Mitigating DNS or Domain Name Threats:
A View from Ground Zero

Dave Piscitello
VP Security and ICT Coordination
January 2016
dave.piscitello@icann.org

Agenda

- Online Crime Landscape
- Myths and Realities
- How we conduct investigations today
- Evolution of trust-based collaboration

Introduction

- VP Security and ICT Coordination, ICANN
- 40 year network and security practitioner
- Roles at ICANN:
  - Technology Advisor
  - Threat responder
  - Investigator
  - Researcher

Setting Context…

Chronology of a typical attack

User receives spam with malicious attachment

Malicious attachment self-installs, connects to criminal host to download malware installer

Malware installer downloads attack-specific malware

Attacks ensue:

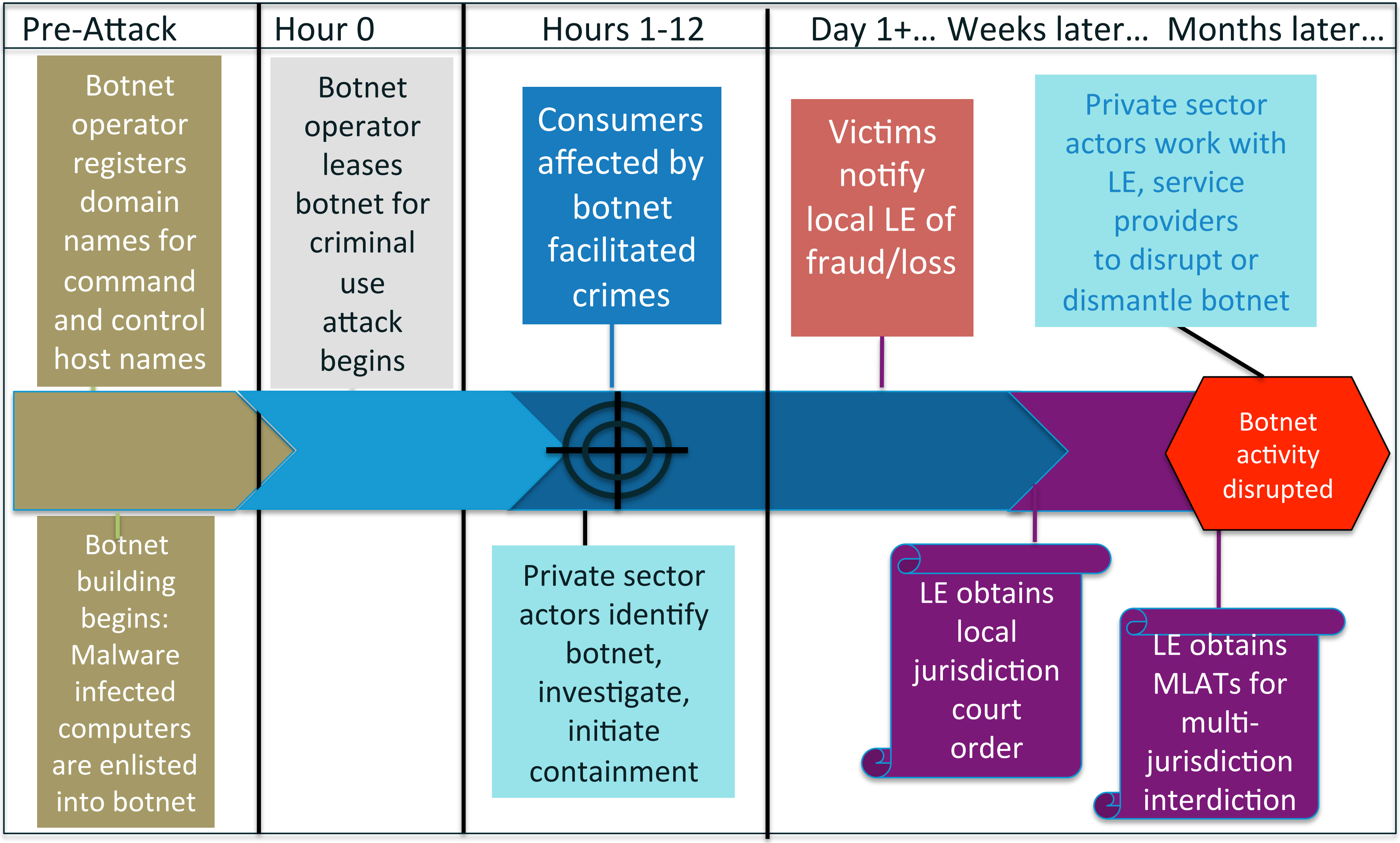
Phishing

Data Theft

Ransomware

Account theft…

Attackers operate at Internet pace: Botnets



Pre-Attack

Botnet operator registers domain names for command and control host names

Botnet building begins: Malware infected computers are enlisted into botnet

Hour 0

Botnet operator leases botnet for criminal use attack begins

Hours 1-12

Consumers affected by botnet facilitated crimes

Private sector actors identify botnet, investigate, initiate containment

Day 1+… Weeks later… Months later…

Victims notify local LE of fraud/loss

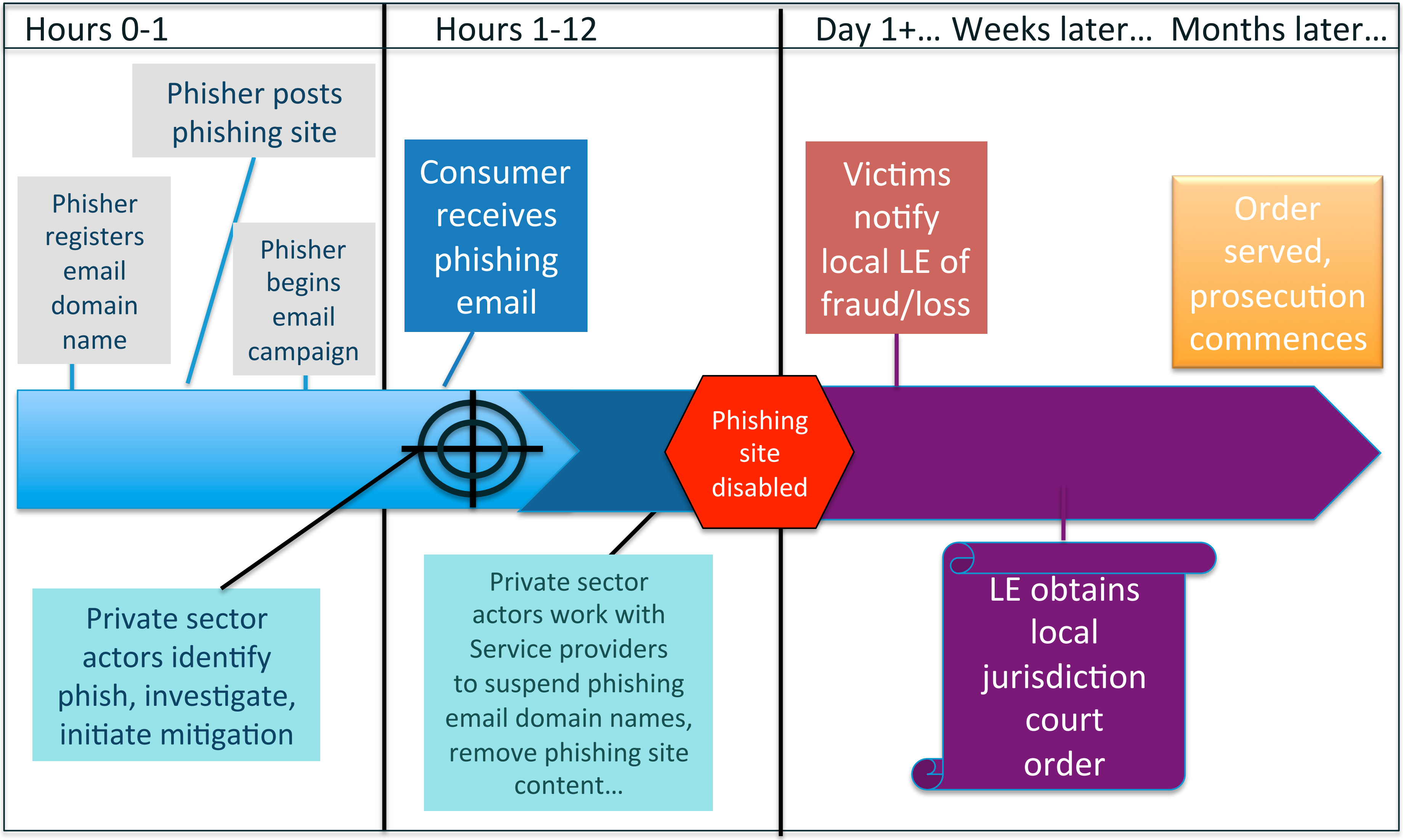
Private sector actors work with LE, service providers to disrupt or dismantle botnet

LE obtains local jurisdiction court order

LE obtains MLATs for multi-jurisdiction interdiction

Botnet activity disrupted

Attackers operate at Internet pace: Phishing



Hours 0-1	Hours 1-12	Day 1+... Weeks later... Months later...

Phisher registers email domain name

Phisher posts phishing site

Phisher begins email campaign

Consumer receives phishing email

Phishing site disabled

Victims notify local LE of fraud/loss

Order served, prosecution commences

Private sector actors identify phish, investigate, initiate mitigation

Private sector actors work with Service providers to suspend phishing email domain names, remove phishing site content…

LE obtains local jurisdiction court order

Debunking popular myth…

Attackers aren't *smarter* than responders.

They *are* able to

move faster than responders,

more economically, and

act unencumbered by

law, jurisdiction, contract, interpretation.

The advantages are staked in favor of attackers

Attackers create *their own* attack infrastructure on infected or compromised devices or servers

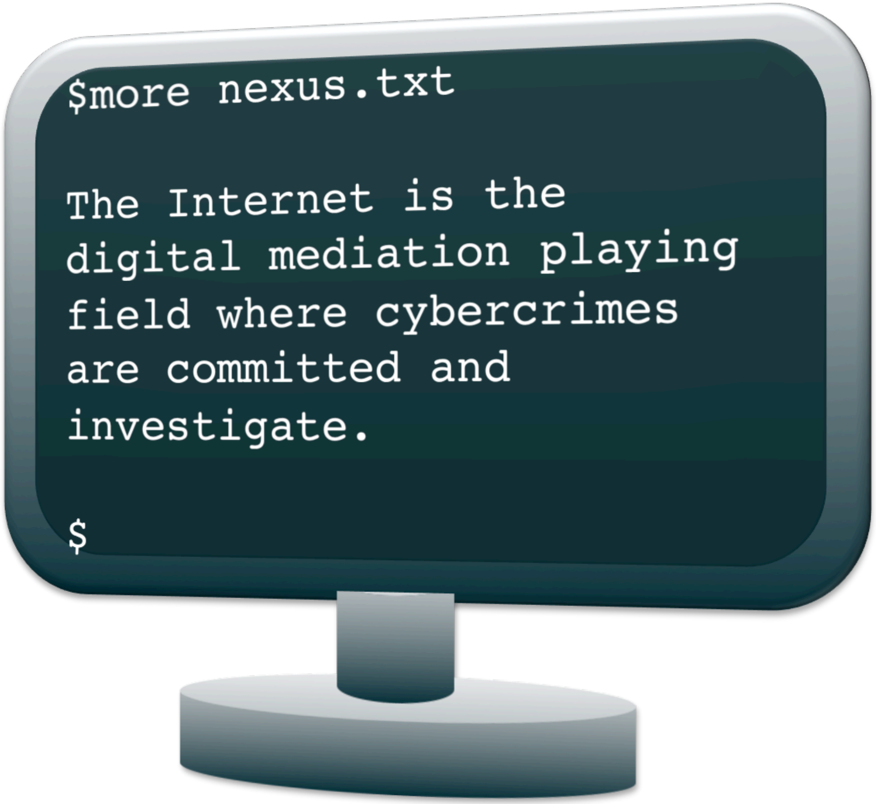
Attackers compromise legitimate infrastructures to operate covertly or to encumber investigations

Attackers don’t need approval, permission, budgets, licenses, or court orders

Do Responders Have Any Advantages?

Yes…

Criminals must use the same hosts, networks address spaces, and same name resolution to reach and victimize users



```
$more nexus.txt

The Internet is the
digital mediation playing
field where cybercrimes
are committed and
investigate.

$
```

Investigators can see what targeted users see

- We can
  - Monitor, intercept or redirect traffic
  - Reverse engineer malicious code
  - Block addresses or services
  - Remove harmful content
  - Disconnect hosts
  - Suspend name resolution
- Such interventions are common
- Mitigation or prosecution is less so…

What Hinders Mitigation or Prosecution?

JURISDICTION	What is the prevailing jurisdiction of content hosting, DNS hosting, domain registration, alleged perpetrators?
LAW	Is this a criminal activity in all relevant jurisdictions?
CONTRACT, INTERPRETATION	Is a contracted party in breach of an obligation? According to whose interpretation?

Intervention Today: Trust-based Collaboration

- Private- and public sector investigators cooperate 24x7 using trusted communications channels
- Information sharing
  - Malware, phishing, spam samples
  - Host names, URLs, addresses, geo-location
  - Activities of persons of interest (e.g., social media posts)
  - Points of contact (targets, victims, operators, investigators)
- Coordination or hand off
  - Mitigating DDoS by squelching sources
  - Providing evidence of AUP violation to operator for action

Trust is Earned

- New participants earn nominations from existing members and are vetted prior to admission
  - Personal references,
  - Prior collaboration and
  - Reputation
- Individuals put own reputation and membership at risk when they nominate
- Strict codes of conduct
- Self-policing model

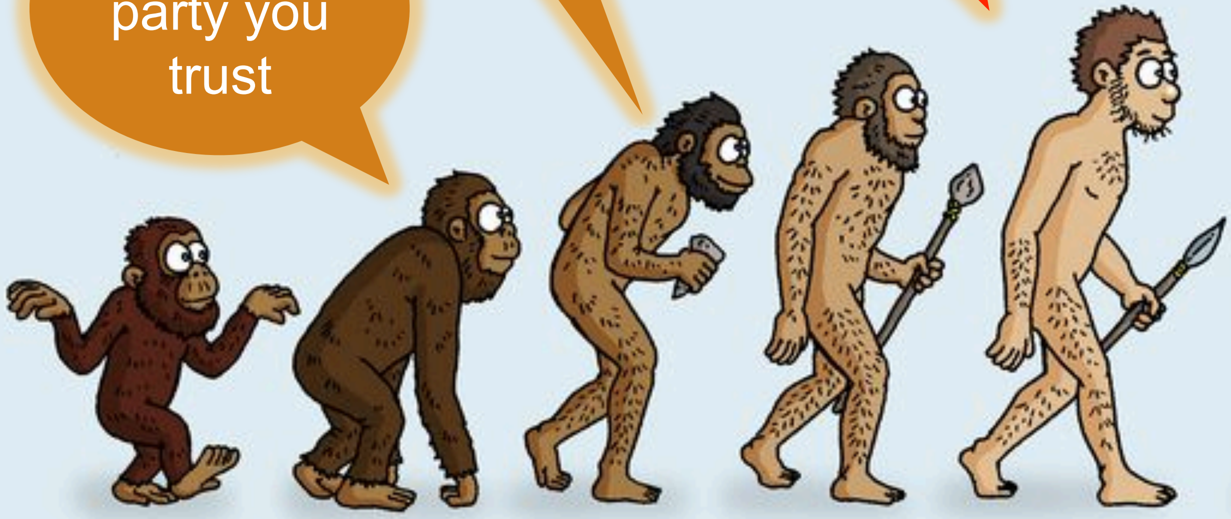
Is trust-based collaboration effective?

Yes. It reduces the attack surface in several ways:

- Sharing "data feeds" forms the bases for blocklisting
- Sharing malware samples expedites remediation
- Sharing intelligence improves dossiers on suspected criminal actors
- Reduces time from threat identification to containment or mitigation
- Gives participating law enforcement agents insights other than direct complaints

BUT… it scales poorly and is not a "universal" solution

Evolution of trust: Trusted intervener programs



Call a party you trust

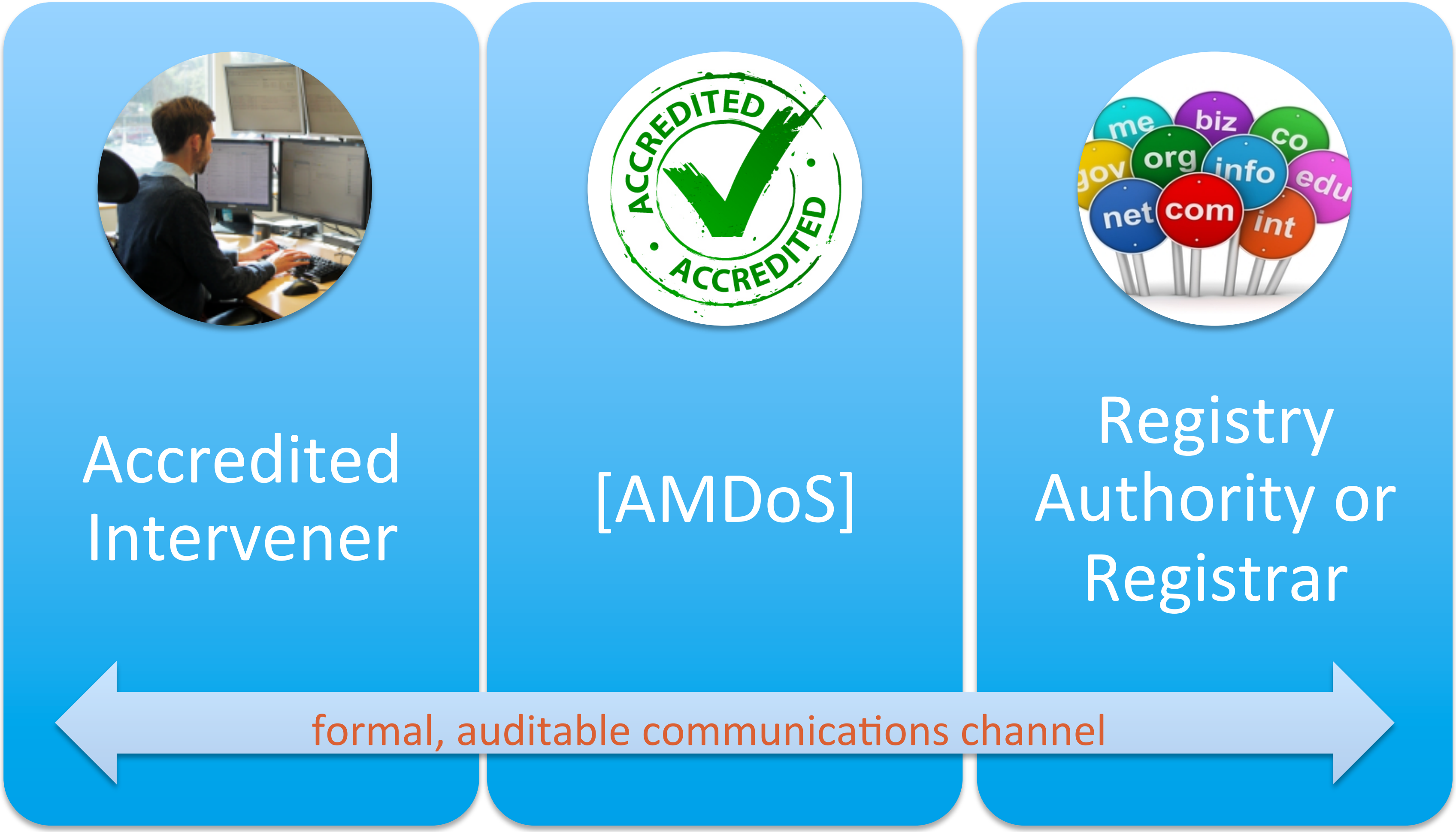
Trust based collaboration community

Trusted Intervener programs

Use trusted third party intermediary programs to allow responders to keep pace with criminal actors

2011 by Steve Kaplan

Trusted Intervener Systems (e.g. APWG AMDoS)



Accredited Intervener

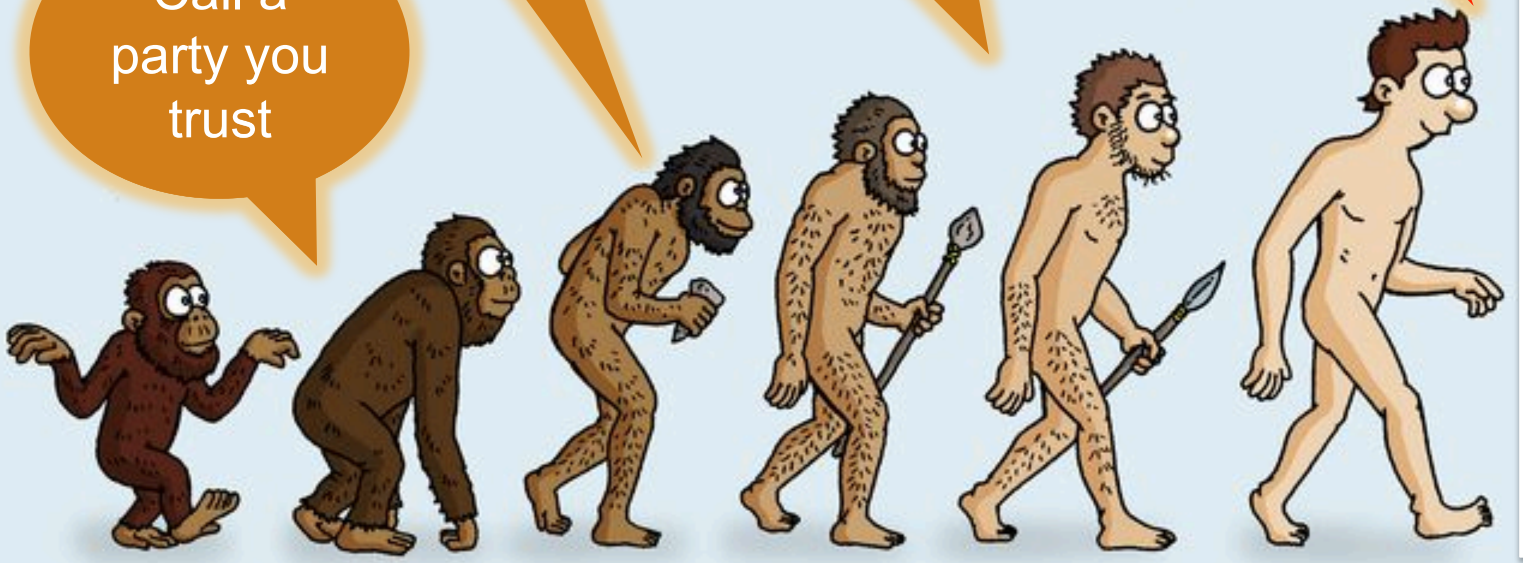
[AMDoS]

Registry Authority or Registrar

formal, auditable communications channel

The concept or framework could be applied to other realms.
Transparent, accountable vetting process for interveners

Evolution of trust: Trusted intervener programs



Call a party you trust

Trust based collaboration community

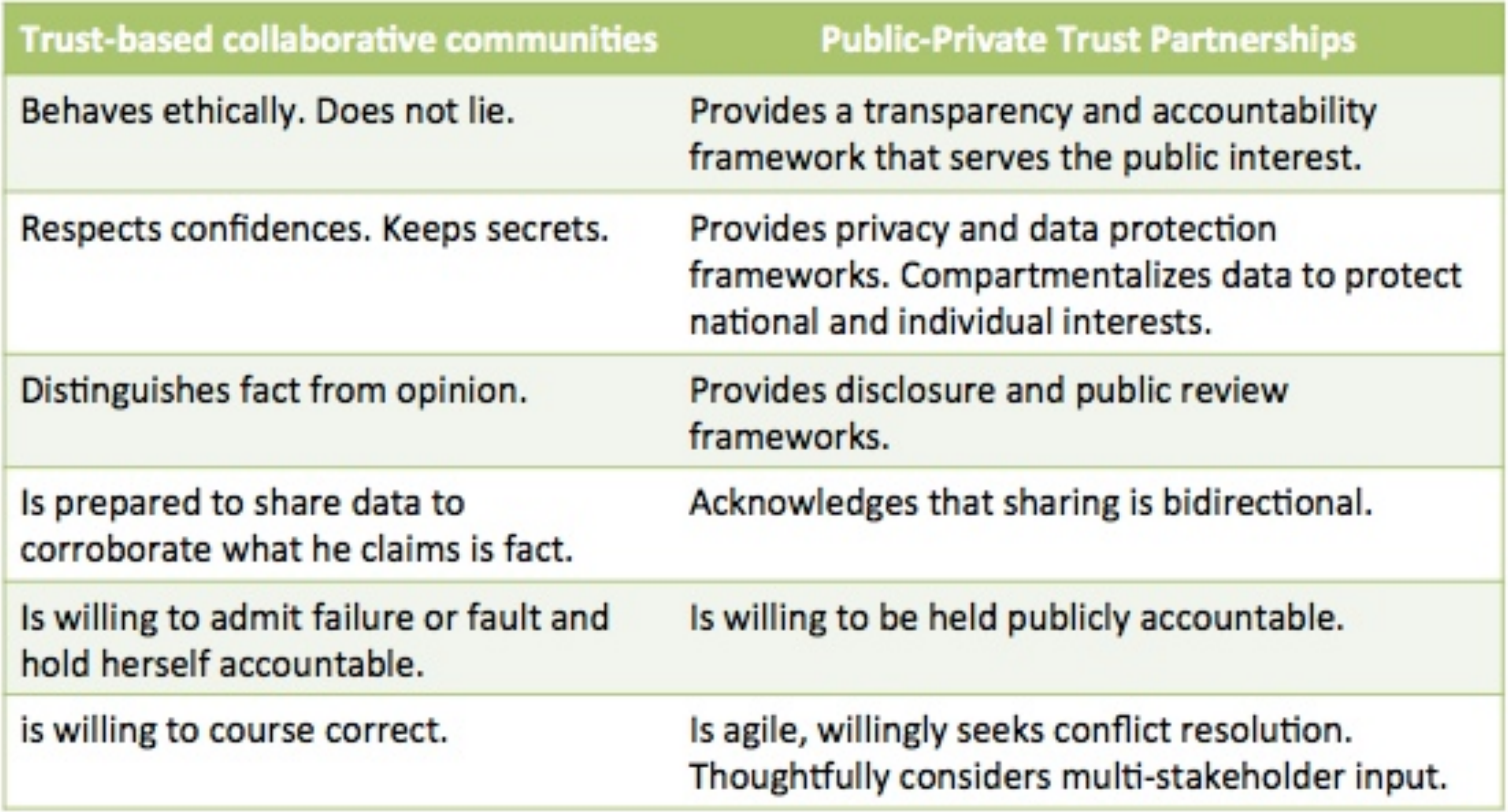
Trusted Intervener programs

Public private trust parthерships

Take trusted intervener programs to next level

2011 by Steve Kaplan

Challenges for formal Public-Private Partnerships

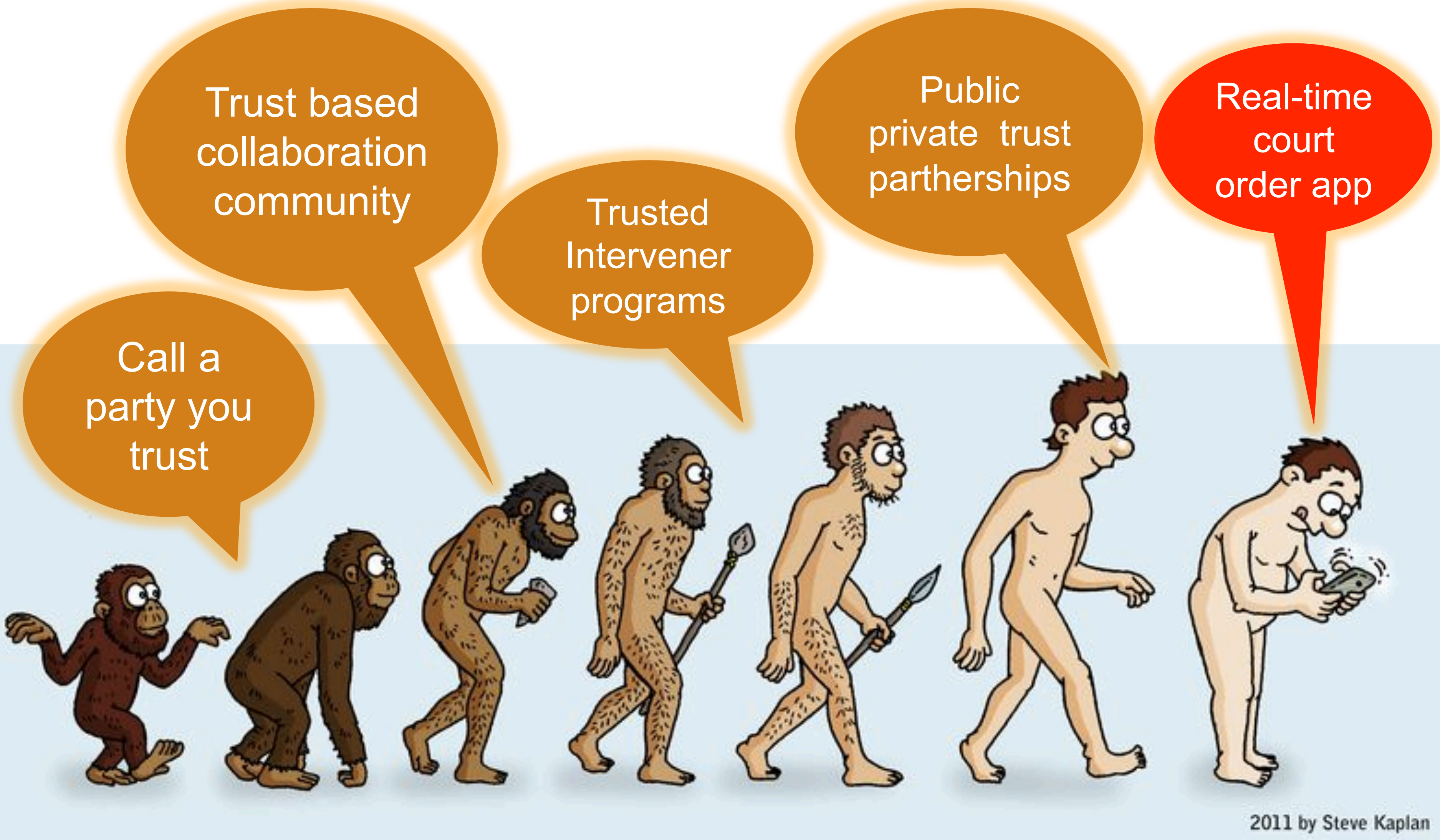


Trust-based collaborative communities	Public-Private Trust Partnerships
Behaves ethically. Does not lie.	Provides a transparency and accountability framework that serves the public interest.
Respects confidences. Keeps secrets.	Provides privacy and data protection frameworks. Compartmentalizes data to protect national and individual interests.
Distinguishes fact from opinion.	Provides disclosure and public review frameworks.
Is prepared to share data to corroborate what he claims is fact.	Acknowledges that sharing is bidirectional.
Is willing to admit failure or fault and hold herself accountable.	Is willing to be held publicly accountable.
is willing to course correct.	Is agile, willingly seeks conflict resolution. Thoughtfully considers multi-stakeholder input.

Formalizing intervener programs takes us only so far…

We still need to accelerate due process to Internet pace

Evolution of trust: an intervener's wish list



Call a party you trust

Trust based collaboration community

Trusted Intervener programs

Public private trust parthership

Real-time court order app

2011 by Steve Kaplan

ICANN

dave.piscitello@icann.org
@securityskeptic
www.securityskeptic.com
about.me/davepiscitello