard Drive incidentally stolen from employees house during burglary <sup>v</sup>	\$500 million <sup>iii</sup>	No coverage in place
Target	Vendor Cybersecurity Failure	\$252 million <sup>vi</sup>	\$90 million
Hannaford Bros	Malware	\$252 million <sup>vii</sup> ; ID theft insurance and replacement card costs held compensable <sup>viii</sup>	No coverage in place
Sony Playstation	Unknown	\$171 million <sup>vii</sup>	Unknown; settlement when appeal pending after bench granted summary judgment against Sony <sup>ix</sup>
TJ Maxx	Poorly Secured Wireless LAN in two stores <sup>x</sup>	\$256 million <sup>xi</sup>	\$19 million <sup>xii</sup>
Sony Pictures Entertainment	North Korea	\$151 million + reputation	\$151 million
Heartland Payment Systems	SQL Injection attack <sup>xiii</sup>	\$140 million <sup>vi</sup>	\$30 million <sup>xiv</sup>
Anthem	Bogus Domain Name/ Phishing	Over \$100 million <sup>vi</sup>	\$100 million <sup>xv</sup>



# Evaluating Coverage- Current Practice and Thinking

- Pricing
- Profitable

Group/ Company	Direct Premiums Earned (\$000)	Loss LAE Ratio	Frequency per \$1000 Earned Premium
XL Group Ltd (SNL P&C Group)	\$ 90,022	115.2%	1.4%
Beazley Insurance Co.	\$ 30,812	8.4%	16.1%
Chubb Ltd. (SNL P&C Group)	\$ 34,050	32.2%	5.7%
Travelers Companies Inc. (SNL P&C Group)	\$ 33,632	53.0%	16.3%
Zurich Insurance Group (SNL P&C Group)	\$ 24,152	163.0%	1.6%
AXIS Capital Holdings Ltd. (SNL P&C Group)	\$ 20,966	4.2%	4.8%
American International Group (SNL P&C Group)	\$ 17,881	53.0%	9.0%
Allied World Assurance Co. (SNL P&C Group)	\$ 15,199	61.9%	6.0%
Tokio Marine Group (SNL P&C Group)	\$ 13,172	34.1%	0.0%
Fosun International Hldgs Ltd. (SNL P&C Group)	\$ 12,555	111.6%	2.4%
Alleghany Corp. (SNL P&C Group)	\$ 11,849	42.4%	7.3%
CNA Financial Corp. (SNL P&C Group)	\$ 11,429	80.1%	15.0%
Endurance Specialty Holdings (SNL P&C Group)	\$ 10,252	60.2%	1.4%
<b>Grand Total</b>	<b>\$373,742</b>	<b>65.2%</b>	<b>15.6%</b>

Data as of 12/31/15. Will update for year-end when data available





# Evaluating Coverage- Current Practice and Thinking

- Terms/Conditions
  - SIRs/ Deductibles
  - Limits
  - Scope of Cover
  - Covered Events
  - Coverage Triggers



# Typical Sublimits (cont)

- Aggregate (\$1M lowest = \$100,000)
- Information Security & Privacy
- Regulatory Defense and Penalties
- Website Media Content Liability
- PCI Fines and Costs
- Cyber Extortion Loss
- Data Protection Loss
- Legal & Forensic Expenses
- Crises Management & Public Relations
- Business Interruption (where offered)



# HSB CyberOne

- \$100,000 limit/\$10,000 deductible or \$50,000 limit/\$5,000 deductible –
- Three of the coverages are subject to sublimits: .
  - Data Recreation: \$5,000 .
  - Business Income: \$10,000 .
  - Public relations: \$5,000



# Possible Mandatory Safety Measures

- Patch Updates sent centrally
- Compulsory and Documented Employee training
- Sub-contractor certificates



# Some Random Rating Factors

- Insured acquired or plans to acquire another entity exceeding 10% of annual revenue:
- CFO > 3 years
- Insured does not have privacy policy
- Members of Control Group turnover
- Insured stores information for a longer duration than necessary
- Insured primarily operates in rural or other low density populated geographic locations
- Website content is informative, controversial or sensitive in nature
- Income stability is closely tied to public opinion
- Revenue from payment card transactions is less than 50% of gross revenue





# Frequency

- Typically Claims-Made Coverage
- But exposure constantly changing



# Severity

- Not yet enough data to model loss distribution
- Exacerbated at tail
- If above insurance limits, may never be fully qualified
- Can use other countries/ coverages as guide for certain aspects e.g. Regulatory penalties; reputation risk; business interruption



# Frequency x Severity

- Frequency/ Severity methods are therefore currently superior than other methods
- Frequency data can be taken from prior experience/ industry studies
- Severity data can be augmented with other data sources
- However, can have “Catastrophic Frequency”





# TRIA & Cyber

- Definitely Included in Terrorism Risk Insurance Program as of December 27, 2017
- Insureds are eligible if they have purchased insurance
- Covers Stand-alone Cyber Policies
- Specifically excludes Professional Liability & Omissions policies. So if a technology company relies on PLO, TRIA won't cover them.
- Other insurance policies are in grey area - so standalone better than endorsement to existing policy
- Wouldn't cover other malicious actors
- How do you prove who & why with cyber attack?





# CONCEPTUALIZING EMERGING CYBER RISK

- CYBER COPE™ FRAMEWORK
- "FOOD FOR THOUGHT"
- SCADA
- HACKING OF MEDICAL DEVICES
- HACKING OF DRIVERLESS CARS



# COPE- APPLICATION TO CYBER

- COPE- construction, occupancy, protection, exposures
  - Each category represents a set of data points
  - Used to evaluate combined property risk for a structure/building

COPE applied to cyber/technology to create Cyber COPE™  
(Cohen, 2016)



# Summary of COPE to Cyber-COPE™

COPE	CYBER COPE™	MEASUREMENT TYPE	SAMPLE DATA ELEMENTS
CONSTRUCTION	COMPONENTS	OBJECTIVE	NUMBER OF ENDPOINTS, NETWORK CONNECTIONS, SOFTWARE VERSIONS, DATA CENTER LOCATIONS
OCCUPANCY	ORGANIZATION	OBJECTIVE	POLICY HOLDER'S INDUSTRY, QUALITY OF IT/SECURITY RELATED POLICIES, USE OF INDUSTRY STANDARDS

Retrieved October 27, 2016 at <https://www2.chubb.com/us-en/business-insurance/transforming-cyber-underwriting.aspx>.



# Summary of COPE to Cyber-COPE™

COPE	CYBER COPE™	MEASUREMENT TYPE	SAMPLE DATA ELEMENTS
PROTECTION	PROTECTION	SUBJECTIVE	DATA RETENTION POLICIES, FIREWALLS, MONITORING, INCIDENT RESPONSE/READINESS POLICIES
EXPOSURES	EXPOSURES	SUBJECTIVE	POLITICAL OR CRIMINAL MOTIVATION, TYPES OF OUTSOURCING, TYPE/AMOUNT OF SENSITIVE INFORMATION

Retrieved October 27, 2016 at <https://www2.chubb.com/us-en/business-insurance/transforming-cyber-underwriting.aspx>.





## Hacking in action- Use of smart phones

- Max Cornelisse, Netherlands
  - hacking train schedule board
  - turning building lights on/off
  - raising/lowering drawbridge
  - changing digital highway road sign
- Videos available on YouTube
- Real, not real?



# SCADA

- Supervisor Control and Data Acquisition
  - Refers to industrial control systems (ICS)
    - Computer systems that monitor and control industrial, infrastructure or facility-based processes
    - System collects data from various sensors at factory, plant or other remote locations
    - Sends data to central computer that manages and controls the data



# Possible SCADA Hacking Scenarios

- Power outages (blackouts, across grids)
- Waste water mixed with drinking water
- Disruption of manufacturing lines
- Transportation disruption/shut down
  
- **NOTEWORTHY**
  - Potential for impact far away from the compromised source itself
  - Amplification of impact
  - Cascade effect





# Actual SCADA Incidents

- Thirteen assembly lines shut down at Daimler-Chrysler, Zotob worm, 2005
- Springfield, Illinois public water supply pump burned out after being cycled on and off repeatedly (November 2011) through an IP address in Russia



# Actual SCADA Incidents

- Ohio Davis-Besse nuclear power plant safety monitoring system off line for 5 hours, January 2003, Slammer worm
- Brisbane hacker used radio transmissions to create raw sewage overflows on Sunshine coast (2000)
- CSX Transportation computers infected by virus (August 2003) halting train traffic in Washington, D.C.



# Emerging threats to critical infrastructure

- A computer virus attacked a turbine control system at a U.S. power plant
  - A third party technician had unknowingly used an infected USB drive on the network
  - Plant was down for three weeks



# Insulin Pump Hacking

- “J&J Warns Insulin Pump Vulnerable to Cyber Hacking”  
- October 4, 2016, Wall Street Journal
- OneTouch Ping uses unencrypted radio signal
- Hacker in close proximity could use equipment to detect signal and program the device



# Driverless Car Technology

- Apps to unlock doors, start cars
  - “Now is the transitional period, and it’s kind of ugly. They’re old-school industries. They were mechanic or electronic kinds of systems, and now they’re software-based companies—and they haven’t realized they’re software-based companies, and that’s sort of the problem.”
    - [Craig Smith, founder of Open Garages](http://www.vocativ.com/332734/driverless-car-hack/) <http://www.vocativ.com/332734/driverless-car-hack/> (June 29, 2016)
  - DECISION ALGORITHM TO AVOID CRASHES
    - SACRIFICE DRIVER TO SAVE GROUPS OF PEOPLE





# Stuxnet



Natanz Nuclear Complex

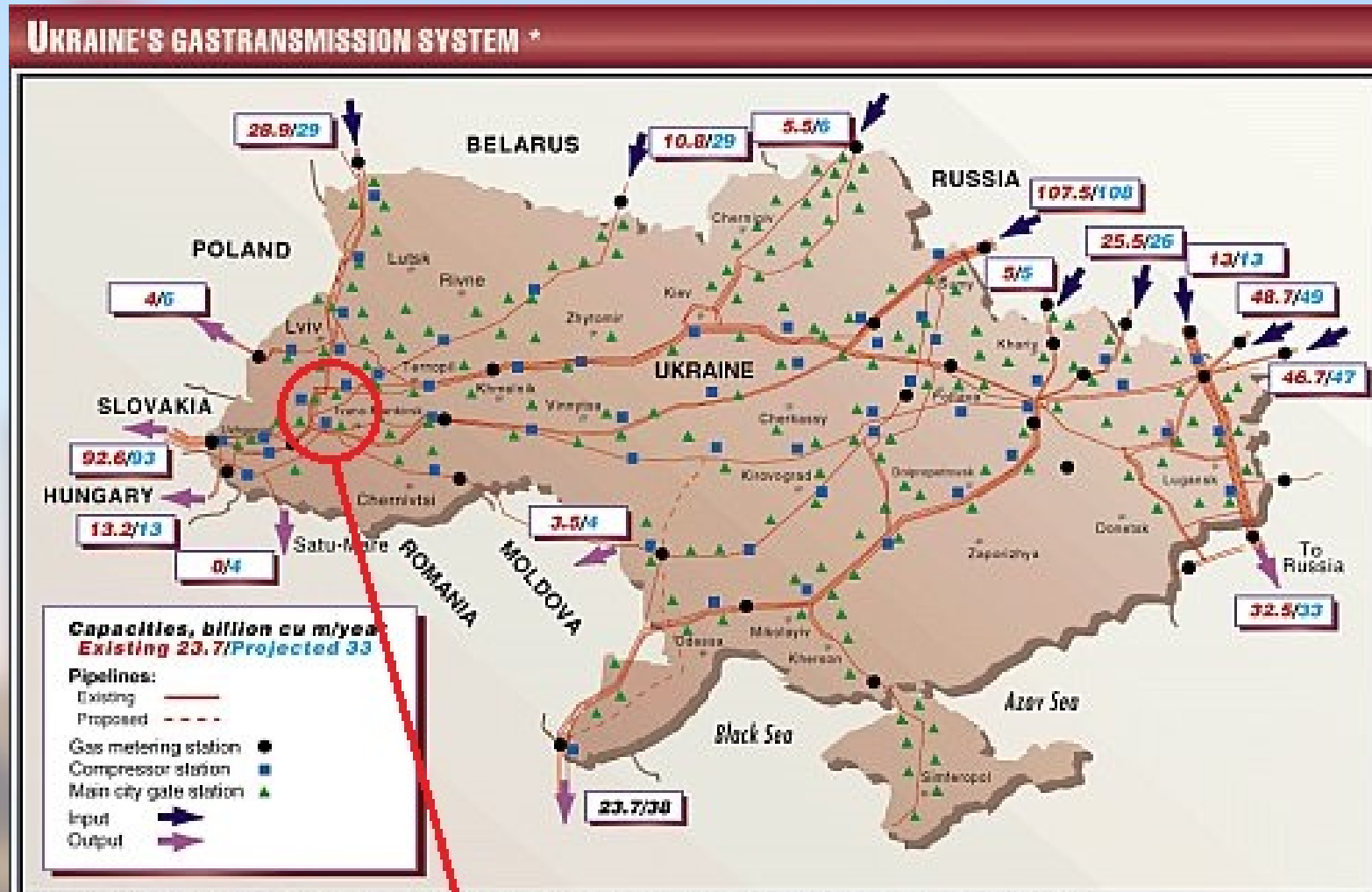


# Property Damage (not Ransomware)



German Steel

# Ukraine's Power Grid (twice!)



\*Projected figures are estimates. Map does not show facilities such as underground storage, production, and gas processing plants.

Location of power system outage



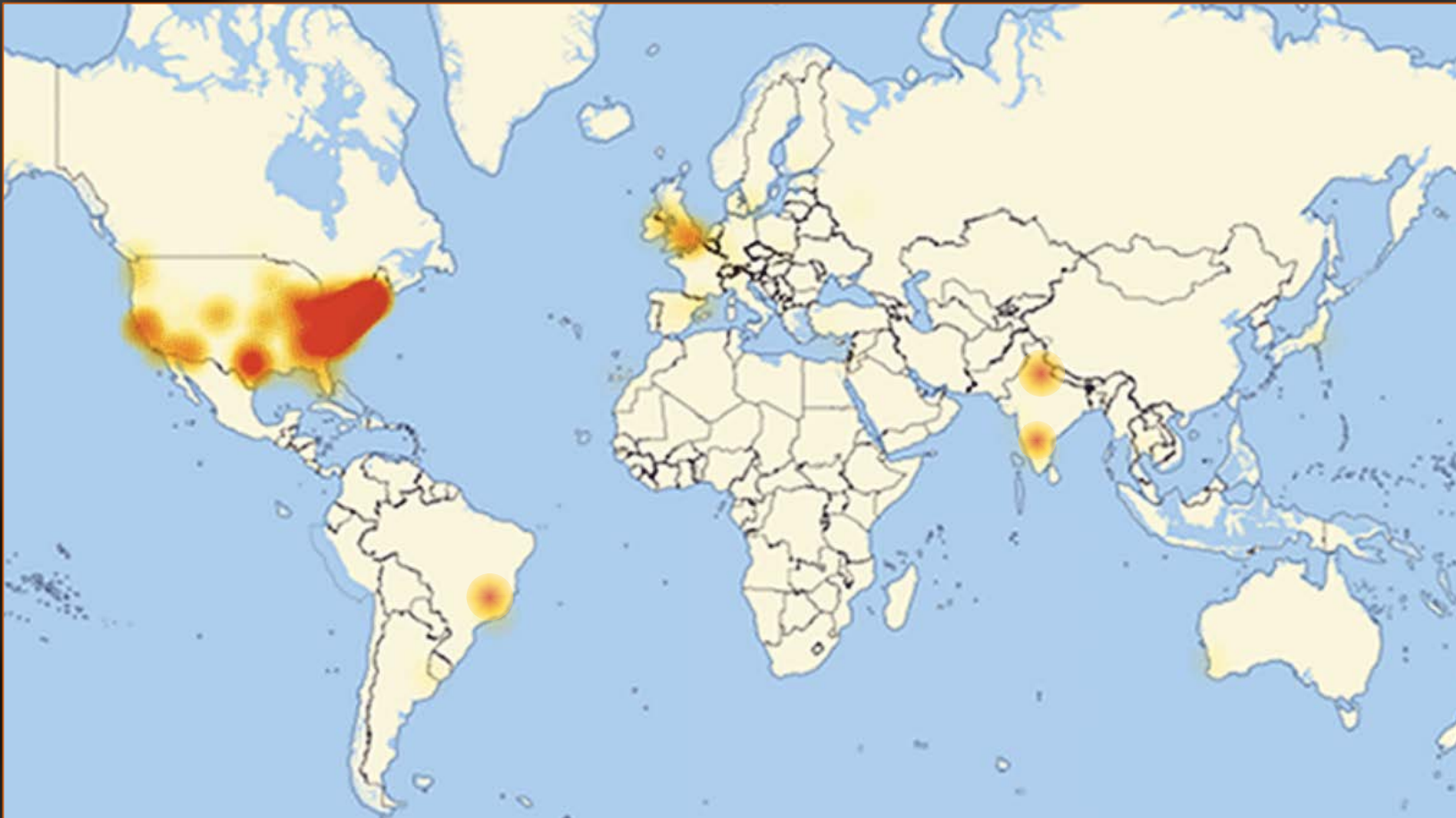


# Wall Street – Nation State actors





## INTERNET OF THINGS WEAPONIZED



TECHNOLOGY

# Hackers Used New Weapons to Disrupt Major Websites Across U.S.

**THE VERGE** TECH SCIENCE CULTURE CARS REVIEWS LONGFORM VIDEO MORE

REPORT TECH CYBERSECURITY

## The internet apocalypse map hides the major vulnerability that created it

*Where's the infrastructure?*

by Ingrid Burrington | Oct 24, 2016, 10:10am EDT

Blue Sky Innovation / Blue Sky Originals

## Another internet outage takes down services in U.S. and U.K.

Opinion / Editorial

## Editorial The massive U.S. Internet outage demonstrates the dumb power of smart devices

## 3rd Cyberattack 'Has Been Resolved' After Hours of Major Outages: Company

The company at the heart of the attack told CNBC it was hit by "tens of millions of IP addresses" Friday afternoon

## This Is Why Half the Internet Shut Down Today