PCH
Packet Clearing House

Lessons Learned from the Russian-Estonian Cyber-Conflict

Version 1.0

June, 2007

Bill Woodcock

Packet Clearing House

PCH
Packet Clearing House

What Was New?

Incidents beyond counting in the last twenty years, but...

PCH
Packet Clearing House

What Was New?

Incidents beyond counting in the last twenty years, but very few have been state-actor...

PCH
Packet Clearing House

What Was New?

Incidents beyond counting in the last twenty years, but very few have been state-actor, this one was relatively large (though not optimized for size or network impact)...

PCH
Packet Clearing House

What Was New?

Incidents beyond counting in the last twenty years, but very few have been state-actor, this one was relatively large (though not optimized for size or network impact), and very few have been defended with such complete success.

PCH
Packet Clearing House

What Was New?

Incidents beyond counting in the last twenty years, but very few have been state-actor, this one was relatively large (though not optimized for size or network impact), and very few have been defended with such complete success.

Thus, there are new lessons to be learned, and not just the usual NSP operators should be paying attention.

PCH
Packet Clearing House

What Made Estonia so Successful?

Command structure was young and connected.

They skipped the whole “is the network worth protecting” step that older countries seem to invariably get hung up on.

They already had the necessary channels of communication established prior to the attack.

PCH
Packet Clearing House

What Makes Other Countries More Vulnerable?

Lack of understanding and conviction.

Lack of commitment to funding defensive operations.

Scale. Many countries are too large for everyone who matters to already know everyone else who matters.

PCH
Packet Clearing House

Roles in Cyber-Conflict

User population
Network service providers
CERT
Law enforcement
Ministry of Foreign Affairs
Military

PCH
Packet Clearing House

Roles in Cyber-Conflict

User population	Intelligence
Network service providers	Defense
CERT	Analysis & coordination
Law enforcement	Domestic prevention
Ministry of Foreign	International prevention
Military	Credible threat of offense

PCH
Packet Clearing House

User Population

The population of users – people in their homes and offices – are essentially the only ones who can determine authoritatively that an attack is taking place and provide the intelligence that differentiates an attack from productive traffic.

What differentiates a DDoS from a slashdotting? Only end-user expectations.

PCH
Packet Clearing House

Network Service Providers

NSPs have absolute control over the field of action when they choose to exercise it, but are essentially neutral until called into play by their user constituencies or attacked directly.

The cost of exercising control can be immense and unrecompensed.

PCH
Packet Clearing House

CERTs

Computer Emergency Response Teams provide the dedicated intelligence analysis, real-time forensic capabilities, and specialized channels of coordination that end-users cannot afford to each maintain individually.

CERTs are the primary site of national shared investment in common defense.

PCH
Packet Clearing House

Law Enforcement

A coherent and comprehensive system of laws which prohibit cyber-offense, and effective and obvious enforcement of those laws, are the mechanism whereby domestic attacks are forestalled.

PCH
Packet Clearing House

Ministry of Foreign Affairs

Diplomacy, on the part of the department of state or foreign affairs or its equivalent, is the mechanism whereby a nation forestalls attacks on the part of other state actors or forces under their control.

PCH
Packet Clearing House

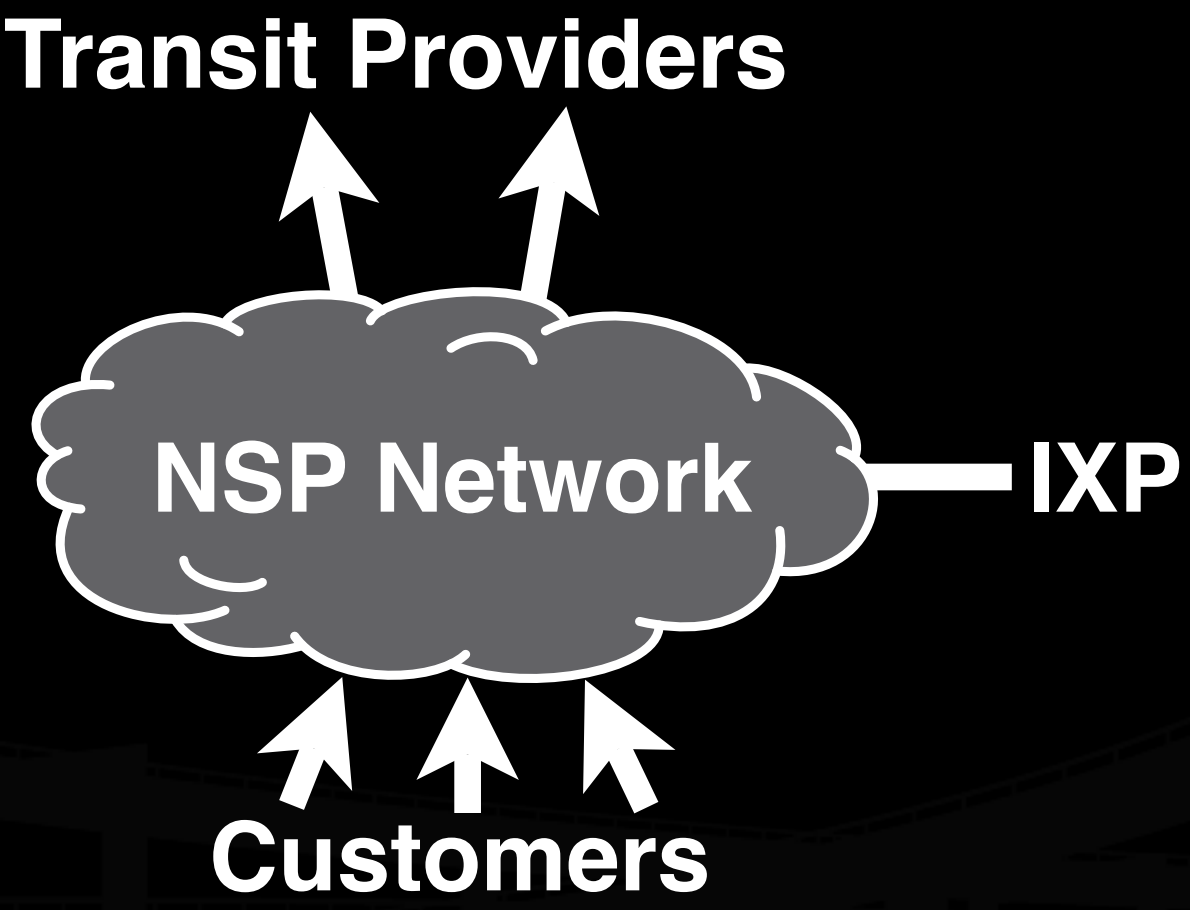
Military

In countries other than China, militaries do not have privileged access to or control over the field, so militaries are reduced to solely offensive roles in cyber-conflict.

In this regard, they provide the credible threat behind diplomatic negotiation.

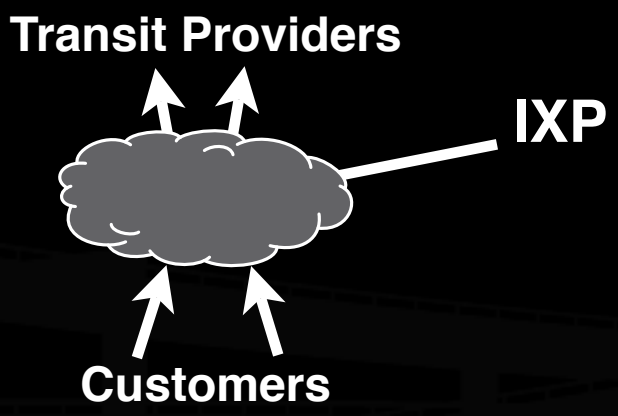
PCH
Packet Clearing House

Essential Model of an ISP



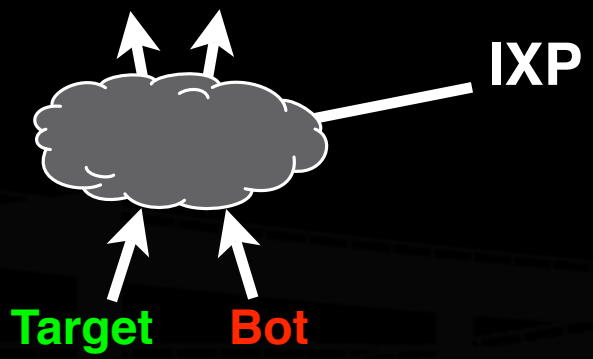
PCH
Packet Clearing House

Topology of the Field



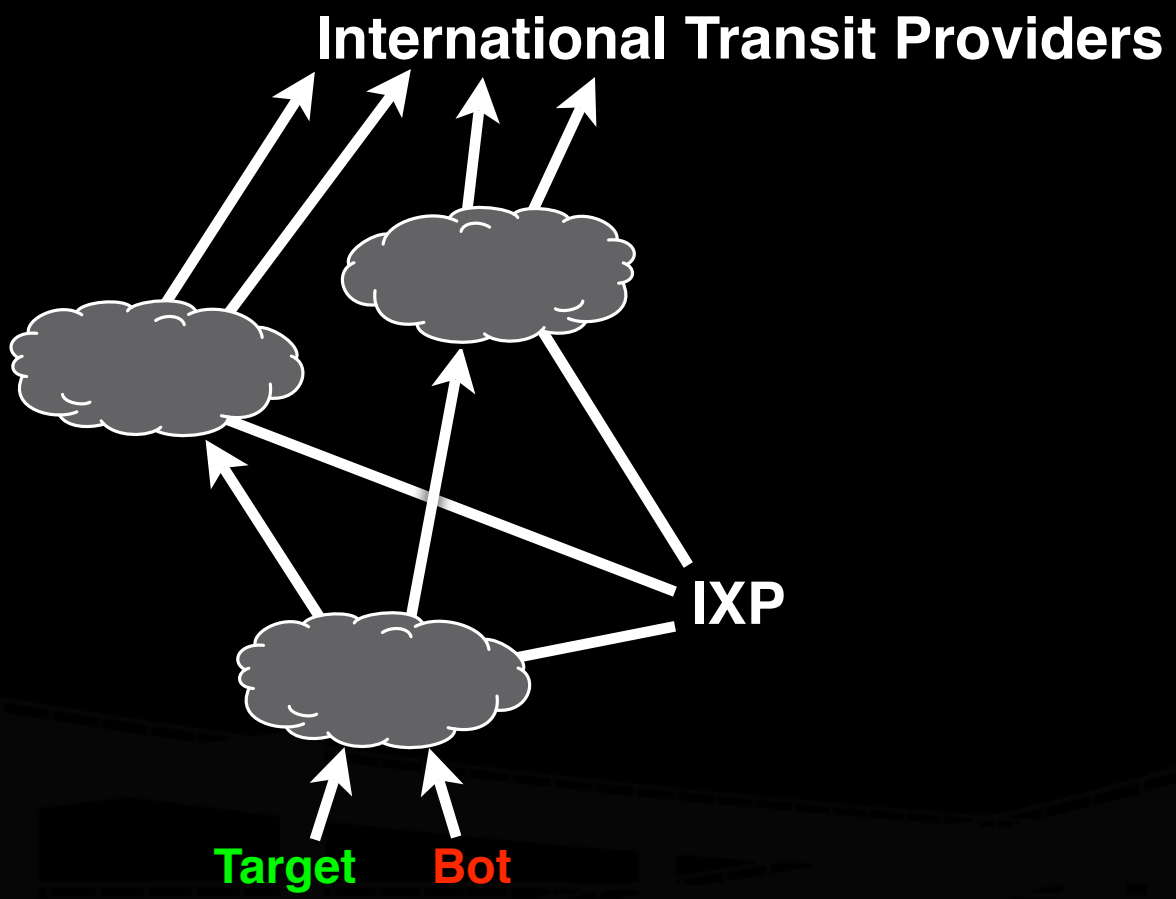
PCH
Packet Clearing House

Topology of the Field



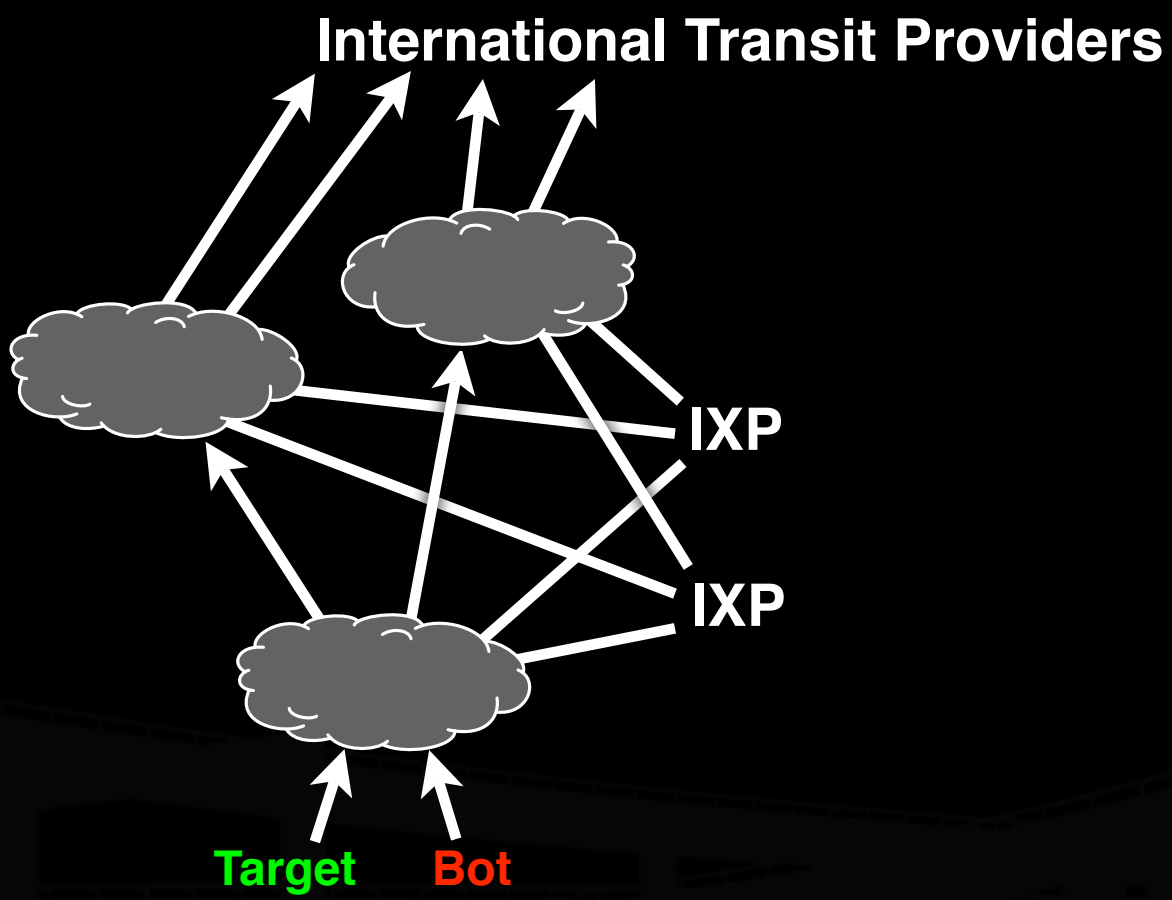
PCH
Packet Clearing House

Topology of the Field



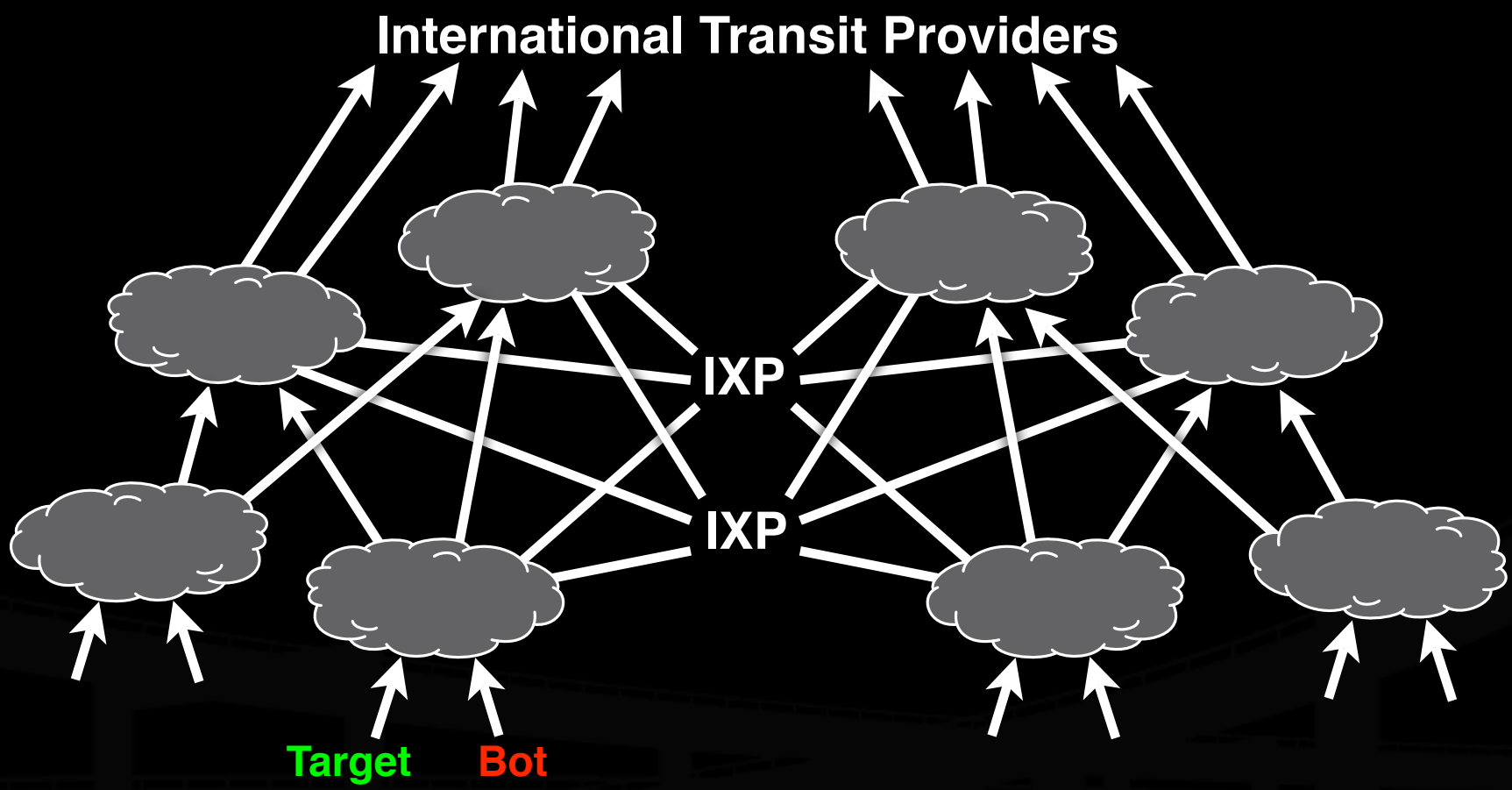
PCH
Packet Clearing House

Topology of the Field



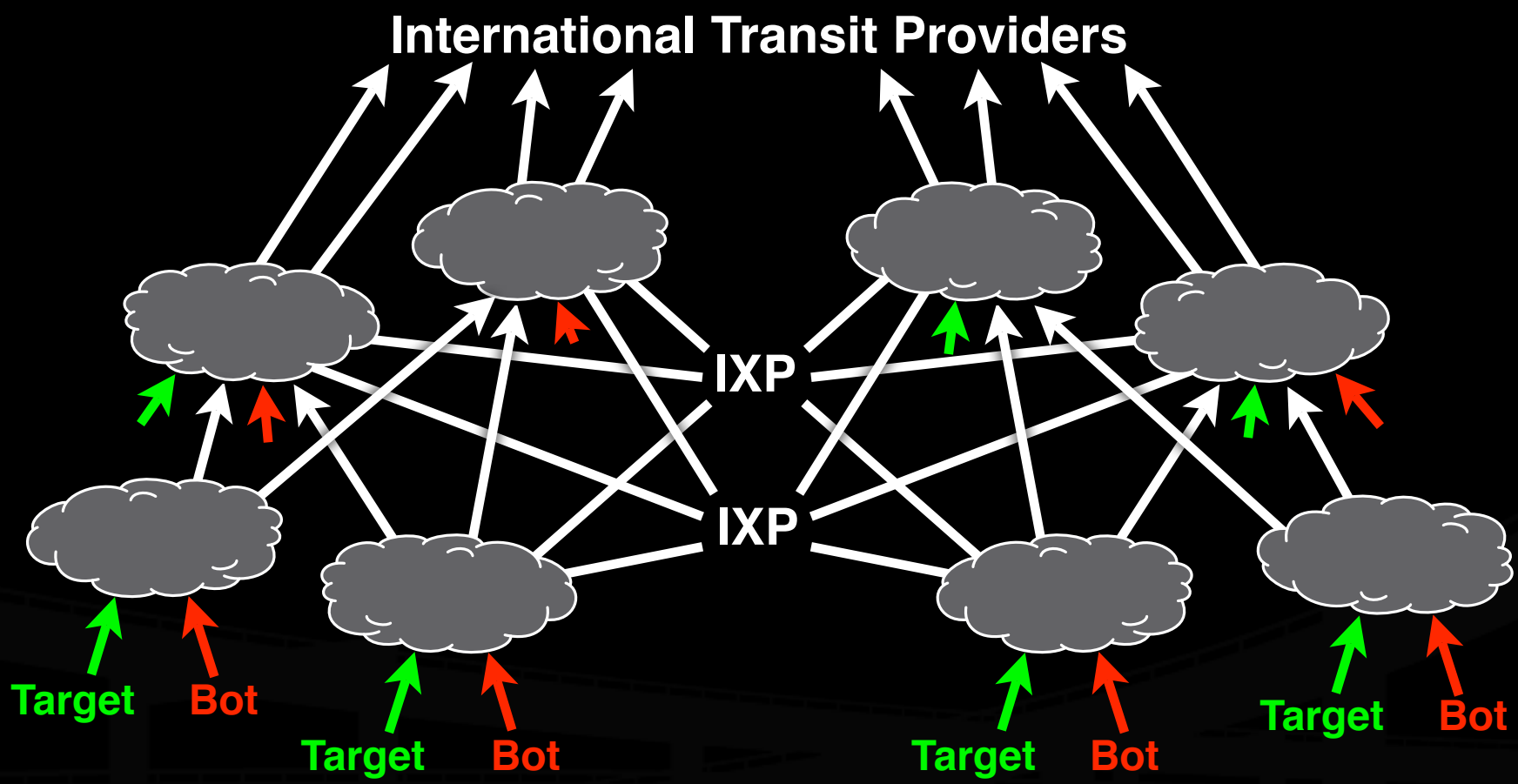
PCH
Packet Clearing House

Topology of the Field



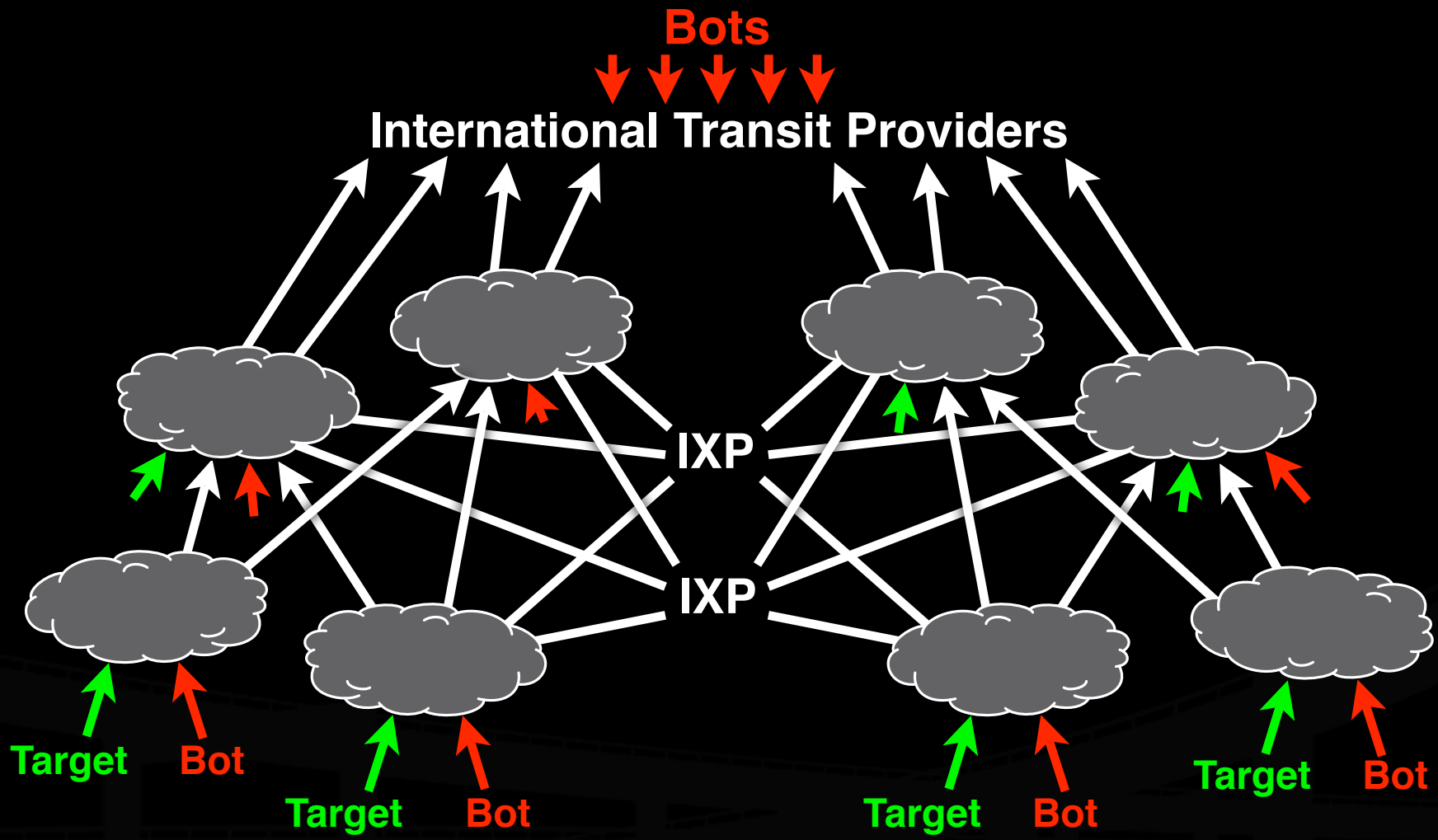
PCH
Packet Clearing House

Topology of the Field



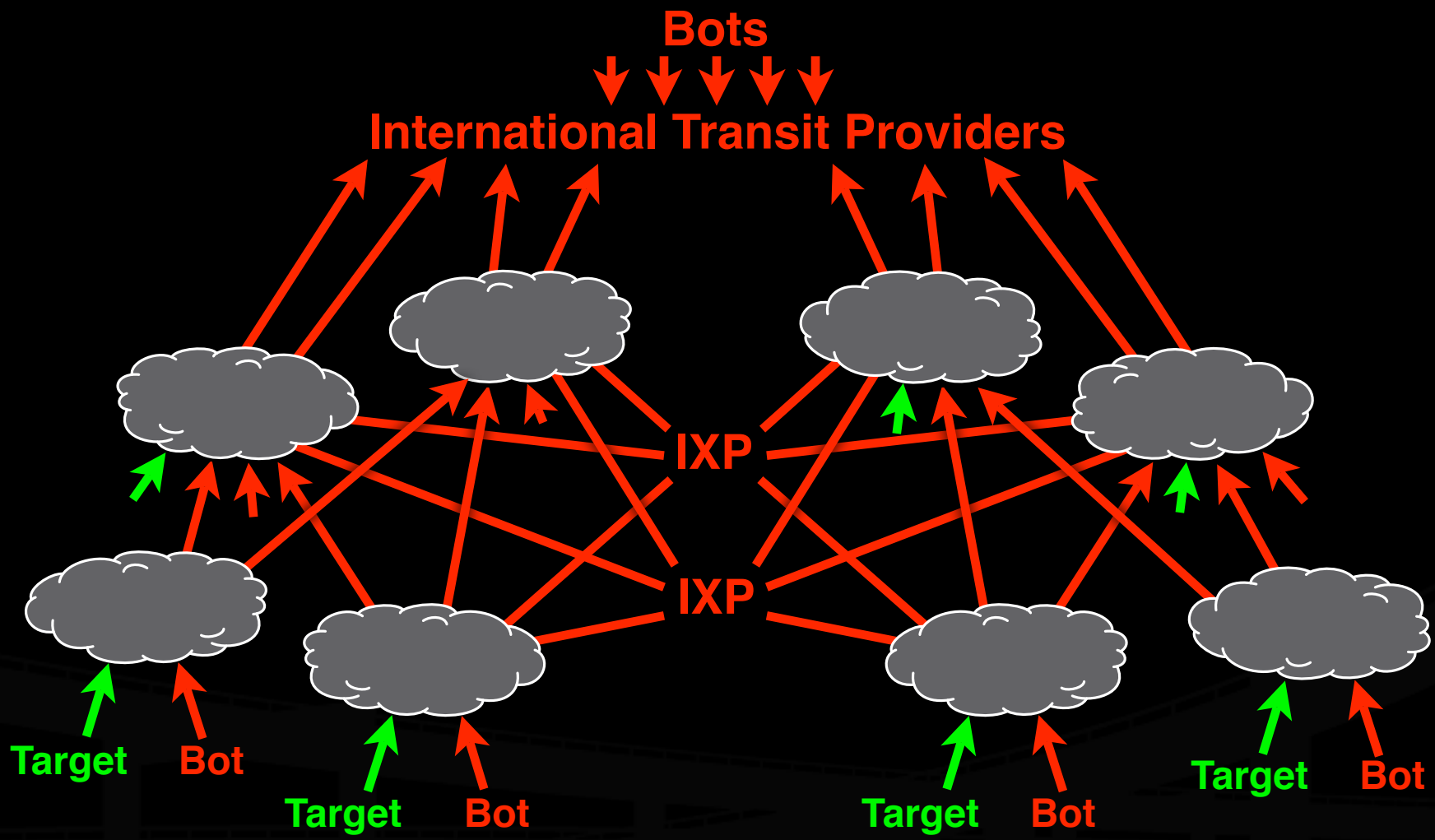
PCH
Packet Clearing House

Topology of the Field



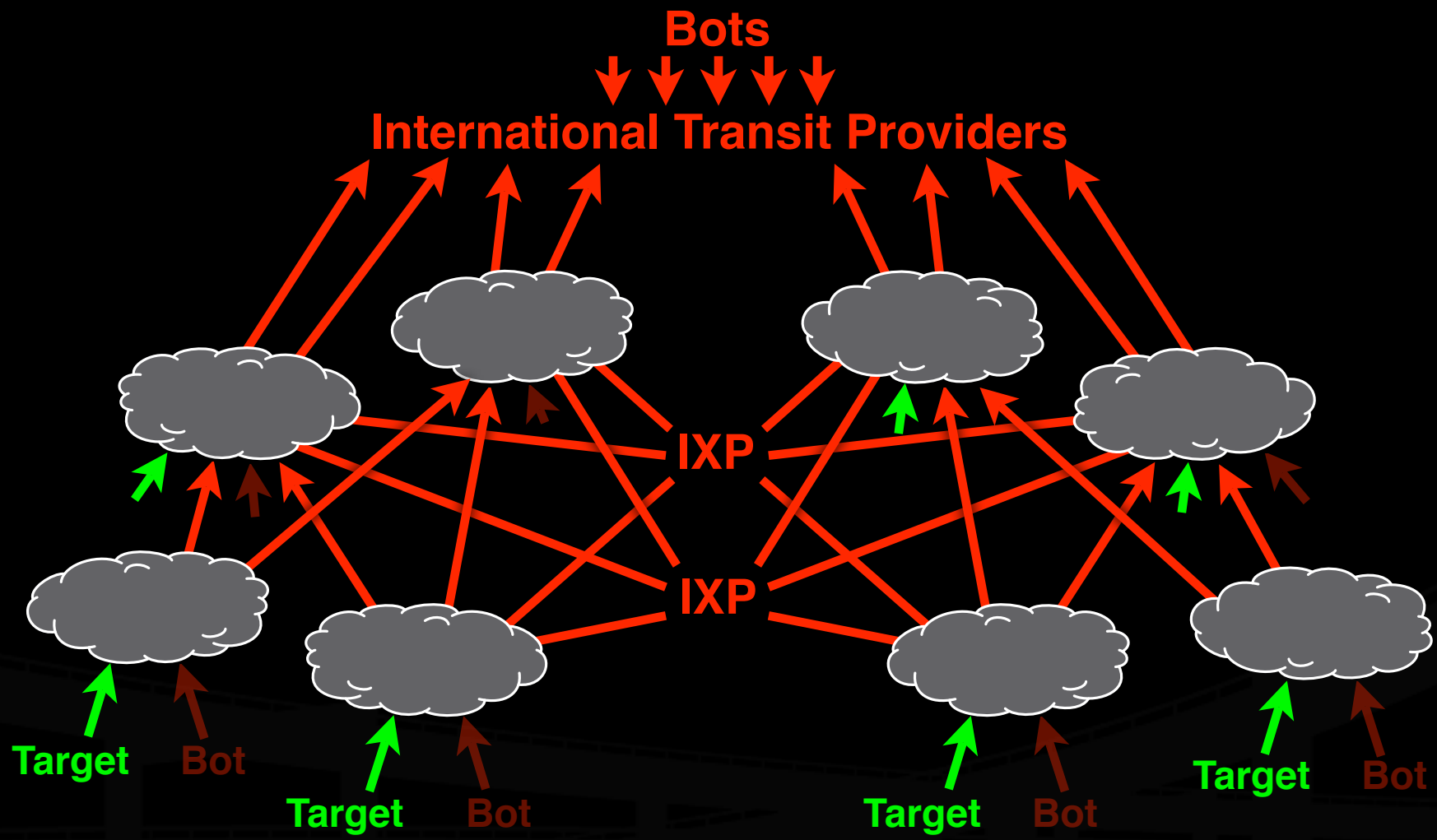
PCH
Packet Clearing House

Topology of the Field



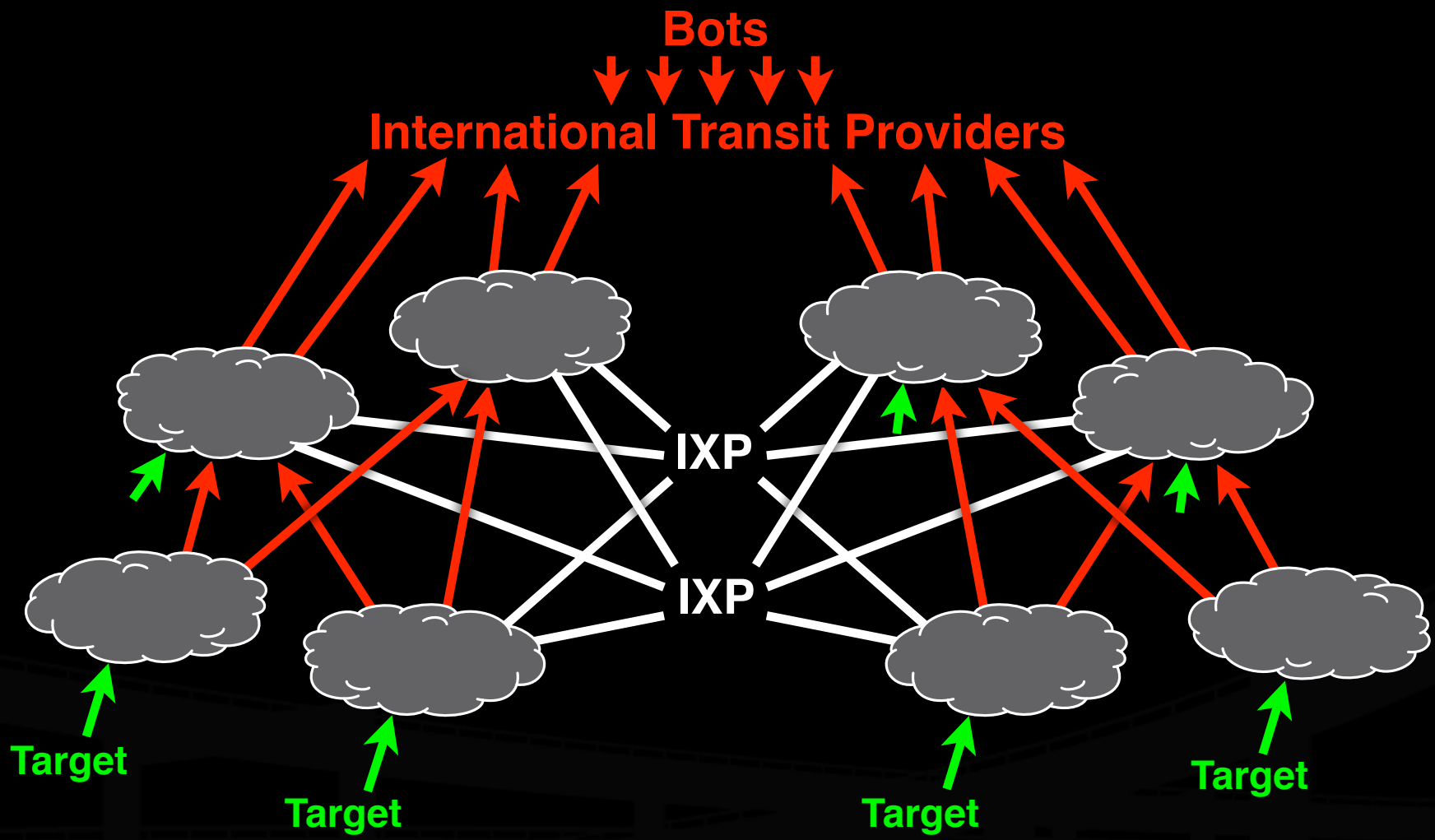
PCH
Packet Clearing House

NSPs and Law Enforcement



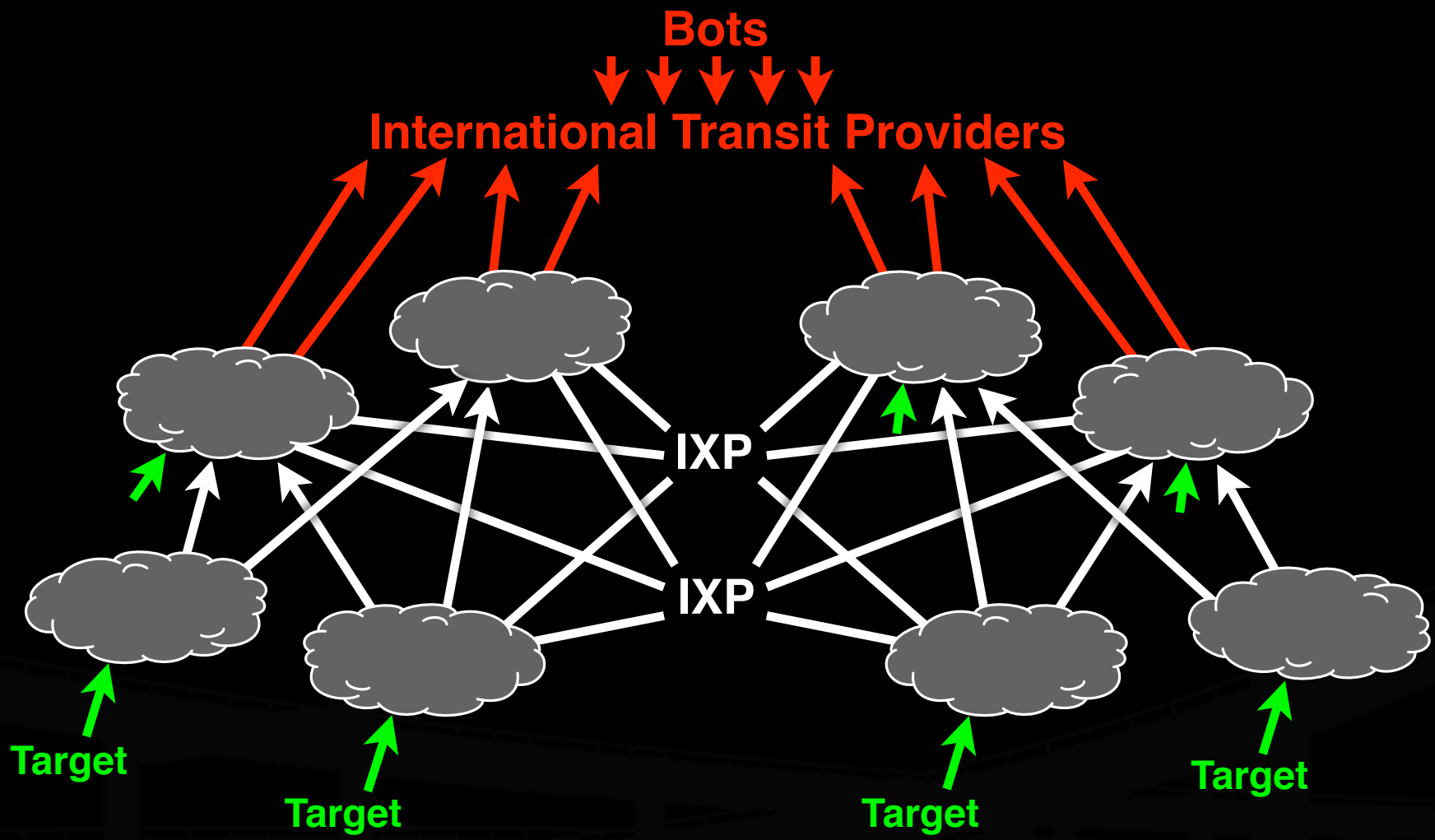
PCH
Packet Clearing House

NSPs and Law Enforcement



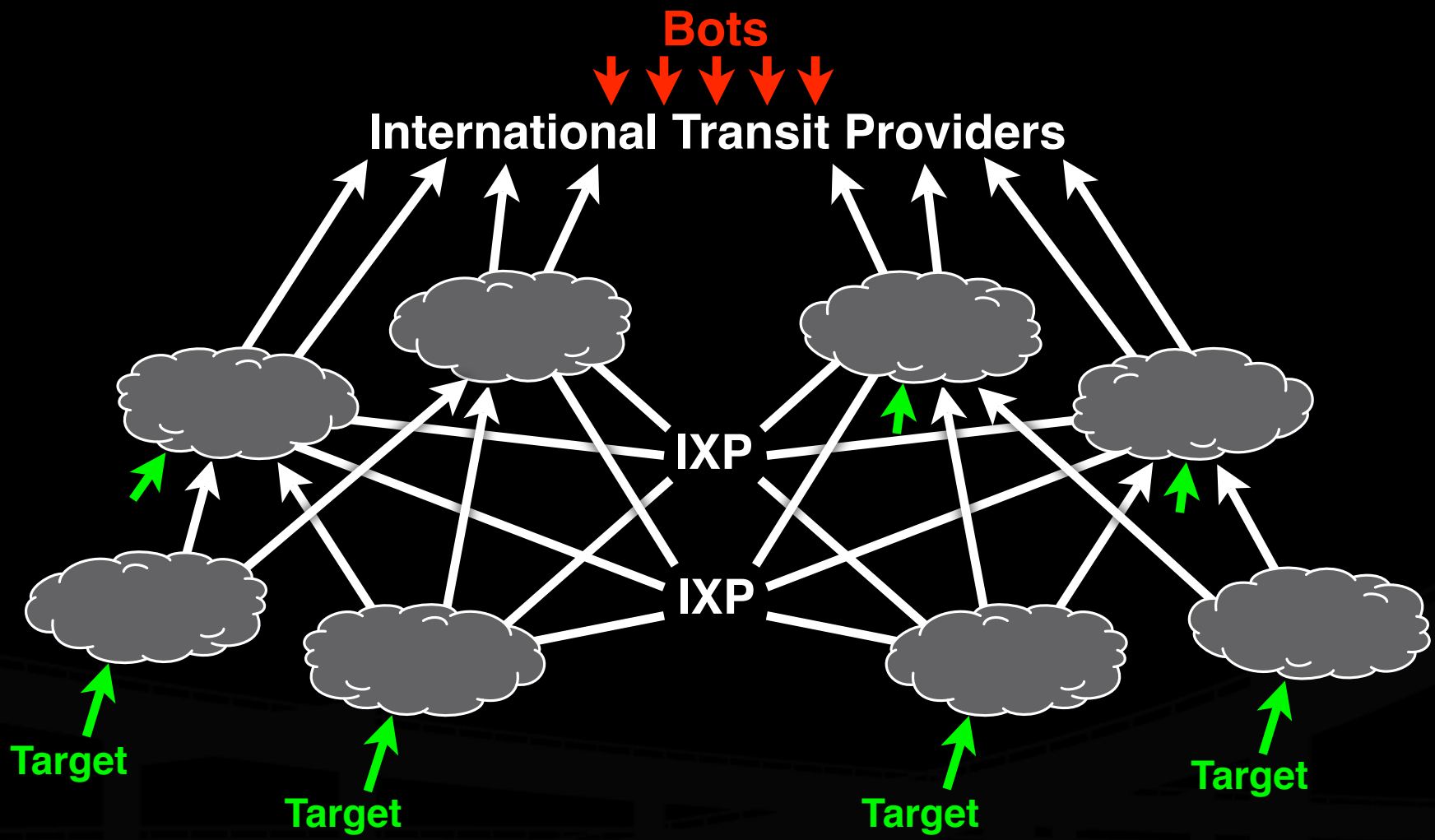
PCH
Packet Clearing House

NSPs and CERT



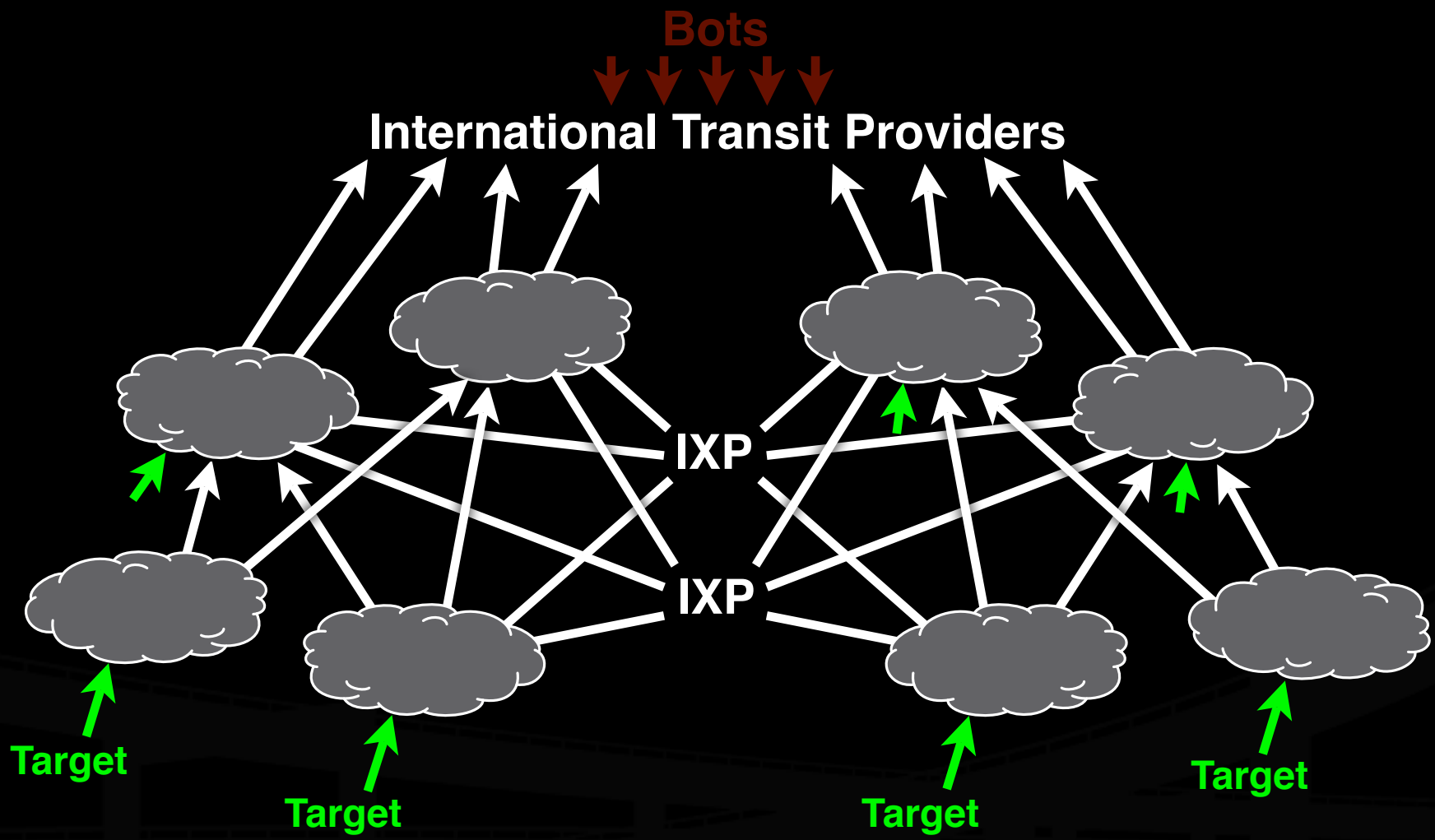
PCH
Packet Clearing House

NSPs and CERT



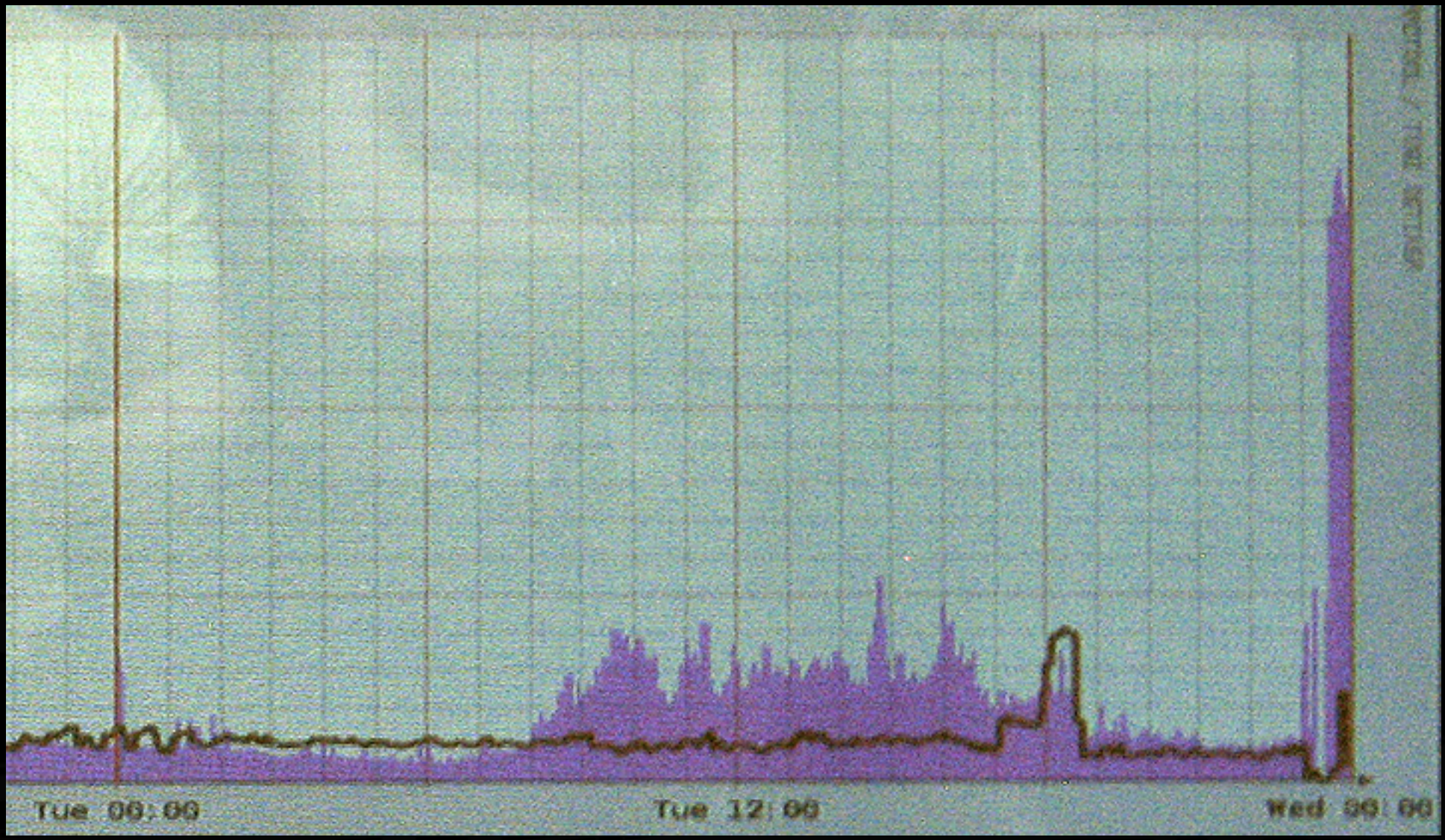
PCH
Packet Clearing House

Diplomacy and International Law Enforcement



PCH
Packet Clearing House

International Capacity



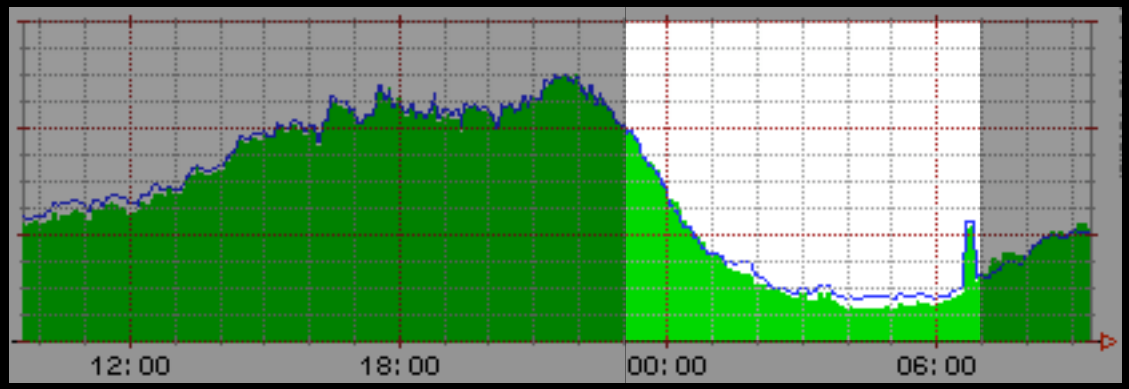
PCH
Packet Clearing House

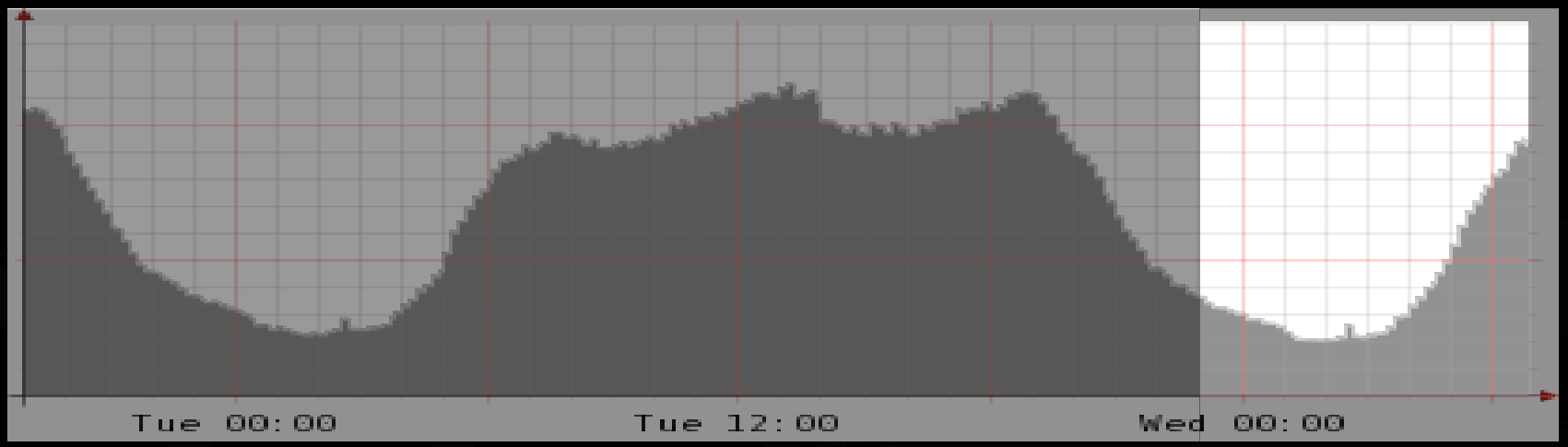
Impact on International Capacity

More than 3mpps at peak
Mitigated to 30kpps by 7am by diligent work through the night on the part of the CERT-EE and many NSPs.

PCH
Packet Clearing House

Domestic Capacity





PCH
Packet Clearing House

Impact on Domestic Capacity

None.
Entirely prevented by timely and decisive action by law enforcement.

PCH
Packet Clearing House

Diplomatic Efforts

Despite a lot of effort on the part of the Estonian government, and their status as a recent NATO member, there has been little or no diplomatic pressure brought to bear on Russia thus far.

Although Nashi has claimed responsiblity, no arrests nor extraditions have been made.

PCH
Packet Clearing House

Military Efforts

The Estonian National Defense Force has no known cyber-offense capability and little kinetic offense capability, and thus poses no credible threat to Russia to back diplomatic efforts of its own.

No nation with cyber-offense capability has offered any force to back Estonia's diplomatic position.

PCH
Packet Clearing House

All Cyber-Conflict is Insurgency

Defenders have absolute control over means of production and access to the field of battle. Their weapon is intelligence.

Attackers have the initiative, and win through attrition and asymmetric expenditure. Their weapon is disruption.

PCH
Packet Clearing House

Goals of a Defending Force

- Maintain order
- Maintain means of production
- Maintain the confidence of the population
  - Continued efficient labor
  - Creativity and innovation
  - Investment and reinvestment
  - Low-friction transactions

PCH
Packet Clearing House

Goals of an Attacking Force

Disable the defender's means of production
Disable the defender's means of defense
Deny them privacy
Remove their confidence
Increase their cost of operation
Increase their cost of capital

Thanks, and Questions?

Copies of this presentation can be had
in Keynote or PDF on request.

Bill Woodcock
Research Director
Packet Clearing House
woody@pch.net