# Distributed Denial of Service Defense (DDoSD)

## Industry Day Briefing

**26 June 2014**

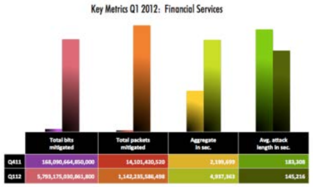
**Dr. Dan Massey**
Program Manager
Cyber Security Division
Science and Technology Directorate

Homeland Security

Science and Technology

# DDoSD Overview

Distributed Denial of Service attacks render key systems and resources unavailable, effectively denying users access to the service



| | Total bits mitigated | Total packets mitigated | Aggregate in sec. | Avg. attack length in sec. |
|---|---|---|---|---|
| Q411 | 168,090,664,850,000 | 14,101,420,520 | 2,199,699 | 183,308 |
| Q112 | 5,793,175,030,861,800 | 1,142,235,586,498 | 4,937,363 | 145,216 |

***USA Today:*** *Why DDoS attacks continue to bedevil financial firms … adversaries may potentially be nation states …*

***The Guardian:*** *Justice for the PayPal WikiLeaks protesters: why DDoS is free speech*

***NY Times:*** *Attacks used the internet against itself to clog traffic Attack traffic exceeds 400 Gbps!*

***eWeek:*** *DHS, FBI Warn of Denial-of-Service Attacks on Emergency Telephone Systems*

***Current Advantage Favors Attackers:***

- *Attack resources are cheap compromised machines while defense requires provisioning*
- *Attackers easily cross boundaries while defense requires cross-organization collaboration*
- *Attack can target many system elements while defense must protect all elements*

**Challenge is to shift advantage in DDoS events toward defense**

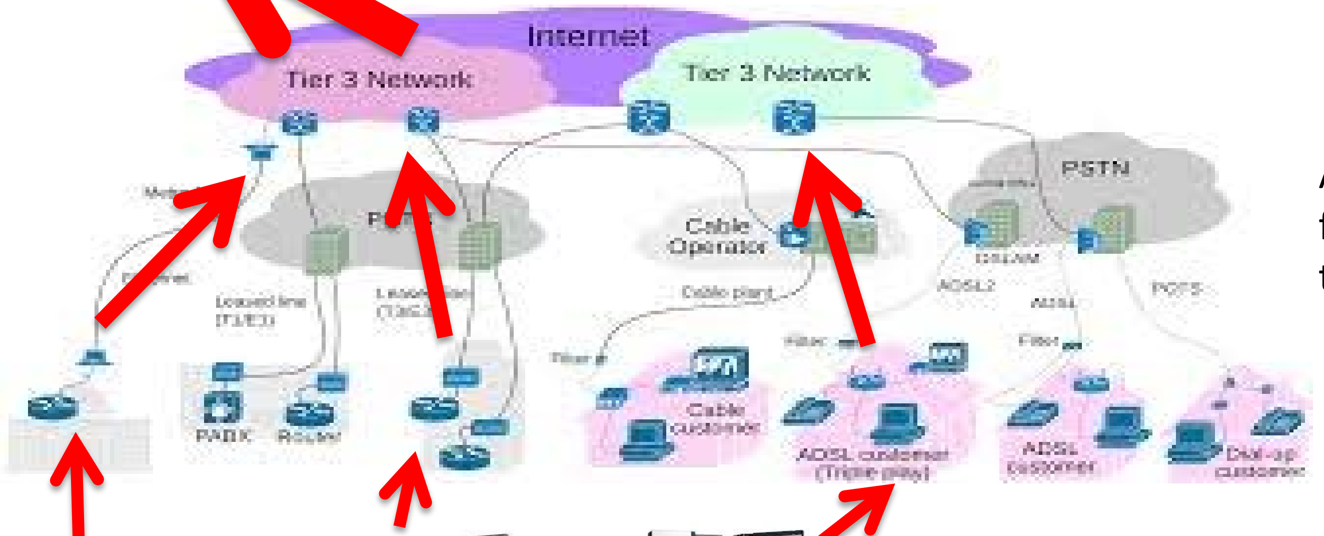
Source: http://arstechnica.com/business/2012/04/bad-bots-ddos-attacks-spike-in-first-quarter-outdoing-all-of-2011/

# Problem: DDoS Attacks 101

HELLO
I'm a
VICTIM

Victim is overwhelmed.   Examples include:
- 400 Gbps traffic to 10 Gbps access link
- Millions of requests to server designed for thousands
- Thousands of 911 calls to a system designed for hundreds

Both brute force and clever ways to overwhelm the target



Attack traffic originated from multiple locations throughout the Internet

Control Over Vast Number of Compromised Devices:
Desktops, laptops, and even refrigerators!
http://thehackernews.com/2014/01/100000-refrigerators-and-other-home.html

Command and Control:
Nation State, Criminal Organization,
Hactivist groups, etc.

Homeland Security
Science and Technology

# Problem: Advantage Favors Attacks

Resources Costs Favor Attackers

- Attacks use large numbers of machines (millions) and send vast amounts of traffics (400 Gbps)
- Defense relies on marshaling more powerful systems that withstand attacks
- Attacker does not pay for computation or bandwidth while defenders purchase and deploy systems
- Known best practices can mitigate attacks but require multi-organizational actions and lack leadership

The ZeroAccess botnet, which is likely to have more than 1.9 million slave computers at its disposal.
http://news.cnet.com/8301-1009_3-57605411-83/symantec-takes-on-one-of-largest-botnets-in-history/

Distributed Nature Favor Attackers

- Attacks use large numbers of systems, ***ignoring multiple organizational policies***
- Filtering at victim requires resources that can be overwhelmed by distributed attacks
- Lack of tools, collaboration mechanisms, and ***requirement to respect multiple polices*** make cross organization response difficult

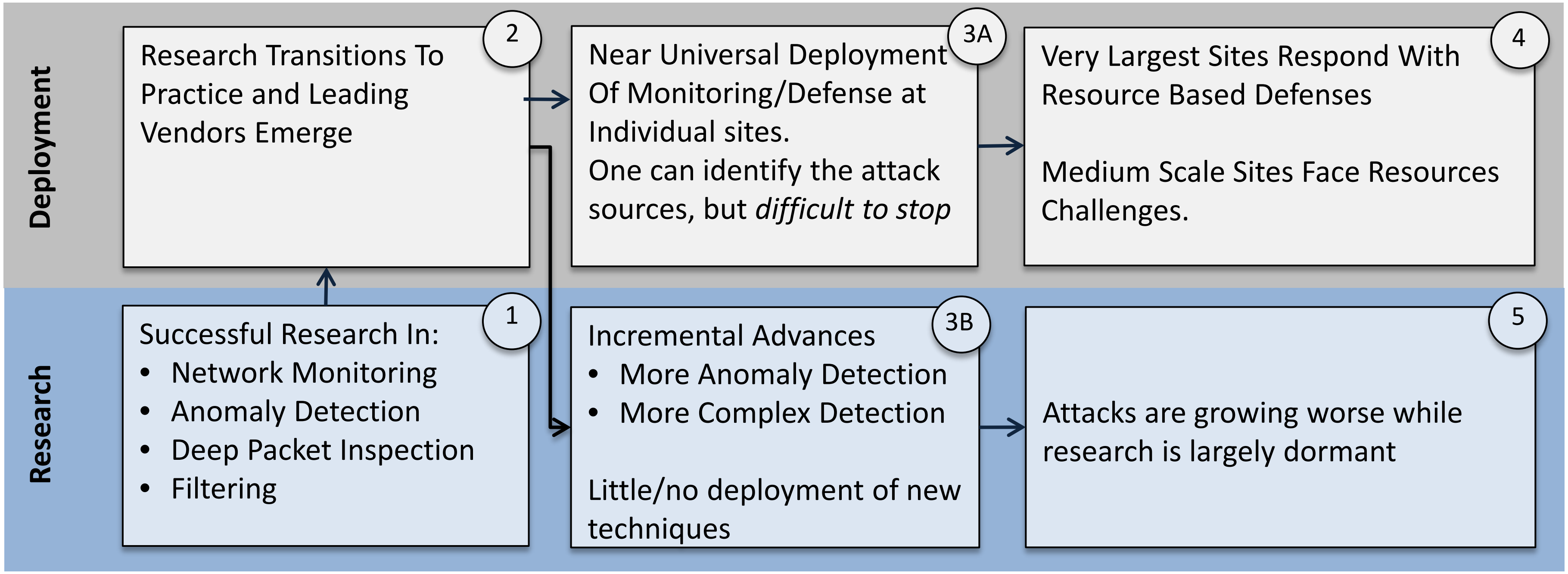
The criminals that are actively controlling botnets must ensure that their C&C infrastructure is sufficiently robust to manage tens-of-thousands of globally scattered bot agents, as well as resist attempts to hijack or shutdown the botnet. Botnet operators have consequently developed a range of technologies and tactics to protect their C&C investment. https://www.damballa.com/downloads/r_pubs/WP_Botnet_Communications_Primer.pdf

Increased demand and new applications provide attackers with a target rich environment

- Attacks can succeed by disabling any key element, and defense must protect all elements
- Attacks will exploit future trends in mobile devices, emergency response systems, sensors, and so forth.

  http://www.eweek.com/security/dhs-fbi-warn-of-denial-of-service-attacks-on-emergency-telephone-systems/
- Defense is almost entirely reactive with little proactive research on next targets

# Status Quo: DDoS Today



Deployment

2 Research Transitions To Practice and Leading Vendors Emerge

3A Near Universal Deployment Of Monitoring/Defense at Individual sites.
One can identify the attack sources, but *difficult to stop*

4 Very Largest Sites Respond With Resource Based Defenses

Medium Scale Sites Face Resources Challenges.

Research

1 Successful Research In:

- Network Monitoring
- Anomaly Detection
- Deep Packet Inspection
- Filtering

3B Incremental Advances

- More Anomaly Detection
- More Complex Detection

Little/no deployment of new techniques

5 Attacks are growing worse while research is largely dormant

1. 1990's major advances in research lead to IDS and filtering concepts

2. Transition To Practice for research produces industry leaders

3A. Research and deployment provide sites with understanding of attack sources, but few mitigations

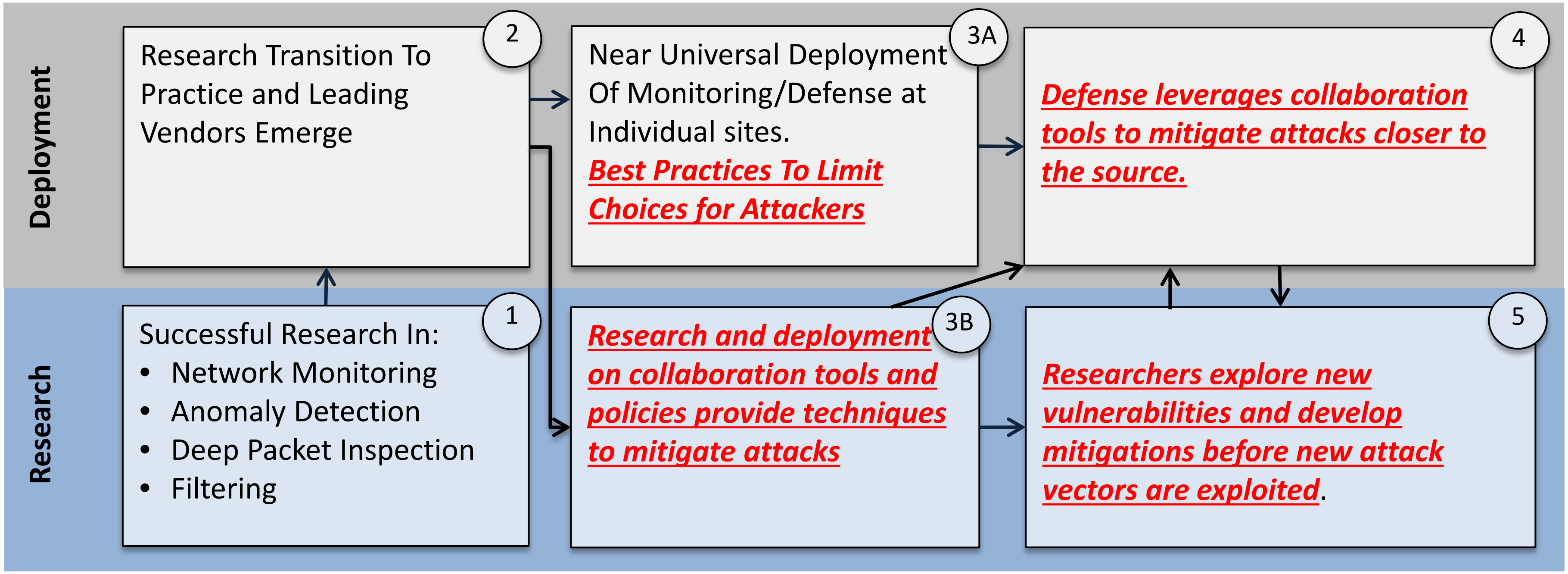
3B. Research focuses on incremental advances with little to know transition

4. With very few options, alarming discussions of defensive counter-strikes

5. Research is effectively dormant while attacks increase in scale and defenders fall further behind

**Attacker Has Inherent Advantage in Resources, Communications, and Targets**

# Status Quo: With DDoSD



Deployment

Research

2 Research Transition To Practice and Leading Vendors Emerge

3A Near Universal Deployment Of Monitoring/Defense at Individual sites. ***Best Practices To Limit Choices for Attackers***

4 ***Defense leverages collaboration tools to mitigate attacks closer to the source.***

1 Successful Research In:

- Network Monitoring
- Anomaly Detection
- Deep Packet Inspection
- Filtering

3B ***Research and deployment on collaboration tools and policies provide techniques to mitigate attacks***

5 ***Researchers explore new vulnerabilities and develop mitigations before new attack vectors are exploited***.

1. 1990's major advances in research lead to IDS and filtering concepts

2. Transition To Practice for research produces industry leaders

3A. Sites have understanding of attack sources and best practices aid in attribution

3B. Research focuses on collaboration tools and polices driven by industry demand

4. Defense leverages best practices and improved communication to block attacks further from victims

5. Research proactively explores new attack vectors and proactively develops mitigations

**Shift advantages toward DDoS defenders through**
**Best Practices, Collaboration Tools, and Novel Defenses**

# DDoSD Program Approach

- DDoSD Identifies Three Topic Areas:

***(1) Measurement and Analysis to Promote Best Current Practices***

Slow the growth in DDoS attacks by adopting best practices

***(2) Tools for Communication and Collaboration***

Provide existing targets more effective tools and techniques for response and mitigation,

***(3) Novel DDoS Attack Mitigation and Defense Techniques***

Anticipate new types of attacks before they occur.

- Proposals must identify one (and only one) topic area.

Homeland Security
Science and Technology

# Topic Area 1: Best Practices

- **Standards Exist That Make Attacks More Difficult and Attribution Easier**
  - Techniques such as ***Best Current Practice 38 (BCP38)*** block spoofing
  - Essentially check the packets leaving your network have your address
    - E.G. Packets leaving DHS network have DHS return addresses (source address)
  - Spoofed packets used in a variety of attacks
    - Computer at DHS reports its source is an NSF computer so others reply to NSF
    - Computer at DHS reports its source is NSF so others think NSF (not DHS) is attacking them
  - Technology to block spoofing largely available, only minor changes needed
  - Tragedy Of The Commons Challenge
    - Deployment blocks spoofed packets used to attack other networks
- **Work to Promote Standards**
  - Incorporate into relevant recommendations
  - Published acquisition policy
  - Increase government and commercial deployment
- **Measurement and Deployment Needed**
  - Modeled on past successful DHS DNSSEC activities
  - Active measurement and reporting
    - Build on successful preliminary work on anti-spoofing measurement

# Topic Area 1: Best Practices

- **Objective 1: Open Source Software Tool for Anti-Spoofing Assessment**
  - Determine whether site has successfully deployed anti-spoofing best practices
  - Provide on-going monitoring to verify anti-spoofing best practices
  - Code release due nine months from project start.
  - Timeline for subsequent updates based on lessons learned from deployment.

- **Objective 2: Anti-Spoofing Metrics and Analysis**
  - Describe how anti-spoofing best practices could be measured and identify metrics.
  - Quarterly Status Reports on how best practice deployment is (or is not) advancing.

- *Analysis Is More Than A Simple Count*
  - Unlikely any efforts will achieve 100% deployment
  - Not clear 100% deployment is necessarily the right goal.
  - Explore the best way to assess best practice deployment status
  - Aide parallel work on promoting the ***most effective*** deployment strategy

# Topic Area 2: Tools For Communication and Collaboration

- **Objective:**
  Develop tools and techniques that allow a **medium size organization** to withstand a **one terabit per second** attack originating from over **one thousand locations.**
- Assumed Attack Volume: 1 Terabit Per Second
  - Attacks continue to grow in volume
  - Attack volume is ambitious: Not aware of current attacks reaching 1 Tbps
  - Attack volume may underestimate threat: Trend suggest it could exceed 1 Tbps
- Assumed Attack Target: Medium Size Organization
  - Intended to focus the communication and collaboration tools
  - Cannot assume medium size organization has global presence
  - Cannot assume a medium size organization can absorb 1 Tbps at its borders
- Assumed Attack Source: Over one thousand locations
  - Intended to focus adversary assumptions
  - Cannot assume attacks originates from a single location
  - Implies attacker is coordinated resources in multiple locations

# Topic Area 2:
# Tools For Communication and Collaboration

- Collaboration and Communication Tools To Aide Defenders
  - Attacks rely on sophisticated communication techniques
  - Defense has not kept pace and innovative approaches are needed
  - Approach could be centralized or distributed
  - Must address challenges appropriate to the chosen direction
- **Address Combination of Technical Challenges and Policy Challenges**
  - Expectation is for implementations and working prototypes
  - Policies and realistic operational expectations must be included
  - Not valid to any one approach would be deployed on all Internet routers or deployed at all Autonomous Systems
  - Approach must recognize the inherent diversity in operational practices and diversity in organizational policies

- Testing and Evaluation
  - Testing and Evaluation are mandatory part of proposals
  - May be based on simulations,  emulations,  analysis
  - Plan for demonstration of progress on annual basis (minimum)
  - Ultimate objective is to withstand 1 Tbps attack from 1,000+ locations

# Topic Area 3: Novel New Directions

- **DDoS Attacks Continue To Hit New Targets**
  - Classic DDoS attacks overwhelm access links or specific servers
  - Next attacks expanded to infrastructure including routers and data centers
  - New attacks growing into new spaces including *emergency response and power*
  - No clear defense preventing attacks on new systems; autos to medical devices
- **Research Is Largely Dormant**
  - Few active projects
  - Novel new attacks “should have been foreseen”
  - Defense operating in a largely reactive environment
- **Reinvigorate Research on New Directions**
  - Focus on new attack targets and new attack strategies
  - Produce corresponding mitigations
  - Proactively address new challenges

# Topic Area 3: Novel New Directions

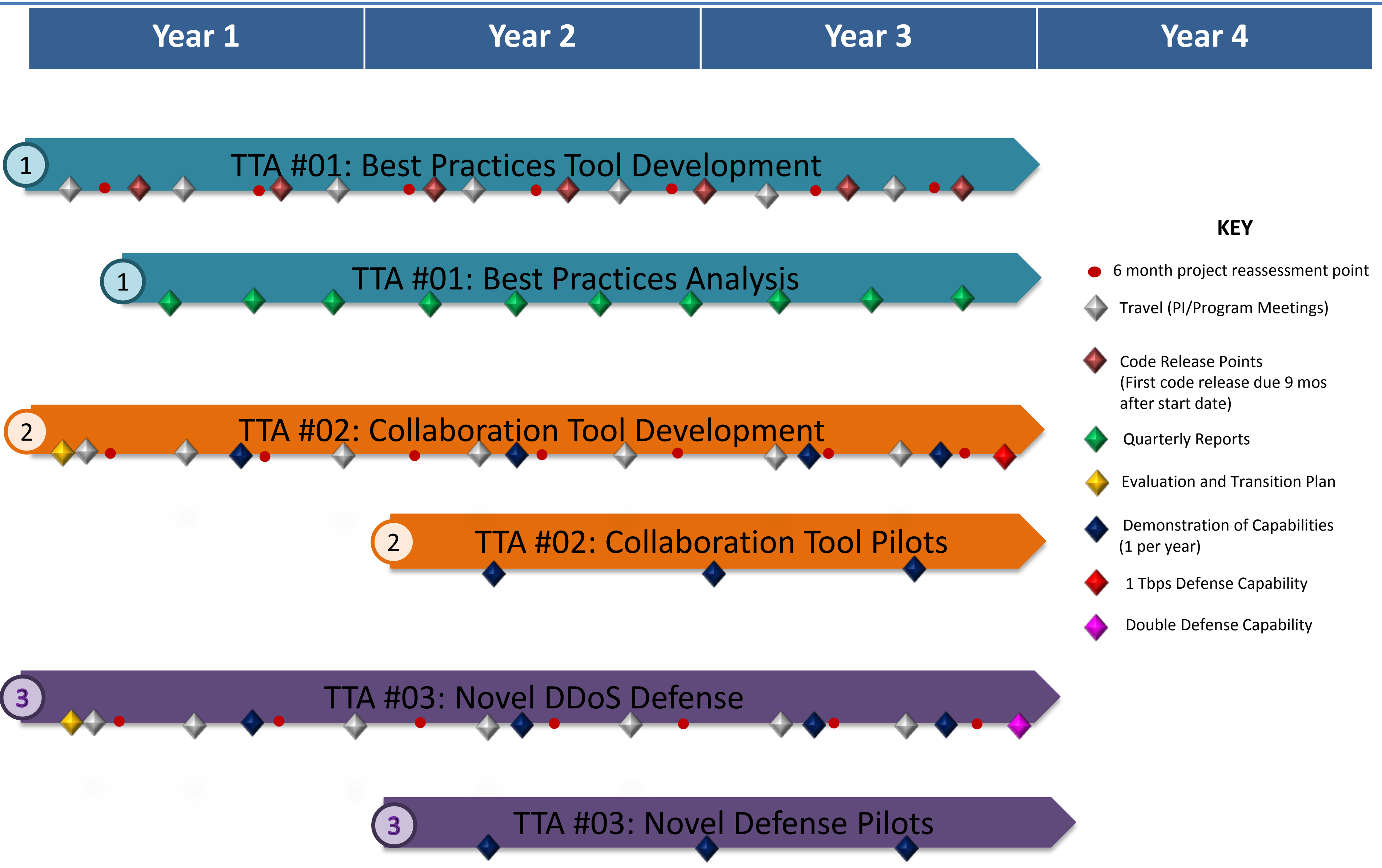
- **Proposals Must Identify Metrics  Relevant to The Target**
  - Topic area encourages flexibility and creativity for new types of targets
  - Topic area encourages flexibility and creativity for new types of attacks
  - Recognizes the metrics for these novel systems may be different
  - Ex:   Attacks on a 911 system may be measured in phone calls rather than  in bits per second
  - Require the proposal to explicitly identify the relevant metric(s)
  - Evaluation will be tied to the selected metric(s)

- Testing and Evaluation
  - Testing and Evaluation are mandatory part of proposals
  - May be based on simulations,  emulations,  analysis
  - Plan for demonstration of progress on annual basis (minimum)
  - Ultimate objective is to double the capacity to withstand attacks

# Program Impact: DDoS Defense

- Best Practice Impacts
  - Increased Deployment of Best Practices
  - Reporting and Monitoring on Security Deployment
  - Reduction of attack surface used in DDoS
  - Additional Benefits to Attribution, Anti-BotNet, Spam, Phishing
- Communication and Collaboration Impacts
  - Open source tools and template policies
  - Improved ability for organizations to counter DDoS attacks
  - Applicability to critical infrastructure sectors
- Novel DDoS Impacts
  - Re-ignite research in area of growing threats
  - Move from reactive post-attack analysis to preventive actions

# Schedule and Milestones



Year 1 | Year 2 | Year 3 | Year 4

1 TTA #01: Best Practices Tool Development

1 TTA #01: Best Practices Analysis

2 TTA #02: Collaboration Tool Development

2 TTA #02: Collaboration Tool Pilots

3 TTA #03: Novel DDoS Defense

3 TTA #03: Novel Defense Pilots

**KEY**

- ● 6 month project reassessment point
- ◆ Travel (PI/Program Meetings)
- ◆ Code Release Points (First code release due 9 mos after start date)
- ◆ Quarterly Reports
- ◆ Evaluation and Transition Plan
- ◆ Demonstration of Capabilities (1 per year)
- ◆ 1 Tbps Defense Capability
- ◆ Double Defense Capability

# References

- Distributed Denial of Service (NY Times, April 1, 2013); http://www.nytimes.com/2013/04/02/science/distributed-denial-of-service.html
- Understanding Denial-of-Service Attacks: http://www.us-cert.gov/ncas/tips/ST04-015
- DHS Cyber Security Division Broad Agency Announcement HSHQDC-14-R-B005; https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-14-R-B0005/listing.html
- Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing; P. Ferguson and D. Senie; RFC 2827; http://www.ietf.org/rfc/rfc2827.txt
- Ingress Filtering for Multihomed Networks,; F. Baker and P. Savola, RFC 3704; http://tools.ietf.org/html/rfc3704
- DHS Software Assurance Marketplace (SWAMP); https://www.dhs.gov/csd-swamp
- Initial Longitudinal Analysis of IP Source Spoofing Capability on the Internet; Robert Beverly, Ryan Koga, kc claffy; http://www.internetsociety.org/doc/initial-longitudinal-analysis-ip-source-spoofing-capability-internet
- A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms; Mirkovic, Martin, Reiher; http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf
- REN-ISAC Alert: Prevent Your Institution From Being An Unwitting Partner In Denial Of Service Attacks; http://www.educause.edu/discuss/discussion-groups-related-educause-programs/security-discussion-group/ren-isac-alert-prevent-your-institution-being-u
- A Framework for Collaborative DDoS Defense G. Oikonomou, J. Mirkovic, P. Reiher and M. Robinson, ACSAC 2006, http://www.isi.edu/~mirkovic/publications/ACSAC06.pdf
- DHS Homeland Open Security Technologies (HOST); https://www.dhs.gov/csd-host
- DHS Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT), https://www.predict.org
- DHS, FBI warn over TDoS attacks on emergency centers, http://www.csoonline.com/article/731069/dhs-fbi-warn-over-tdos-attacks-on-emergency-centers
- "Power Attack: An Increasing Threat to Data Centers", Zhang Xu, Haining Wang, Zichen Xu, and Xiaorui Wang, the 21st Network and Distributed System Security Symposium (NDSS 2014), San Diego, California, February 2014.
- DHS Cyber Defense Technology Experimental Research (DETER) network, (http://deter-project.org

Homeland Security

Science and Technology