RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Eight Cyber Conflicts Which Changed Cyberspace

SESSION ID: STR-F01

Jason Healey

Director of the Cyber Statecraft Initiative
Atlantic Council

@Jason_Healey

Cyber Truisms

Cyber conflict is moving incredibly quickly.

Change is the only constant…

Army Cyber Command/2nd ARMY

Evolving Cyber Threats

Pre-2007 **Cyber "Noise" on Networks**

Present **Potential Limited Disruption to Mission Command**

Next **Potential Destruction… Isolation of Tactical Forces**

Our Mission Command - increasingly reliant on networks – will become more and more at risk

From Army Cyber Command Update,

http://www.afcea.belvoir.org/images/uploaded/AFCEABelvoir_ARCYBERCommandBrief_COLSchilling_22APR12.pdf

Cyber Truisms

Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.

The almost obsessive persistence of serious penetrators is astonishing.

Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations … insulated from risks of internationally embarrassing incidents

The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.

Cyber Truisms

1979 Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.

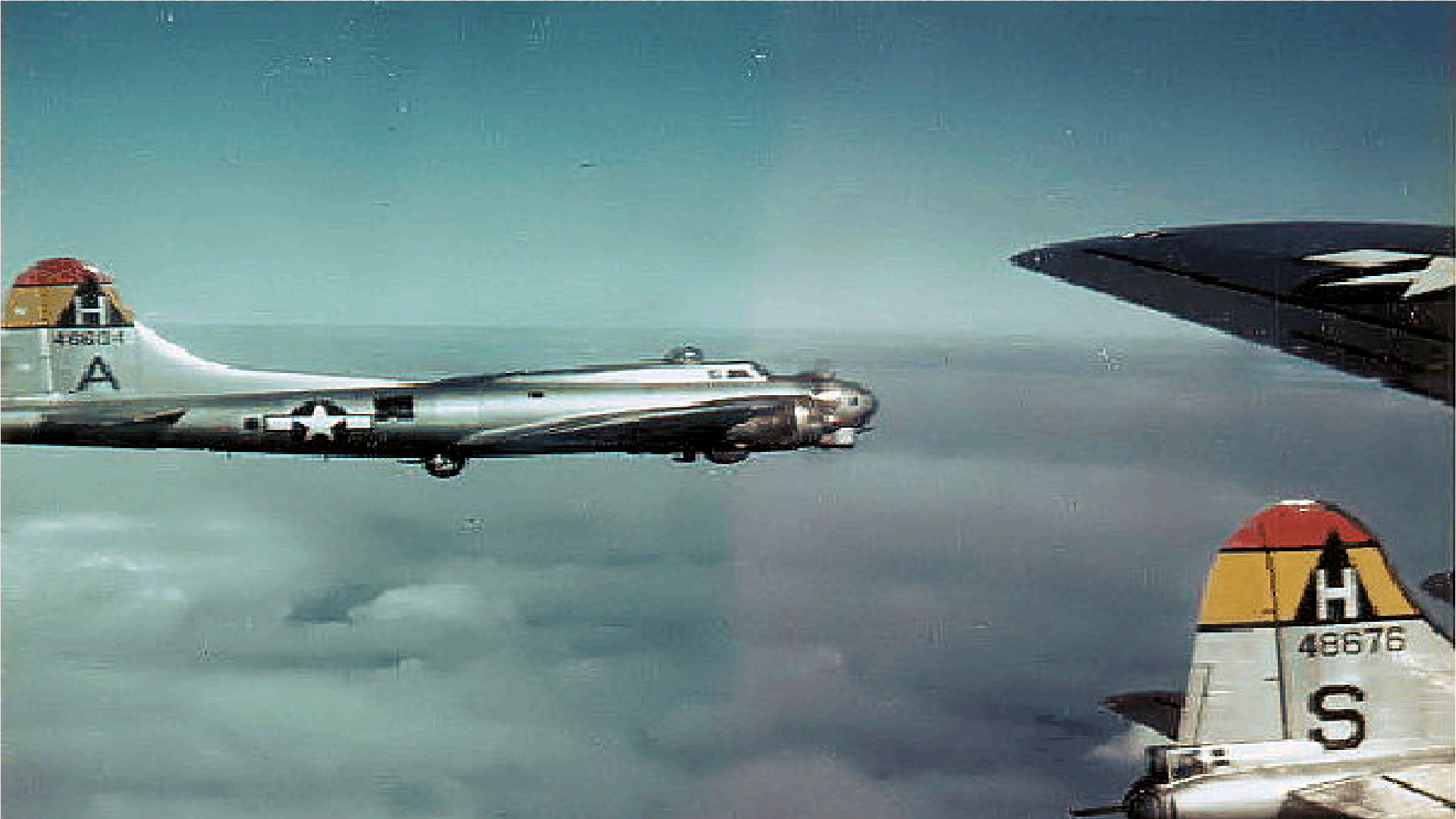
1988 *The almost obsessive persistence of serious penetrators is astonishing.*

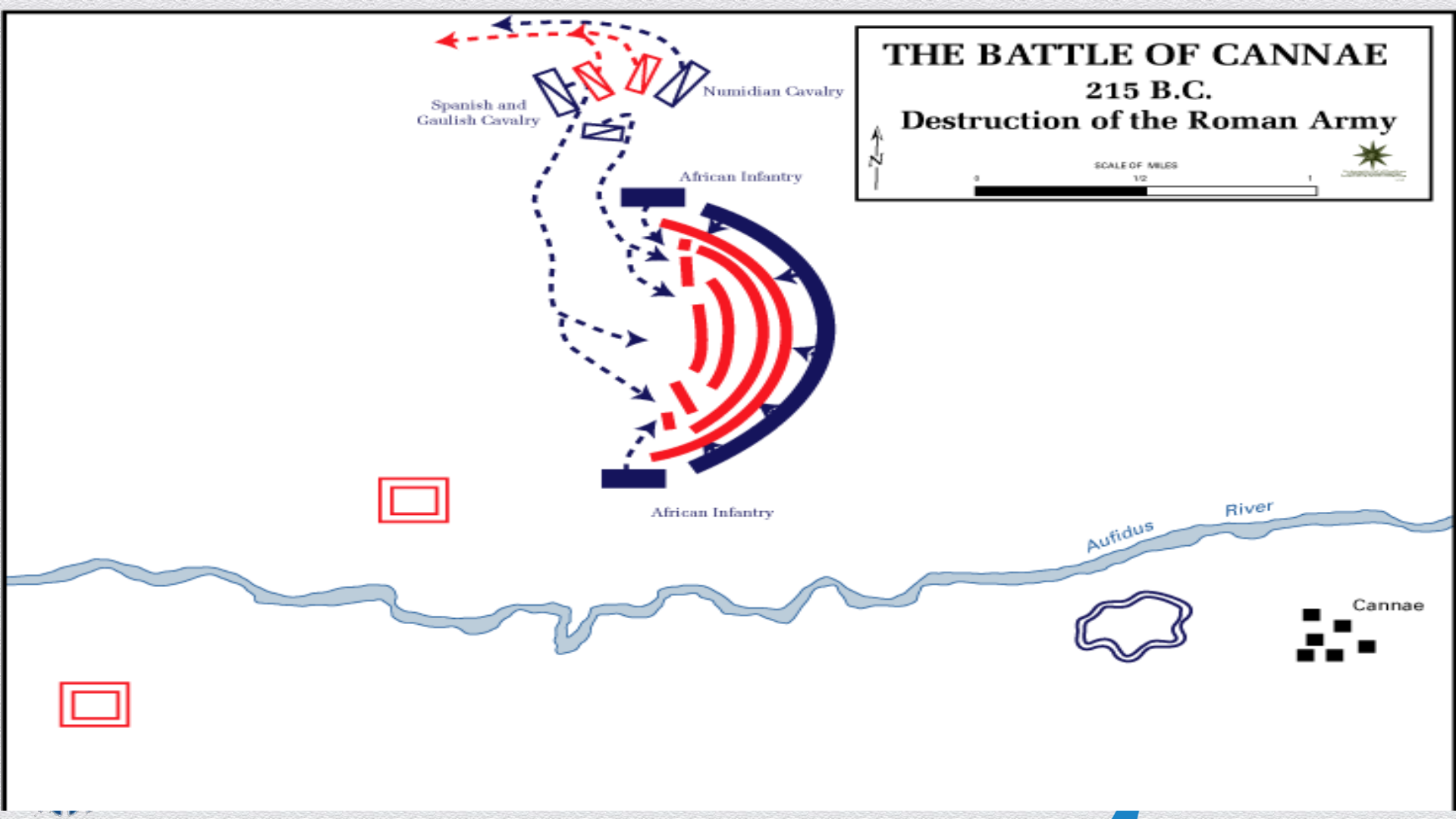
1988 Espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations … insulated from risks of internationally embarrassing incidents

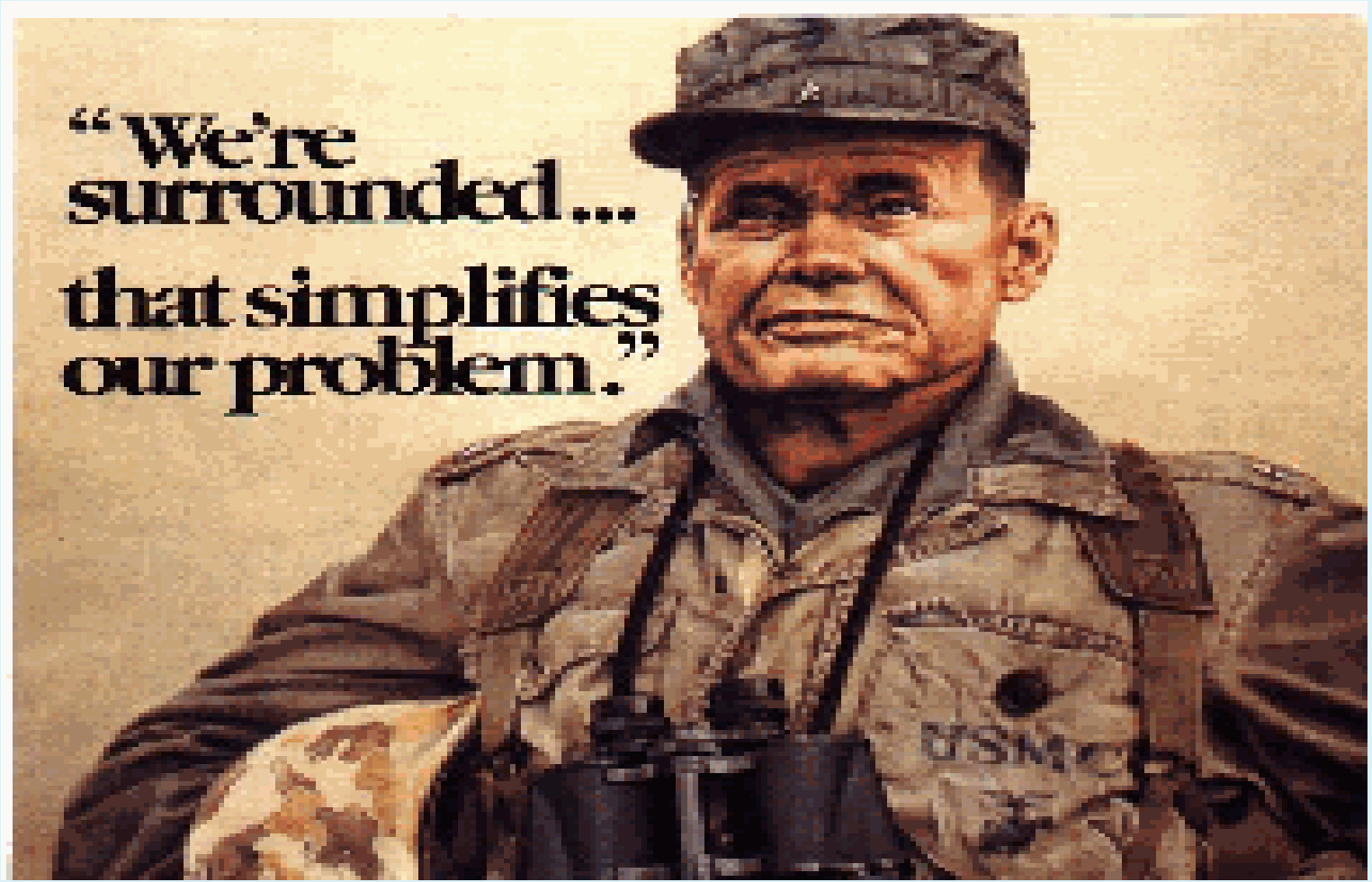
1991 *The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.*

Eight Cyber Conflicts

1. Cuckoo's Egg (1986) – only DoJ paid attention
2. Morris Worm (1988) – Led to first CERT
3. ELIGIBLE RECEIVER and SOLAR SUNRISE (1997, 1998) – JTF-CND
4. MOONLIGHT MAZE (2000+) – Cooperation and coordination
5. Chinese Espionage (2000s) -- Led to billions spent through CNCI
6. Estonia and Georgia (2007, 2008) – Global attention, NATO focus
7. BUCKSHOT YANKEE (2008) – US Cyber Command
8. Stuxnet (2009) – Global attention, possible counterattack on US banks

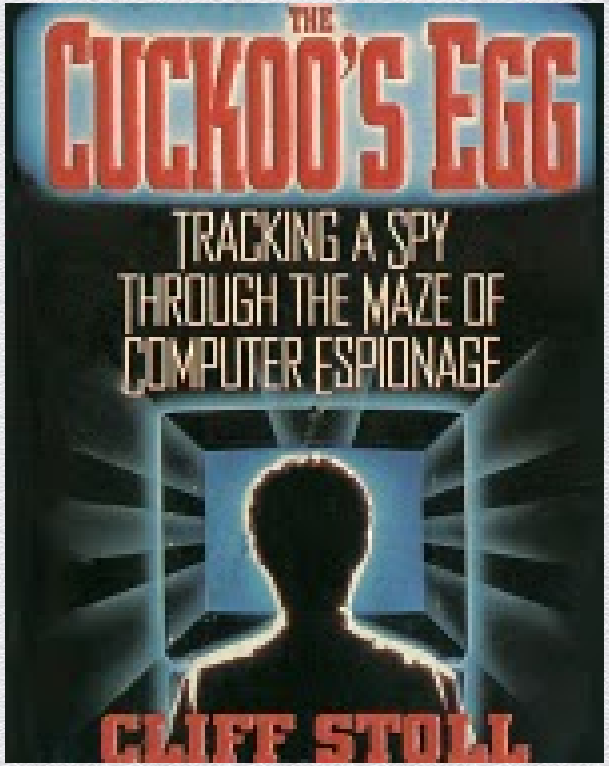

H
A
H
48676
S


THE BATTLE OF CANNAE
215 B.C.
Destruction of the Roman Army
N
SCALE OF MILES
0
1/2
1
Spanish and
Gaulish Cavalry
Numidian Cavalry
African Infantry
African Infantry
Aufidus River
Cannae


"We're surrounded...
that simplifies our problem."
USMC

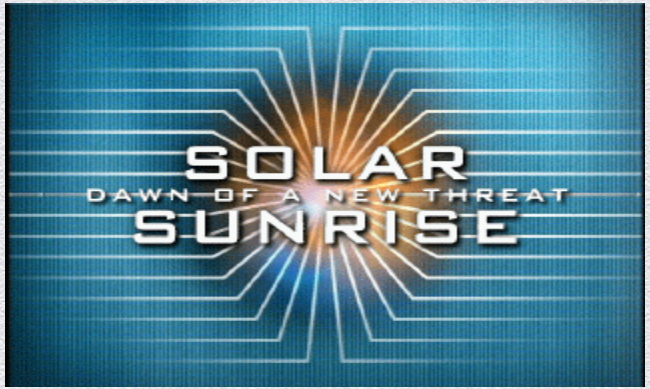
WHAT HAPPENED IN 1986?

Cuckoo's Egg: ~1986



Morris Worm: 1988

ELIGIBLE RECEIVER and SOLAR SUNRISE



MOONLIGHT MAZE: late 1990s, early 2000s

Chinese Espionage: 2000s- Today

Estonia (2007) and Georgia (2008)

BUCKSHOT YANKEE

Stuxnet and US-Iran Covert Conflict: mid-2000s to today

Eight Cyber Conflicts

1. Cuckoo's Egg (1986) – only DoJ paid attention
2. Morris Worm (1988) – Led to first CERT
3. ELIGIBLE RECEIVER and SOLAR SUNRISE (1997, 1998) – JTF-CND
4. MOONLIGHT MAZE (2000+) – Cooperation and coordination
5. Chinese Espionage (2000s) -- Led to billions spent through CNCI
6. Estonia and Georgia (2007, 2008) – Global attention, NATO focus
7. BUCKSHOT YANKEE (2008) – US Cyber Command
8. Stuxnet (2009) – Global attention, possible counterattack on US banks

Top-Level Findings
From Cyber as National Security History

- There is a history and we must learn from it!
  - Dynamics are relatively stable despite change…

Top-Level Findings
From Cyber as National Security History

- There is a history and we must learn from it!
  - Comparison to fighter pilots
- The real impacts of cyber conflicts have been consistently overestimated
  - Cyber Pearl Harbor, no deaths yet! (we think)

Top-Level Findings
From Cyber as National Security History

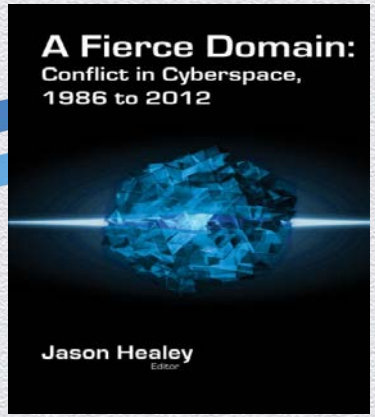
- There is a history and we must learn from it!
- The real impacts of cyber conflicts have been consistently overestimated
- Cyber is more familiar than it seems
  - The *more strategically significant* a cyber conflict is, the *more similar* it is to conflicts on the land, in the air, and on the sea—with one critical exception
  - With implications for
    - Speed of Response
    - Attribution
    - Warning
    - Deterrence

@Jason_Healey

QUESTIONS?

Cyber Statecraft Initiative

- International conflict, competition and cooperation in cyberspace
- Publications (all at our website, acus.org)
- Public and Private Events



- There is a history and we must learn from it!
- The real impacts of cyber conflicts have been consistently overestimated
- Cyber is more familiar than it seems
  - The *more strategically significant* a cyber conflict is, the *more similar* it is to conflicts on the land, in the air, and on the sea—with one critical exception