



DECEMBER 10 - 13, 2012
EMIRATES PALACE | UNITED ARAB EMIRATES

In partnership with:



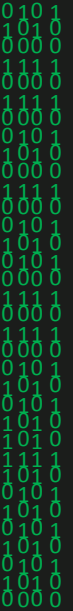
Supported by:



Lessons from History of Cyber Conflict

Jason Healey

Atlantic Council





More Truisms

1979

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

1988

The almost obsessive persistence of serious penetrators is astonishing. [Cliff Stoll]

1988

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

1991

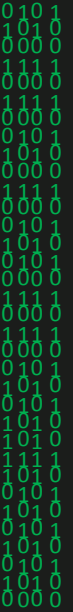
The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems. [Computers at Risk report]

0101
1010
0000
1111
0000
1111
0101
1010
0000
1111
0101
0000
1111
0000
1111
0101
1010
1010
1010
1111
1010
0101
1010
1010
1010
1010
1010
0000



No, No, No:
The Problems I Face Are Different!

The only cyberwar raging is inside the U.S. government where Washington lawyers and policymakers, military leaders, and official hackers battle over the value and legality of network attack.



1000

The only cyberwar raging is inside the U.S. government where Washington lawyers and policymakers, military leaders, and official hackers battle over the value and legality of network attack.

blackhat Sorry...
ABU DHABI 2012



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**

[UNCLASSIFIED]

“Second to None!”



DECEMBER 10 - 13, 2012
EMIRATES PALACE | UNITED ARAB EMIRATES

In partnership with:



Supported by:



THE MAJOR CYBER CONFLICTS



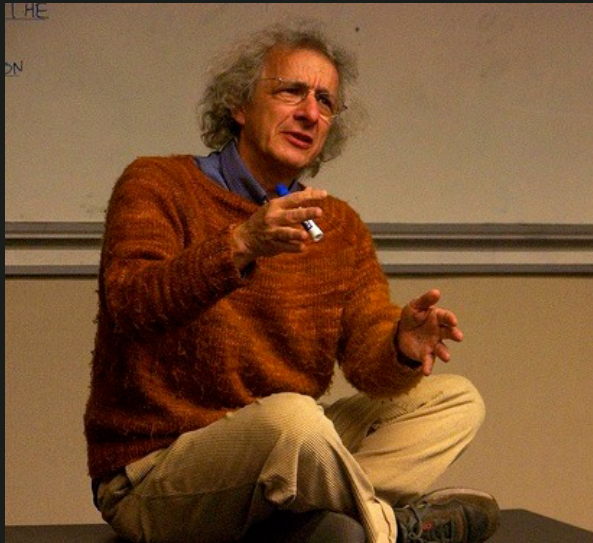
Three Phases

(For the US Anyhow...)

- Realization: to 1998
- Takeoff: 1998 to 2003
- Mobilization: 2003 to Today

The First Cyber Conflict

We Think...

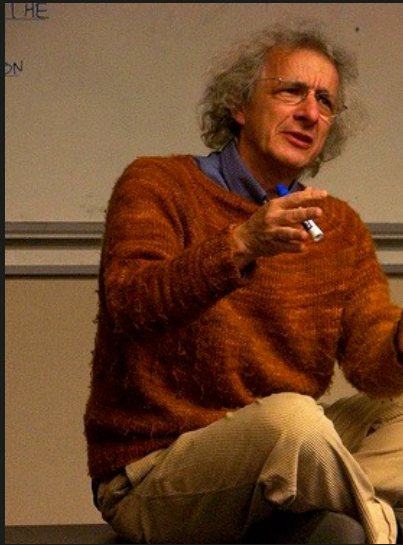


THE CUCKOO'S EGG

TRACKING A SPY
THROUGH THE MAZE OF
COMPUTER ESPIONAGE



CLIFF STOLL



Cyber “Wake Up Calls” for the US



1. **Morris Worm** (1988) – Led to first CERT



2. **ELIGIBLE RECEIVER** and **SOLAR SUNRISE** (1997, 1998) – JTF-CND



3. **MOONLIGHT MAZE** (2000+) – Cooperation and coordination



4. **Chinese Espionage** (2000s) -- Led to billions spent through CNCI



5. **Estonia** and **Georgia** (2007, 2008) – Global attention, NATO focus



6. **BUCKSHOT YANKEE** (2008) – US Cyber Command



7. **Stuxnet** (2009) – Global attention, possible counterattack on US banks



blackhat[®]
ABU DHABI 2012

DECEMBER 10 - 13, 2012
EMIRATES PALACE | UNITED ARAB EMIRATES

In partnership with:

TRA
تجارة
TELECOMMUNICATIONS REGULATORY AUTHORITY

KHALIFA
UNIVERSITY

Supported by:

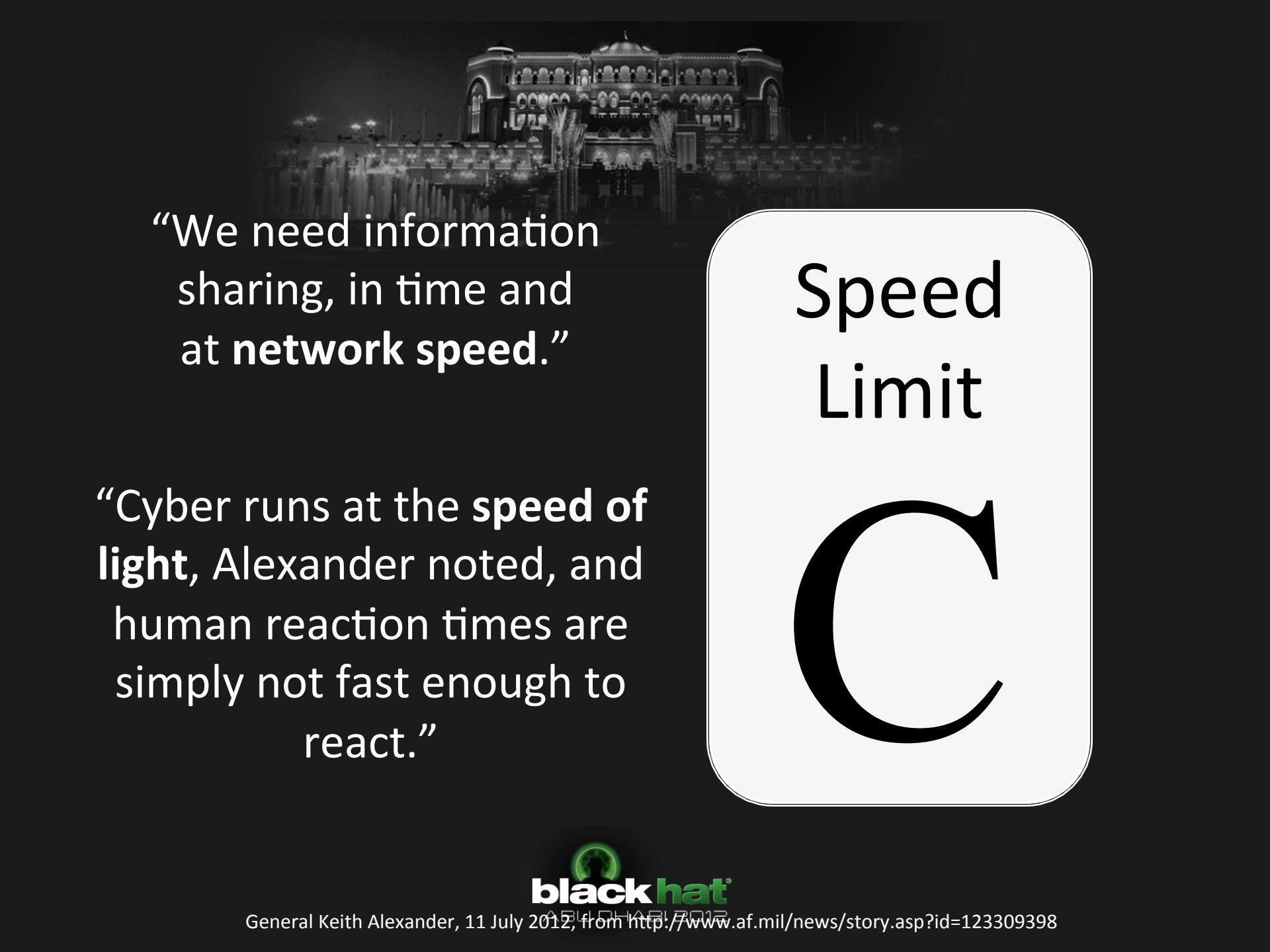
CERT
Computer
Emergency
Response
Team

LESSONS THAT MATTER *TODAY*



Top-Level Findings

1. Cyber conflict has changed only gradually over time, making historical lessons especially relevant (though usually ignored).
2. The probability and consequence of disruptive cyber conflicts has been hyped while the impact of cyber espionage is consistently underappreciated.
3. The common understanding of strategically important cyber conflicts is so distant from their fundamental historical nature as to constitute myth.



“We need information sharing, in time and at **network speed**.”

“Cyber runs at the **speed of light**, Alexander noted, and human reaction times are simply not fast enough to react.”


Speed
Limit

C





- When is this NOT true?
- Why do we have to get it right?



“We need information sharing, in time and at **network speed**.”

“Cyber runs at the **speed of light**, Alexander noted, and human reaction times are simply not fast enough to react.”

Speed
Limit
C

General Keith Alexander, 11 July 2012, from <http://www.afmilj/news/story.asp?id=123309398>



Deterrence is difficult because ... “For someone with the right brainpower and the right cyber abilities, a cheap laptop and Internet connection is all it takes to be a major player in the domain”



- When is this NOT true?
- Why do we have to get this right?



Deterrence is difficult because ... “For someone with the right brainpower and the right cyber abilities, a cheap laptop and Internet connection is all it takes to be a major player in the domain”

Image from American Public Media,

<http://www.marketplace.org/topics/tech/computer-hackers-gather-las-vegas-convention>

General William Shelton, Commander Air Force Space Command, remarks at Air Force Association, CyberFutures Conference, 22 March 2012

Early warning against
and tracing of cyber
attacks is **all but**
impossible, so the most
crucial element of a
deterrence strategy
—“retaliation”—cannot
even be considered.

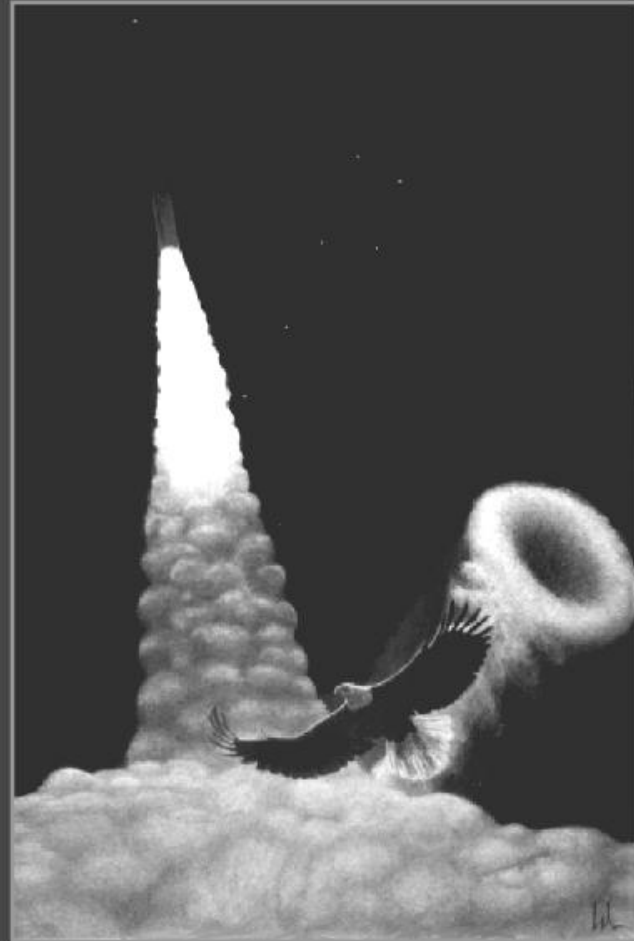


Image from the Bookcliff Group, <http://www.bookcliff-group.com/>

East-West Institute, Global Cyber Deterrence, <http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf>

ABU DHABI 2012



- When is this NOT true?
- Why do we have to get this right?

Early warning against and tracing of cyber attacks is **all but impossible**, so the most crucial element of a deterrence strategy—“retaliation”—cannot even be considered.

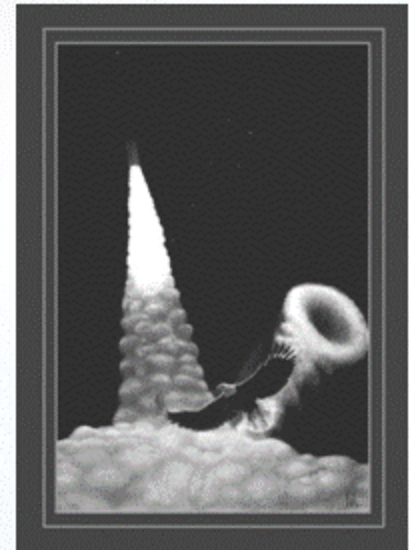


Image from the Bookcliff Group, <http://www.bookcliff-group.com/>

East-West Institute, Global Cyber Deterrence, <http://www.eui.int/system/files/CyberDeterrenceWeb.pdf>

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

Twitter: @Jason_Healey