Asymmetric warfare and interception revealed

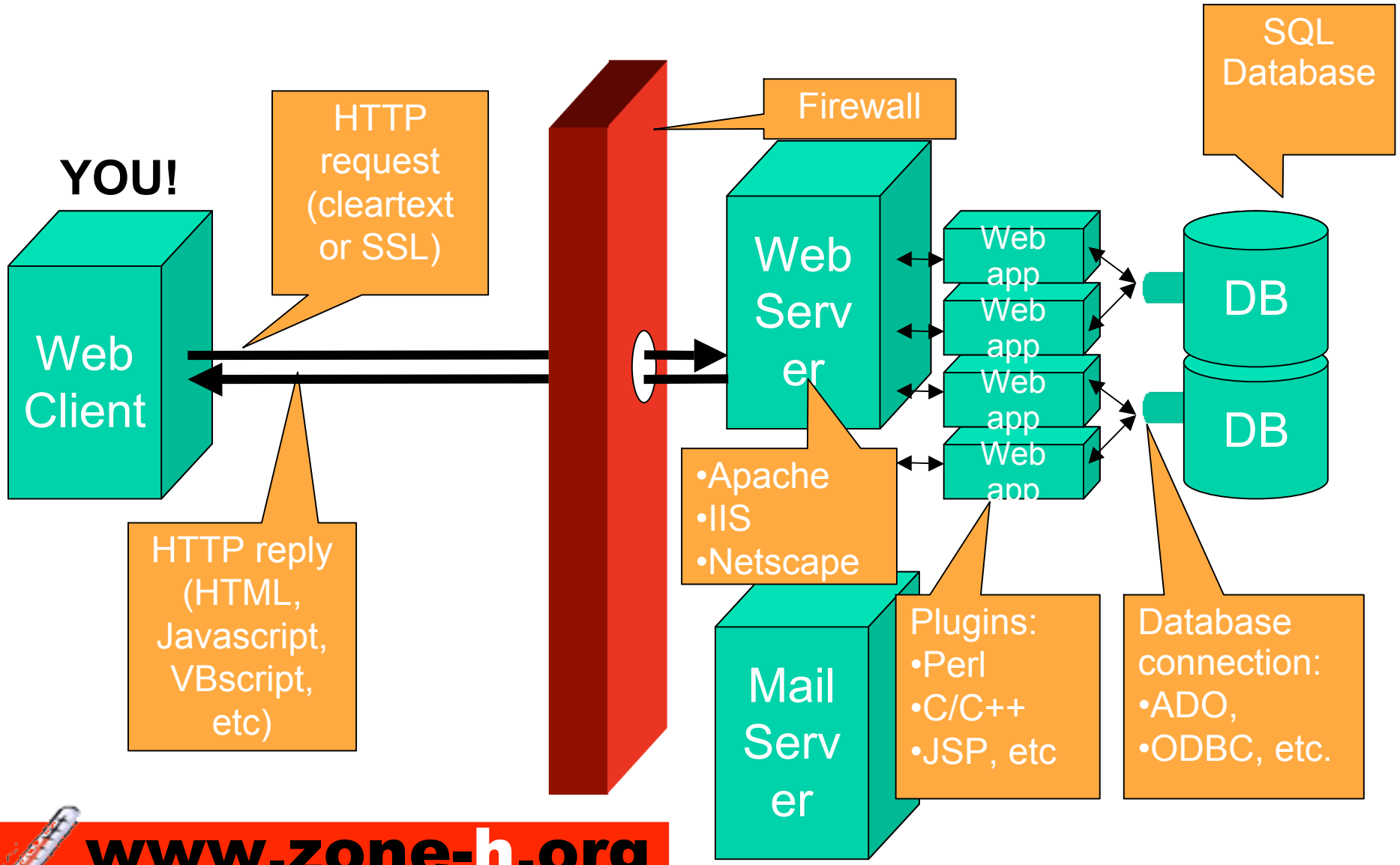
THE LECTURERS

Fabio Ghioni

Roberto Preatoni

www.zone-h.org
the Internet thermometer

Why Zone-H ?



www.zone-h.org
the Internet thermometer

www.zone-h.org

the Internet thermometer

In 2004 35.000+ / months

Internet today

INTERNET

TODAY

40 millions of servers

MOBILE CELLPHONES

TODAY

APPROAX 1 BILLION

www.zone-.org

the Internet thermometer

Internet today

INTERNET TODAY

+

MOBILE CELLPHONES

CONVERTED INTO 3G / 4G

= EXTREME PAIN

www.zone-.org

the Internet thermometer

3g exploitable points

- Protocol
- Telco network component
- OS
- User application level
- SIM / USIM toolkit application level

About terrorism

TERRORISM ?

www.zone-.org

the Internet thermometer

Asymmetric warfare

WHAT IS IT?

“threats outside the range of conventional warfare and difficult to respond to in kind “ U.S. Dictionary of Military Terms

WHEN IS IT USED?

“If the enemy is superior in strenght, evade him. If his forces are united, separate them. Attack him where he is unprepared; appear where you are not expected.” Sun Tzu

www.zone-h.org
the Internet thermometer

Asymmetric warfare and infowar

Asymmetric Warfare (AW)

"Battlefield" where small groups of individuals can produce massive damage with minimum effort and risk from virtually anywhere in the world.

Information Operations (IO)

Hit the adversary's information and IT systems and simultaneously defend one's own information and IT systems.

Information Warfare (IW)

Information Operations conducted in moments of crisis or conflict, aimed at reaching or promoting given objectives towards given adversaries.

www.zone-h.org

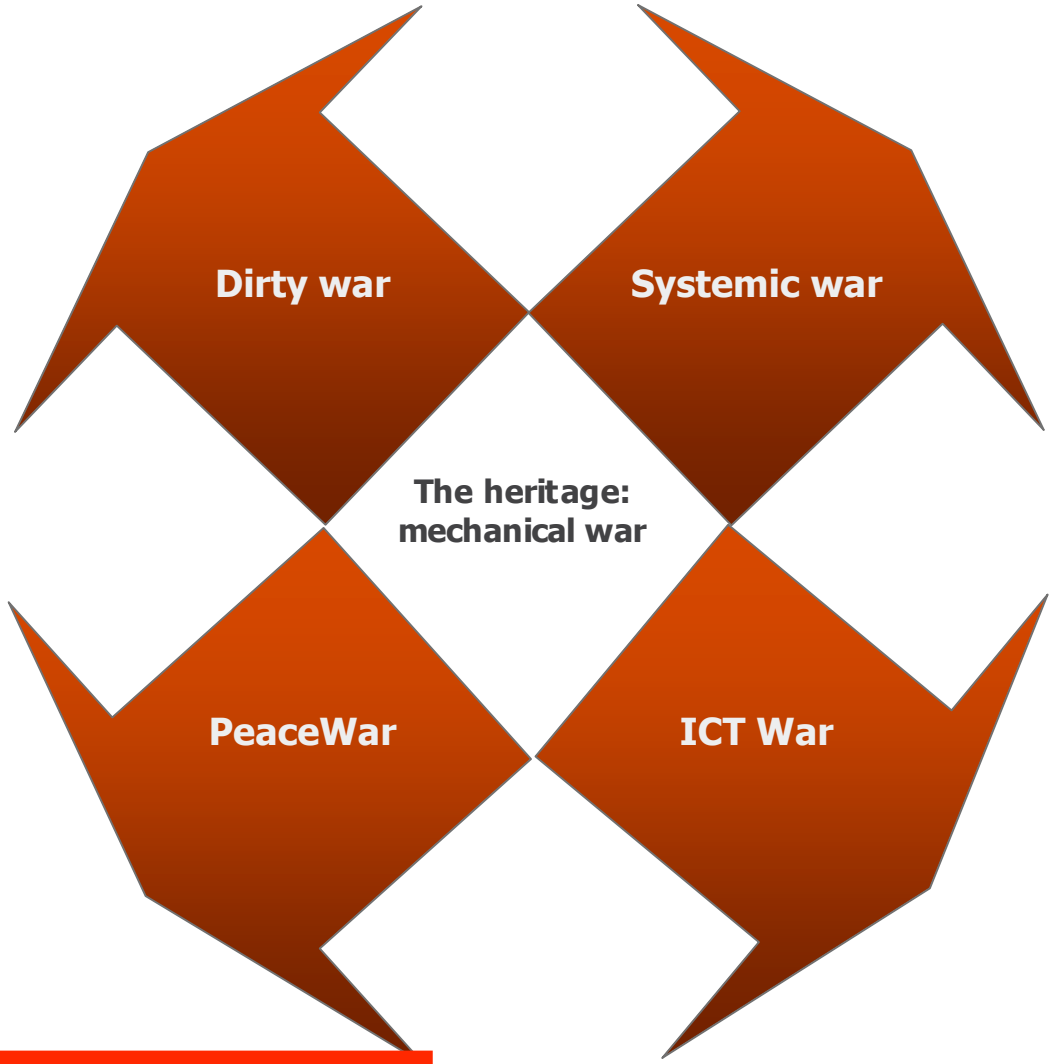
the Internet thermometer

ICT WARFARE

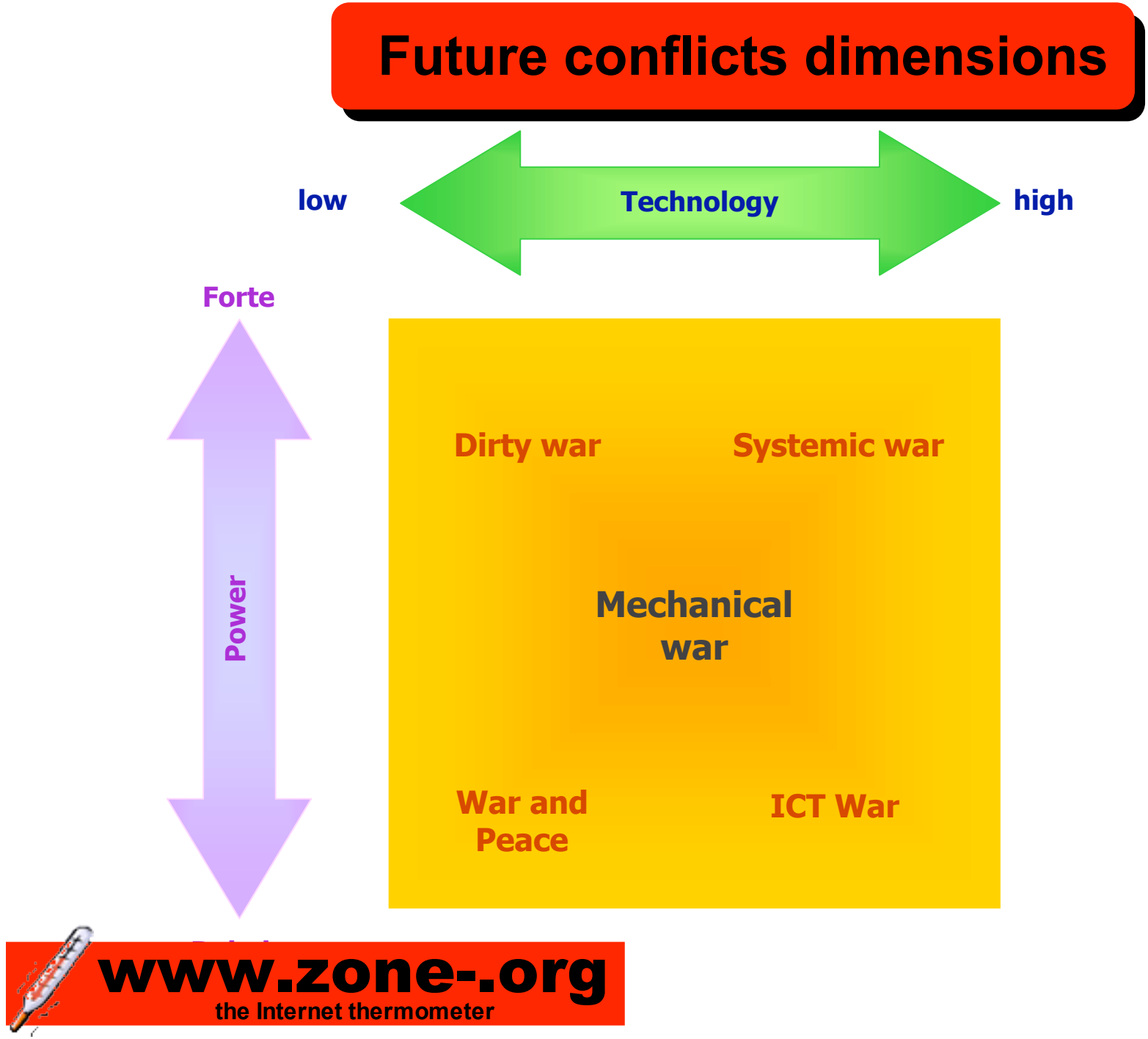
"It's the best strategy for an asymmetric conflict"

- **Distributed attacks, high anonimity**
- **Possibility to use the same enemy's infrastructures**
- **Low cost of technology implementation and R&D**
- **Wide range of critical infrastructures to be attacked**
- **Possibility to carry out unconventional activities**
- **Direct contact with the enemy's command and lowest ranks**

Future conflicts dimensions



Future conflicts dimensions



About terrorism

Usage of different conflict unconventional tipologies to defy an enemy with a superior warfare capability

-“Traditional terrorism”

- Use of chemical/nuclear/biological weapons

- Attack to the ICT infrastructures critical to the economy and national security

ICT war targets against e-nations

-Economy

-Public service infrastructures

-Military and civil defense

Multiplier of the above

Sensored networks and critical infrastructure protection

- National security
- Asymmetric warfare and infowar
- Defence and uses in state of war

National security

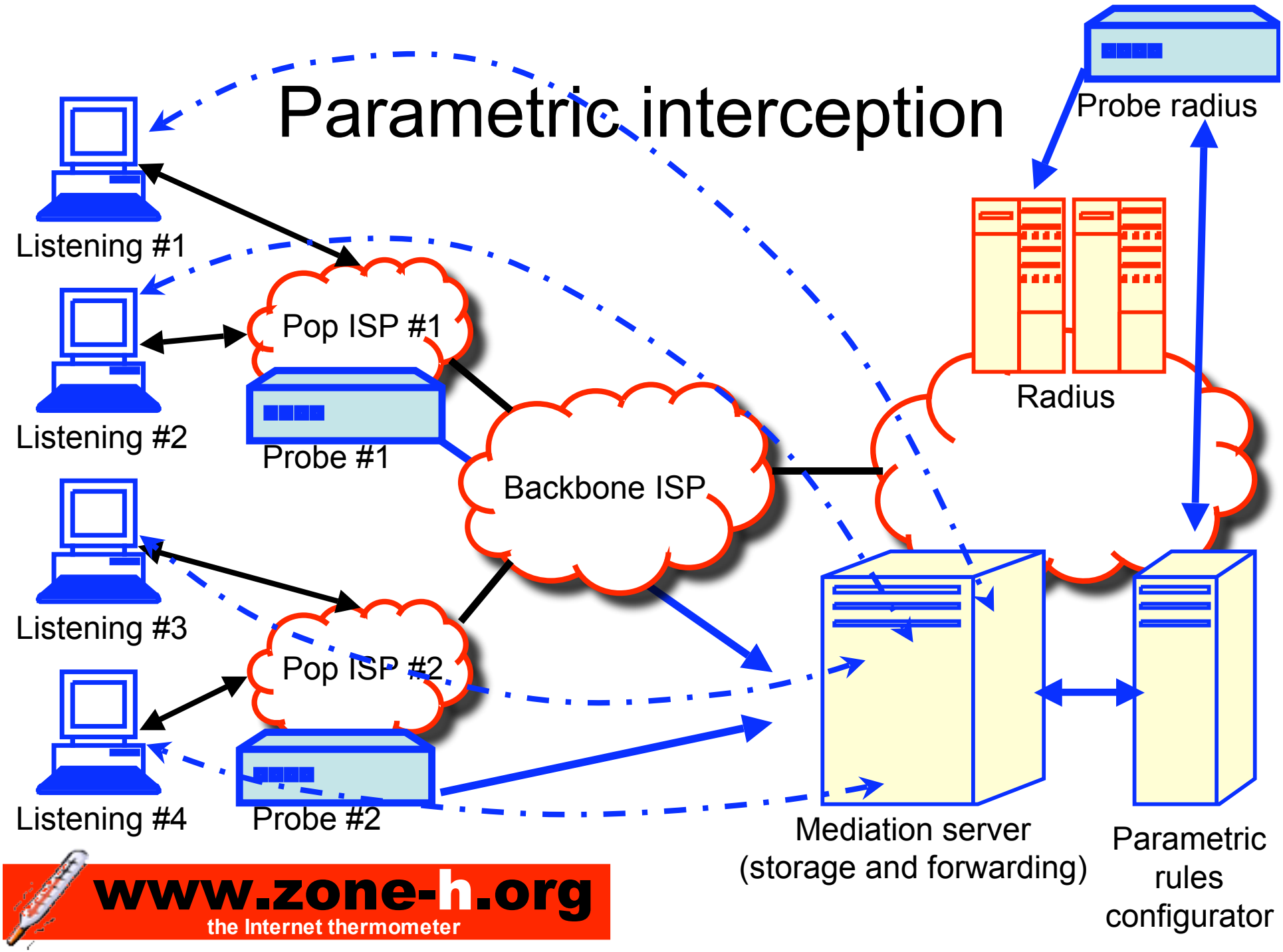
- Protection of public & private critical ICT infrastructures
- Reporting e support for analysts
- Support Defense
- Intelligence
- Offensive & employee infiltration capabilities
- State of alert & automatic activation of defense systems conceived for the protection of strategic national & economic infrastructures
- Enemy analysis, counterattack, elaboration & implementation of offensive strategies
- Counterespionage

National Security & Critical Infrastructure Protection

National Critical Infrastructure

- Public Health and Safety
- Emergency Services
- Water Supply and Sewage
- Transports
- Other Government Operations
- Military Command and Control Systems
- Mass media
- Energy, Oil and Gas Control
- Banking and Financing Activities
- Industrial Production

The beginning of data interception used to solve terrorism cases


Parametric interception
Probe radius
Listening #1
Listening #2
Pop ISP #1
Probe #1
Backbone ISP
Radius
Listening #3
Pop ISP #2
Listening #4
Probe #2
Mediation server
(storage and forwarding)
Parametric
rules
configurator
www.zone-h.org
the Internet thermometer

Parametric interception

- Uses and abuses
 - Technology involved
 - Reliability
 - Usability in investigative procedure
 - Legal uses in court cases and judicial use
 - Basic architecture in asymmetric and symmetric deployment (same nation state standpoint)
 - Real cases

Digimetric interception

Digimetric vs. Parametric

- What it is
- Uses and abuses
- Distributed use on asymmetric and symmetric sensored networks

Return-path: <fabio@xxxxxxxxx.com>
Received: from mail.boot.it (unverified [127.0.0.1]) by boot.it
(Rockliffe SMTPRA 6.1.16) with ESMTP id <B0002856784@localhost> for
<roberto@boot.it>;
Fri, 17 Sep 2004 10:43:28 +0200
Date: Fri, 17 Sep 2004 10:42:58 +0200
From: Fabio xxxxxxxxx <fabio@xxxxxxxx.com>
MIME-Version: 1.0
To: roberto preatoni <roberto@boot.it>
Subject: [Fwd: R: R: report]
Mailer: Mozilla 4.75 [en] (Win95; U)
Content-Type: multipart/mixed;

The process of updating investigative procedure based on interception from voice to data: technological aspects and examples of judicial aspects

Injected interception

-Parametric & direct interception are passive instruments that have limits & don't allow for the analysis of encrypted communications.

- Instruments that guarantee privacy protection and/or anonimity are widely available & easy to use eg. Instant Messaging on SSL; VoIP solutions protected by AeS (eg. SKYPE); there are also systems that allow anonymous file exchange (MUTE) o messaging (Freenet or Entropy).
- - Basic technology
  - When to use it
  - Usability in investigative procedure
  - Can it be detected?
  - Real cases

Injected interception revealed

Intervene on the source

What are the advantages?

- The possibility of having direct access to all the data that the target computer accesses, independent of the means of data transport (physical of telematic).
- The possibility of tracing the target's IP address directly or by reverse connection techniques.

What type of data can be accessed?

- Complete access to all protected data sent on network channels
- All data that DON'T normally transit on the network (USB keys, CDRoms, etc.).
- Access to crypto instruments and keys that allow to decipher the relevant data
  - **Direct access to encrypted physical disks or logical volumes**
- Audio/Video interception, if a microphone and/or webcam are present on the pc
  - Ie. SUB7 trojan

When to Use Injected Interception

- When the subject is able to protect its communications
- When a constant & punctual monitoring of a subject's activity is necessary
- When it isn't physically possible to do environmental interception with traditional methods
- When the subject has an elevated mobility (e.g. notebook)
- When it's not physically possible to access the target's resources

Usability in Investigative Procedures

Forensics know that guaranteeing that all confiscated media & data remain unmodified at the time of analysis, is of paramount importance.

Controversy:

- inserting an external injected agent, modifies the media both physically & logically with its *Install* function
- who inputs the surveillance SW has the same privileges as the monitored subject

Privacy vs. Security

- Formal procedures for requesting the interception;
- Univocal agents, guaranteed by digital signatures & encrypted time stamping;
- Non repudiable auditing of the operations that are managed manually or automatically by the agent;
- Possibility of recreating the agent's assembly process from the source code to the generation of the univocal executable.

Can the Agent be Uncovered?

It depends on the motivation & the know-how used in the attack and the defence.

In general, an agent can be discovered if the network to which the target pc connected is correctly monitored

Therefore, the greatest effort must be funneled into reaching an extremely high technical complexity in the *functions* of:

- Hiding
- Camouflage
- Autodestruct
- Non-reverse trace back

Virus Technology at the Service of Justice: an Overview

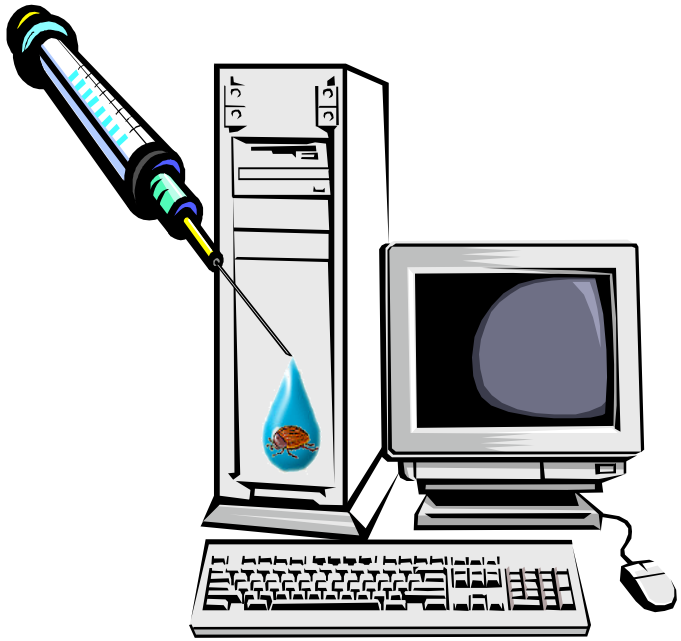
How do you inject an agent into the interested party's computer?

The means are many but the ways to be considered are principally:

Technology

Social Engineering

Separately or in tandem



Trojans

- Usability in investigative procedures
- Potentiality in sensored networks
- Trojan planning and development
- Real cases
- Usability of Trojans in Investigative Procedures

Potentiality in Sensored Networks

- Integration with parametric interception infrastructure
- Anonymity of Agent Communication through *destination IP spoofing* (e.g. Mailing of a letter to a nonexistent address. If we control the central post office exchange, we will be able to intercept and retrieve the letter and any other mail sent to the fictitious address.)

Trojan planning and development

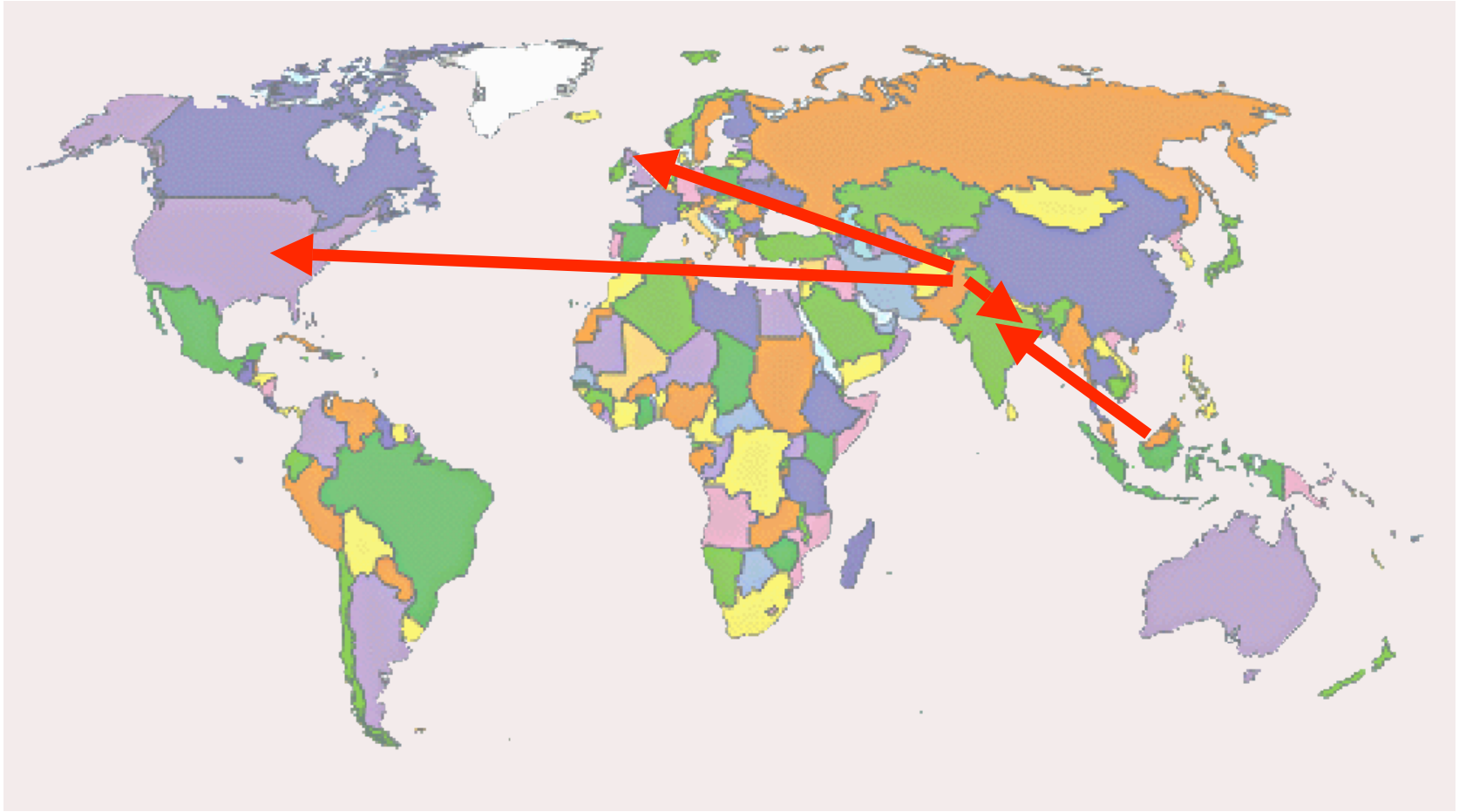
- A lot of trojans are available on the net
- Many trojan coders privately sell releases of their trojans that are not detectable by antivirus programs for less than 100-200 USD

- Trojans available on the Internet are not a good choice because:
  - They are undetectable by antivirus programs but are detectable by humans
  - Made by script kiddies (no design, bad source code)
  - Not so paranoid
    - No encrypted communication
    - No polymorphic self-encryption
    - No self-destruction capabilities
  - Not written for usage in formal investigative procedures
- Trojans used for intelligence must be written, tested and approved with a formal development approach.
- Real cases

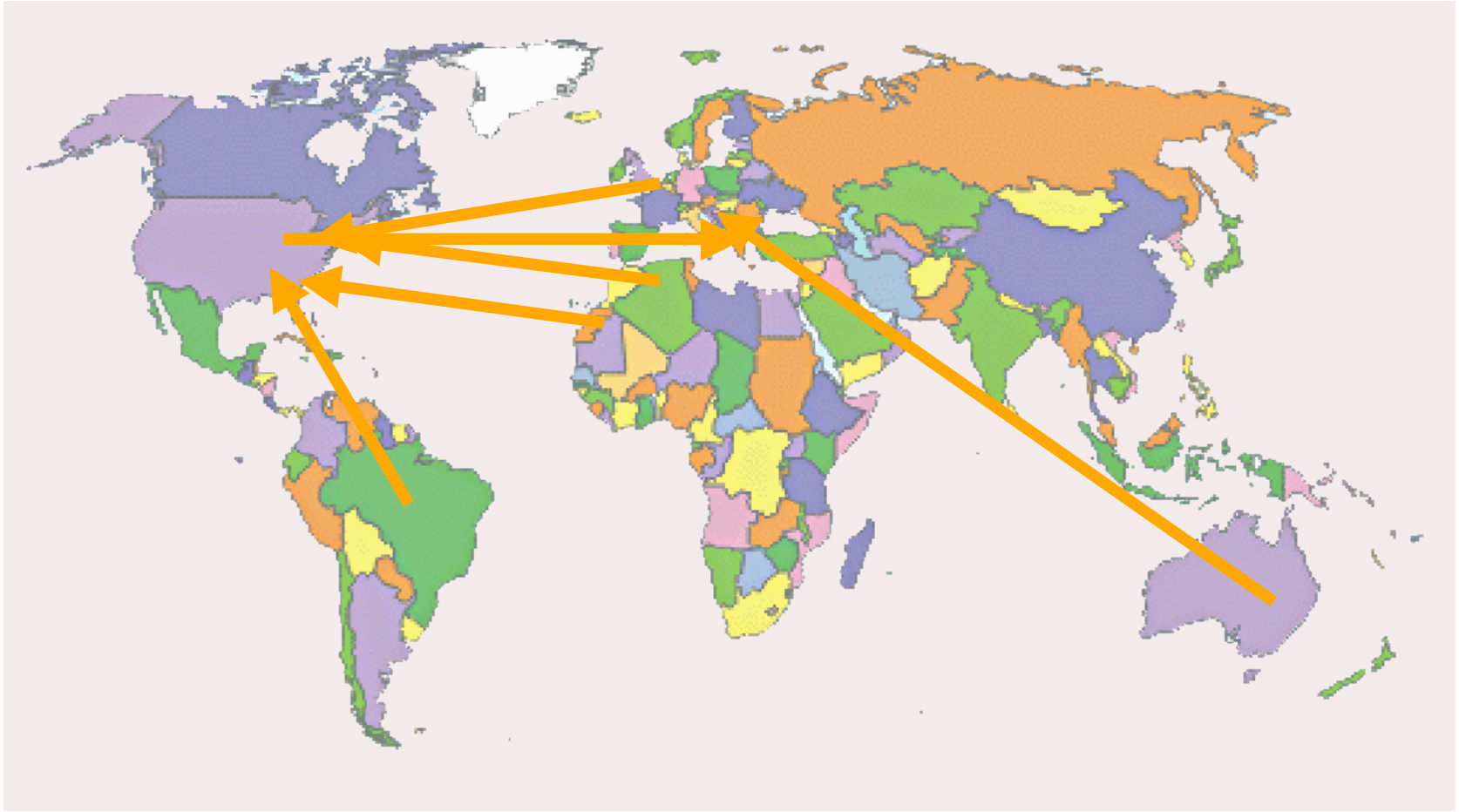
Cyber attacks : an abstract built on Zone-H's experience

www.zone-h.org

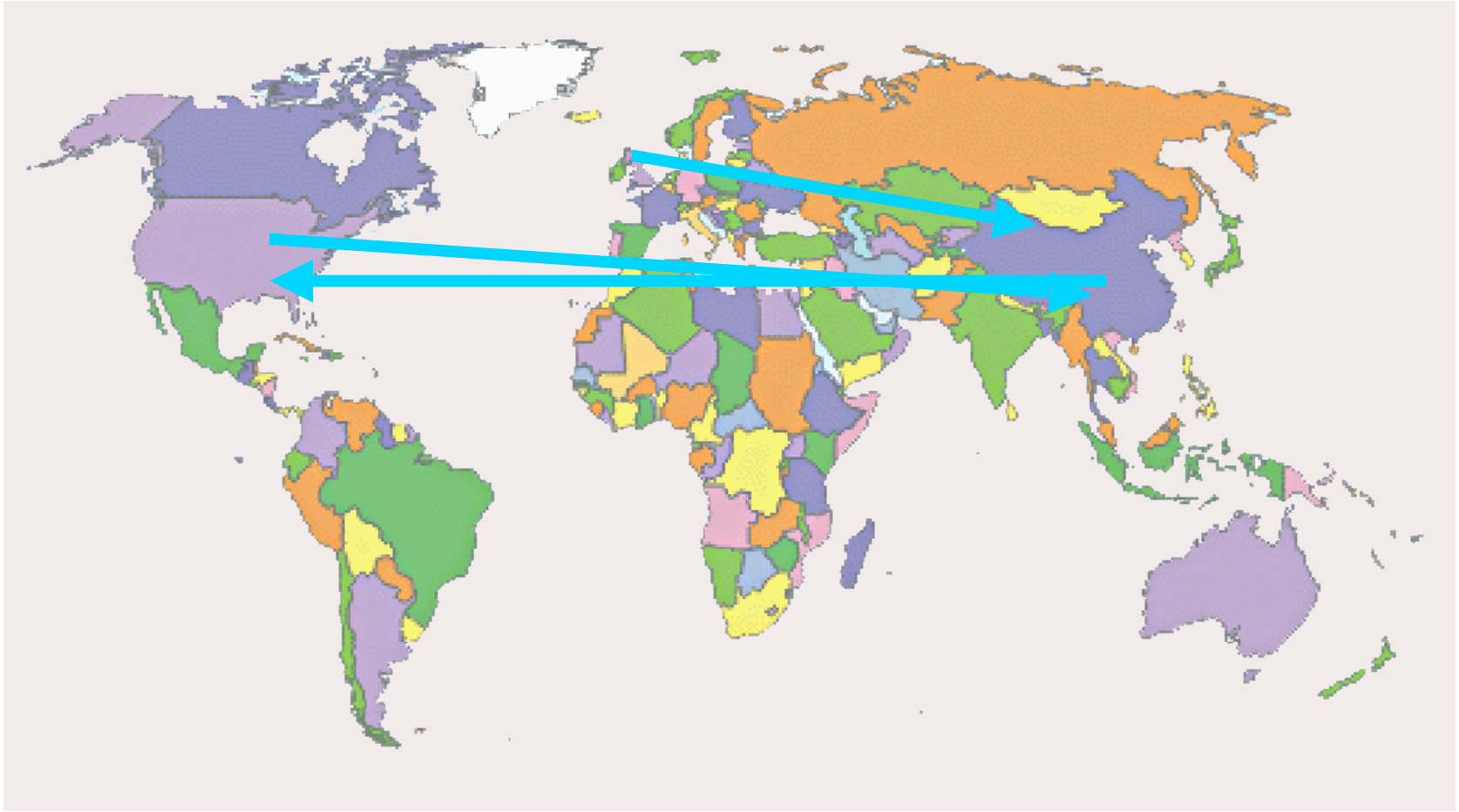
the Internet thermometer



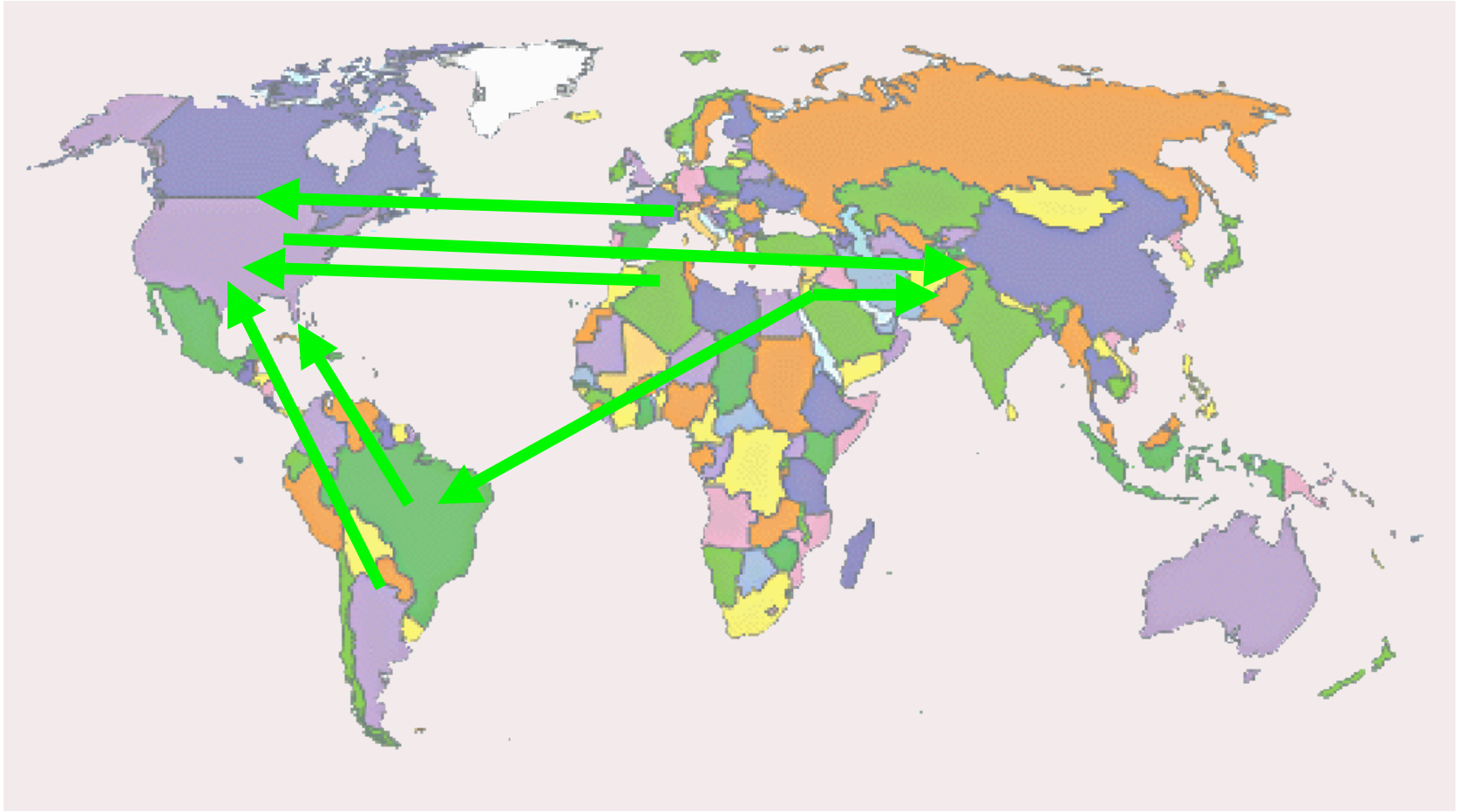
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related



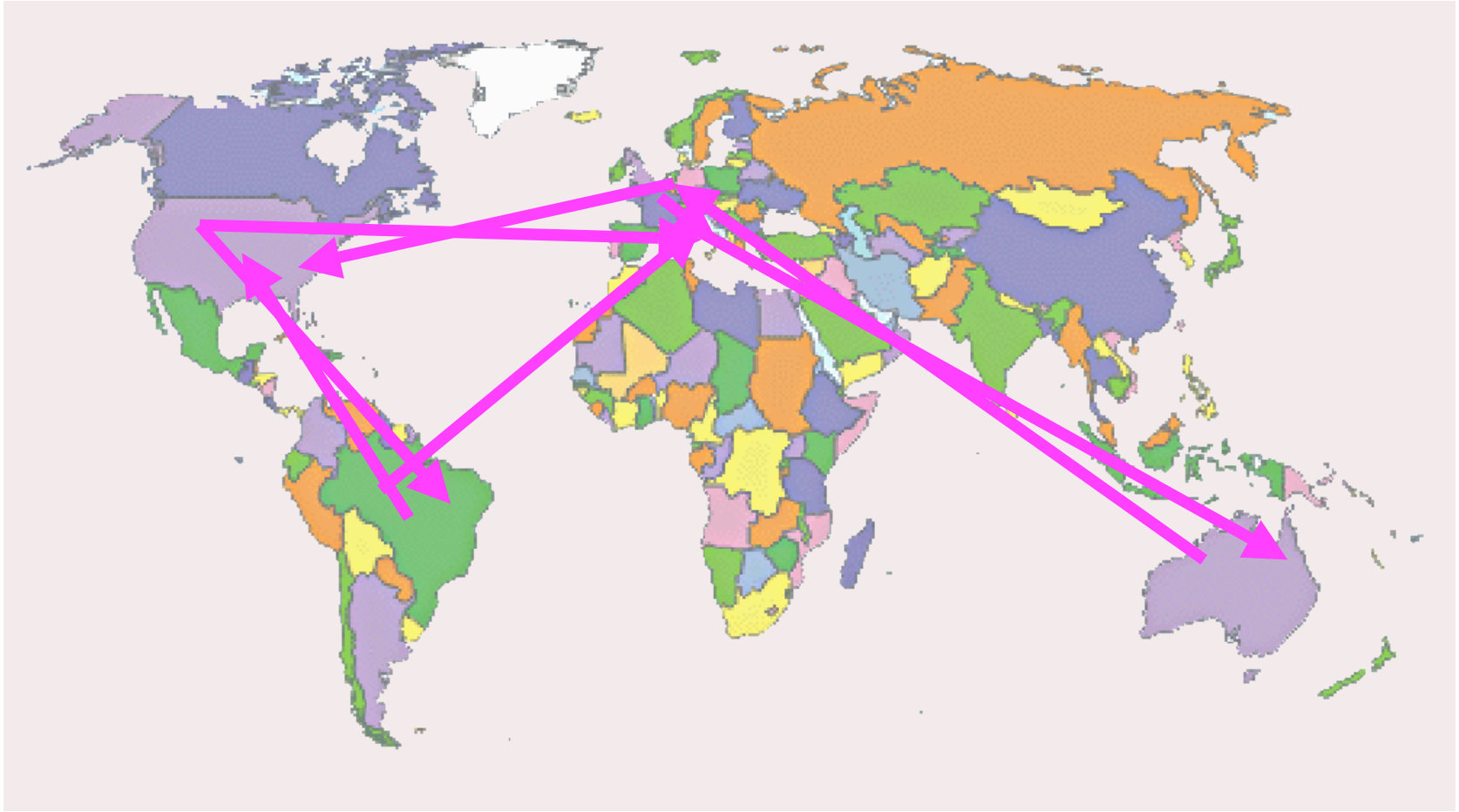
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related



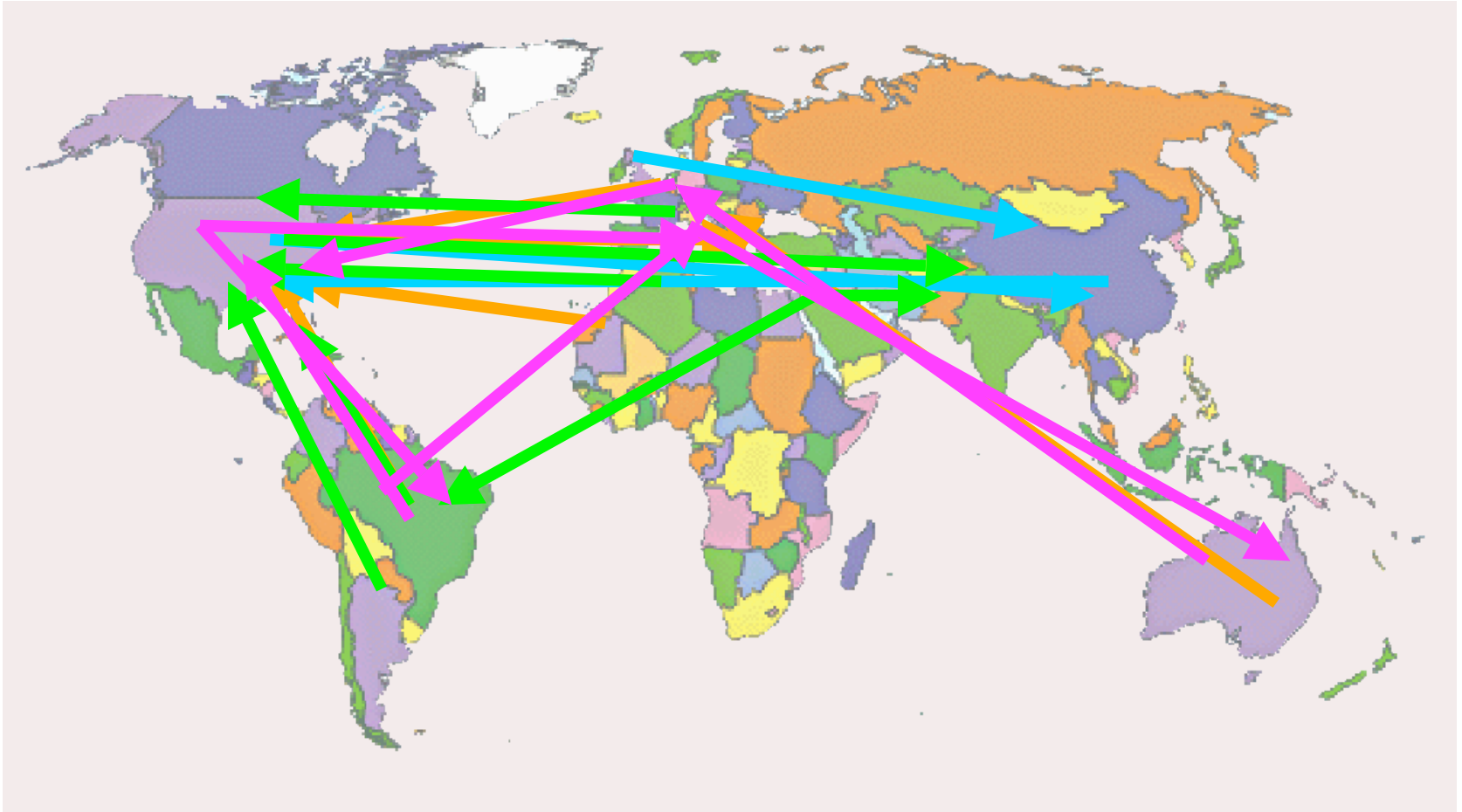
CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related



CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related



CYBERFIGHTS
Kashmir related
Iraq war related
Code red release related
Palestine-Israel related
No-Global related



CYBERFIGHTS

Kashmir related

Iraq war related

Code red release related

Palestine-Israel related

No-Global related

CYBER-ATTACKS ARE CONVENIENT BECAUSE:

- Lack of IT laws
- Lack of L.E. international cooperation
- ISPs are non-transparent (privacy law)

CYBER-ATTACKS ARE CONVENIENT BECAUSE:

- General lack of security
- No need to protest on streets
- No direct confrontation with L.E.

CYBER-ATTACKS WILL NEVER STOP BECAUSE:

- Inherent slowness of the Institutions
- The Internet is getting more complicated
- Software producers are facing a market challenge

www.zone-h.org
the Internet thermometer

THE NEW EXPRESSIONS OF THE ASYMMETRIC CYBERWAR

COMMAND & CONTROL

INFORMATION GATHERING

ON ENEMY'S TARGETS

MEDIA MANAGEMENT

PROPAGANDA DIFFUSION

"TAX FREE" MONEY

RAISING & LAUNDERING

www.zone-h.org

the Internet thermometer

Q&A