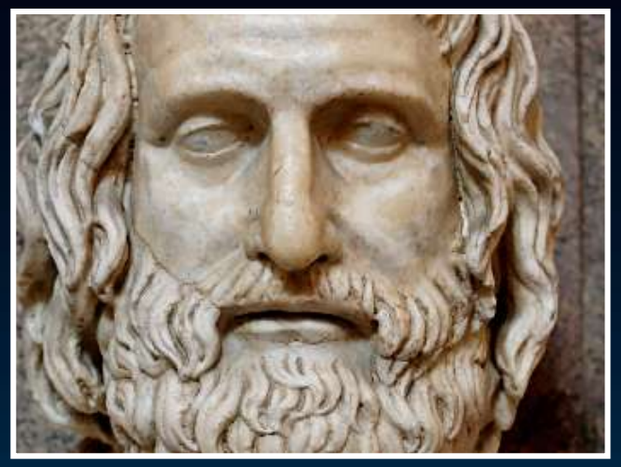
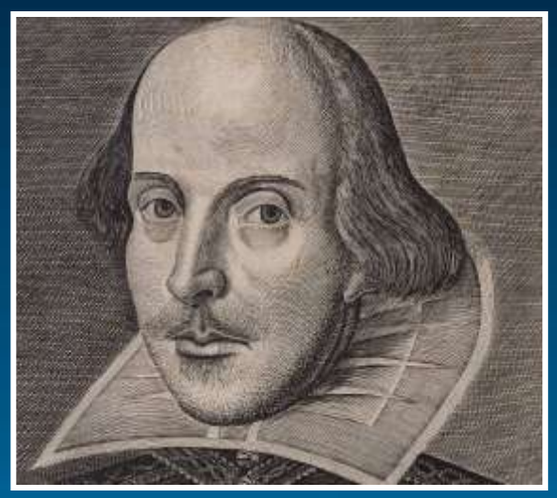
Is the Pen still mightier than the Sword?

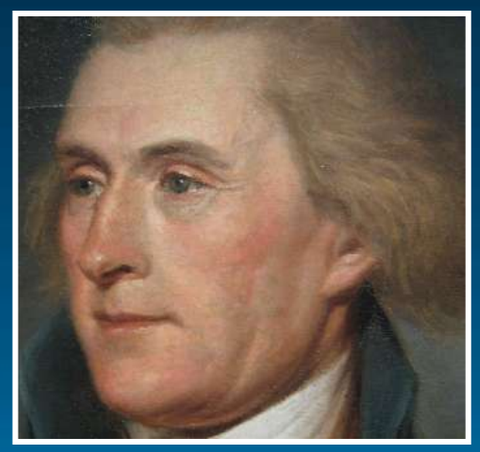
Kenneth Geers

NCIS Cyber Subject Matter Expert

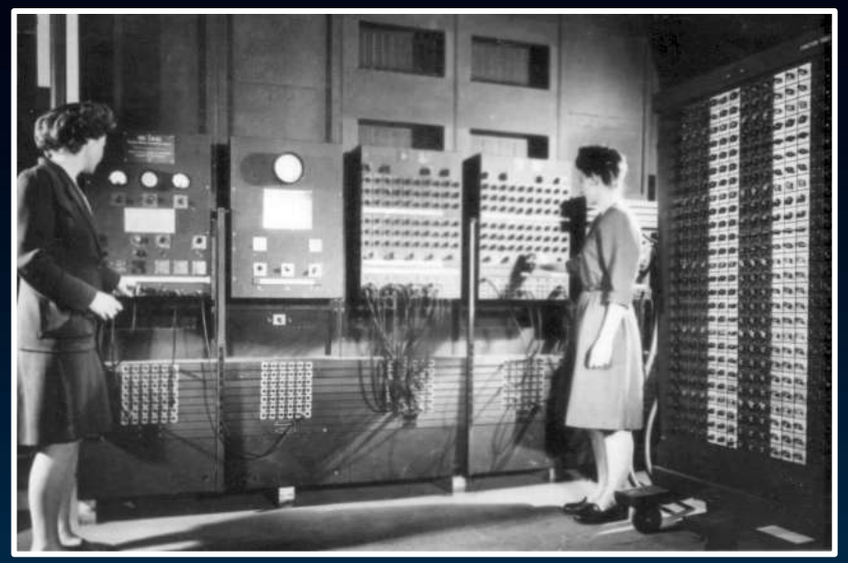
Reconsidering an Adage

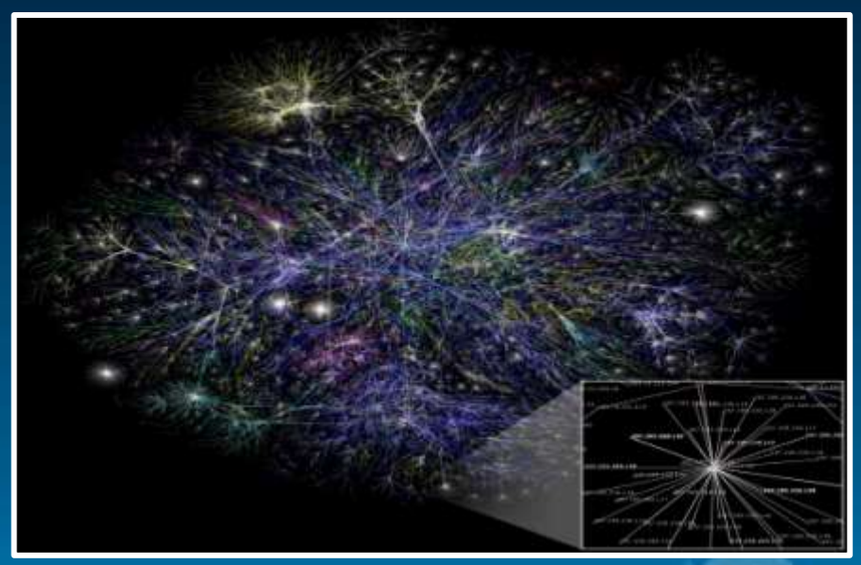






Information Revolution





Long-range weapons

Syria 1982

"…cut all telephone and road communication with the city."

"Exact details ... Incomplete. No reporters"

Syria 2011

Syria 2007

NATO on Cyber

- 1999 Washington: no mention
- 2002 Prague: “strengthen ... to defend”
- 2004 Istanbul: no mention
- 2006 Riga: “develop … capability”
- 2008 Bucharest: “cyber aggression … assist Allies”
- 2010 Lisbon: “threaten ... prosperity, security and stability”

Art of Cyber War

The new Pen


Ne Mutlu Turkum Diyene


The Chinese hackers advoc
We merely make the safe ex
Invades the Person
江南剑书生, FruNyIsE, Shnog , LnSan


G.H.S.
GREEK HACKING SCENE


Øwned by cDc
cDc
www.cultdeadcow.com

The last shall be first

Whom do you trust?

Cell

theSun
TELLING IT AS IT IS

Xinhua
中国新闻

Springer

FOX NEWS Channel

New York Times

FOREIGN AFFAIRS

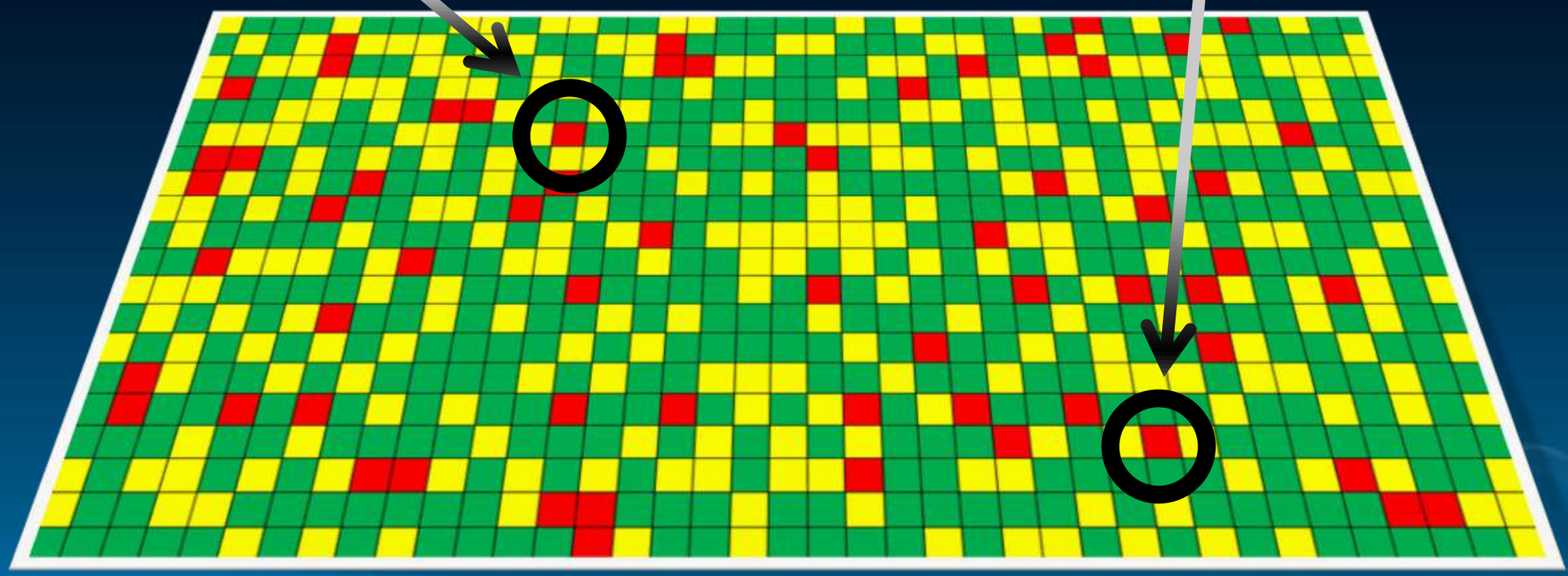
The Economist

ПРАВДА

Outliers

Miyazaki 8.299

Van Damme 4.805



IMDb

Controversy over Sources

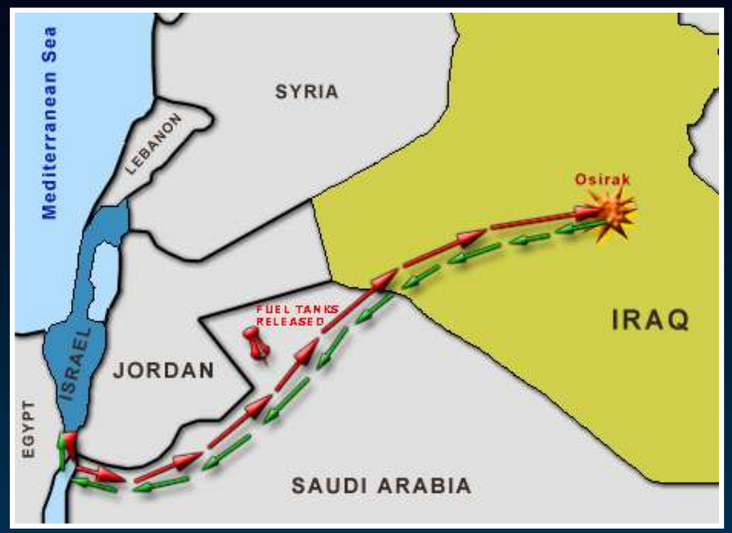
“Consorting with Zimbabwe's sworn enemy ... where the gates of hell are … can only make one smell a rat … investigate cloak-and-dagger meetings … take decisive disciplinary action”

– Harassment, intimidation, torture
– No perpetrators brought to justice

The new Sword

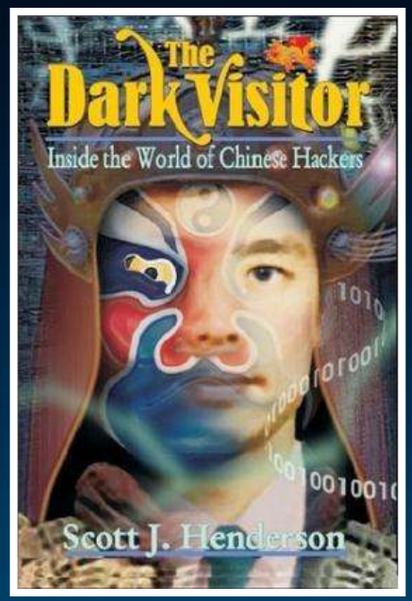
```
#include <windows.h>
#include <defs.h>


//-------------------------------------------------------------------------
// Data declarations

extern int dword_10001CD0[8]; // weak
extern char *off_10001CF2; // weak
extern char byte_10001CF9[3]; // weak
extern char byte_10001DC7; // weak
extern int dword_1000215A; // weak
extern int dword_10002162; // weak
extern int dword_10002166; // weak
extern int dword_1000216A; // weak
extern int dword_1000216E; // weak
extern int dword_10002172; // weak
extern int (__stdcall *dword_10002176)(_DWORD); // weak
extern int dword_1000217A; // weak
extern int dword_1000217E; // weak
extern int dword_10002182; // weak
extern int (__stdcall *dword_10002186)(_DWORD, _DWORD, _DWORD, _DW
extern int (__stdcall *dword_1000218A)(_DWORD, _DWORD, _DWORD, _DW
weak
extern int dword_1000218E; // weak
extern int dword_10002192; // weak
extern int dword_10002196; // weak
extern int (__stdcall *dword_1000219A)(_DWORD); // weak
extern _UNKNOWN unk_10003068; // weak
```

Context


Mediterranean Sea
SYRIA
LEBANON
ISRAEL
JORDAN
EGYPT
IRAQ
Osirak
FUEL TANKS RELEASED
SAUDI ARABIA


421

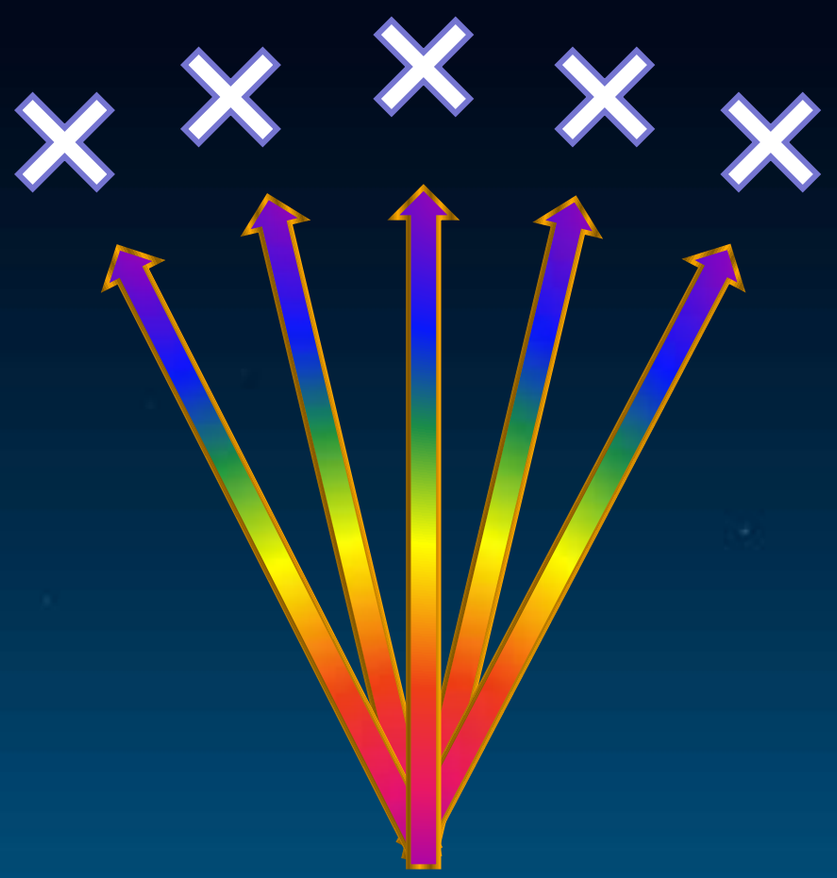
The First Cyber War(s)



Military Grade

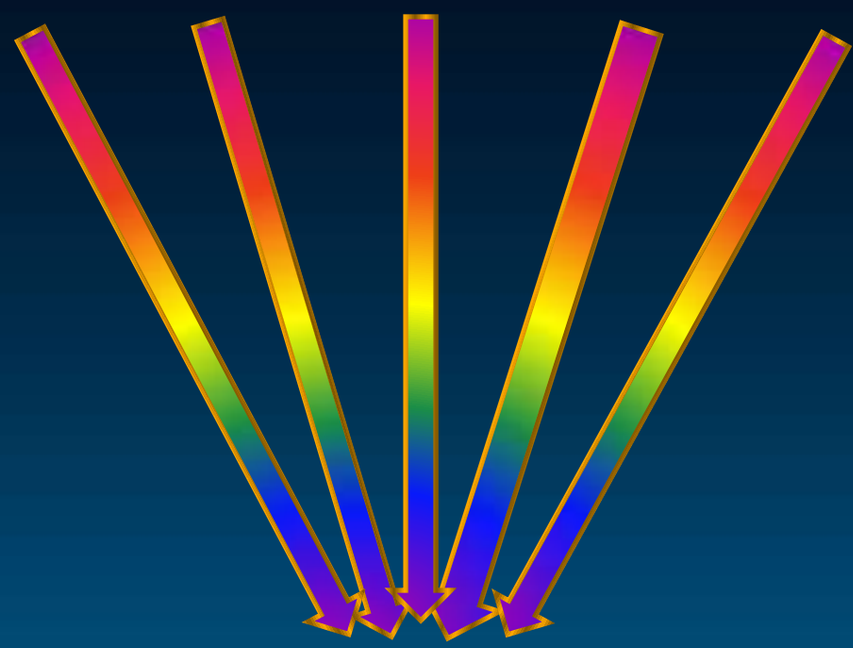
1. Infrastructure test
2. 1st PLC rootkit
3. Multiple 0-days
4. Global operation
5. Stolen certificates
6. Half-megabyte
7. Multiple languages
8. AV evasion
9. Remote C2
10. P2P updates

High Value Target



Slammer, Blaster, Sobig

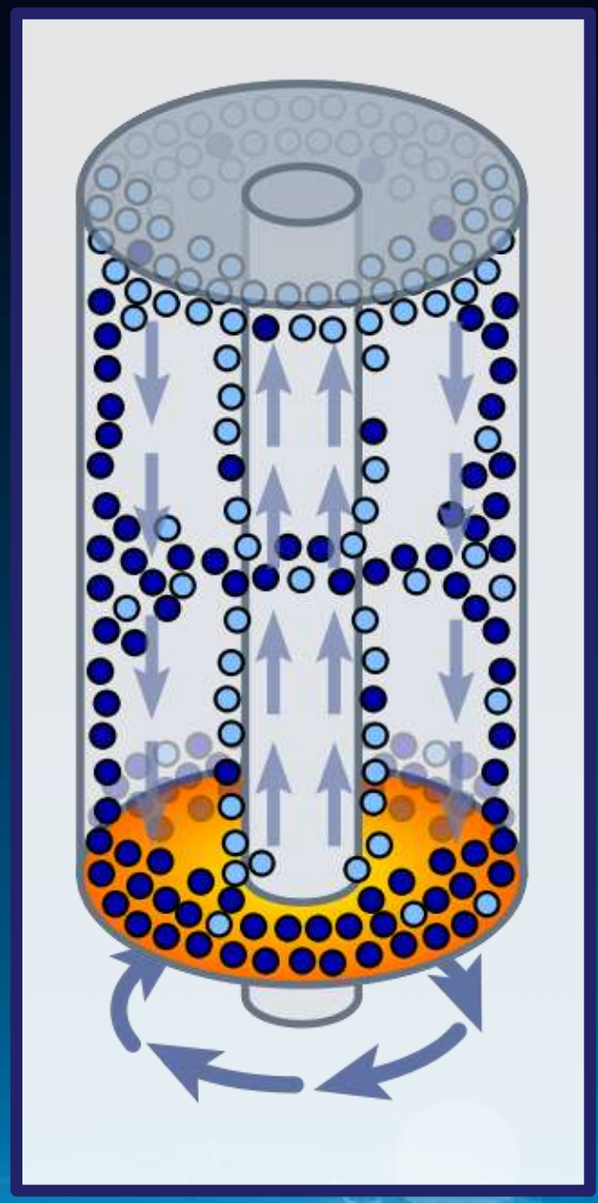
Stuxnet



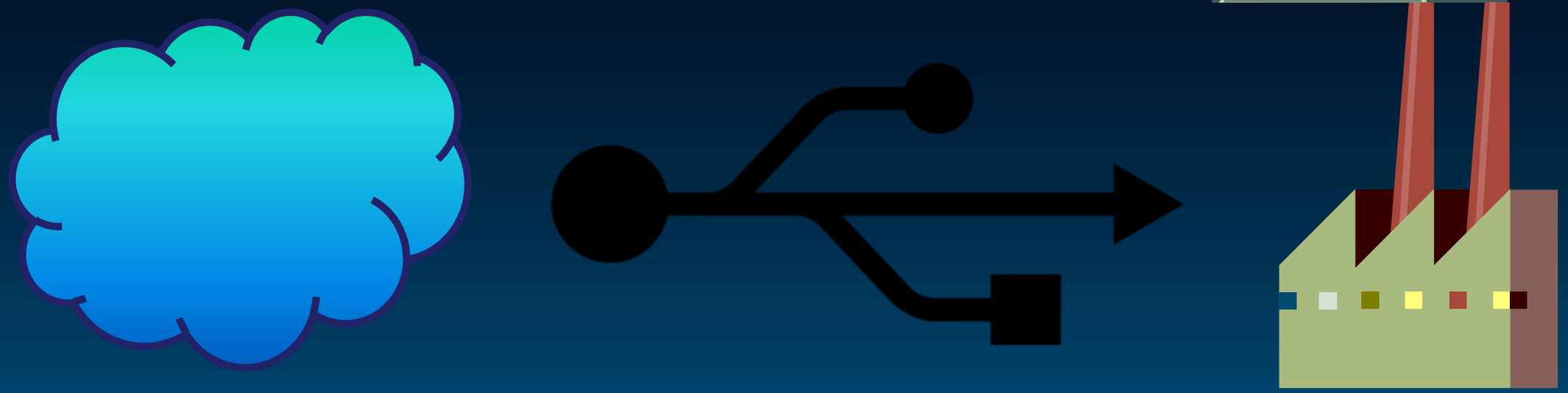
Physical Damage

Siemens PLC

Target centrifuge



The Air Gap



Information Space

Wikileaks

Attack Space

Stuxnet

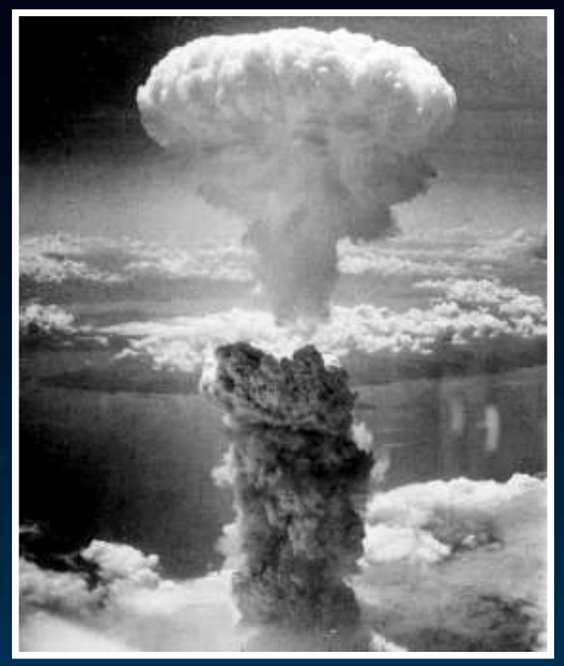
Pen or Sword?

- Wikileaks
  - Important but part of historical trend
  - Now difficult to shape information space
- Stuxnet
  - First of its kind / new era of conflict
  - *NYT*: best counter-proliferation op in Iran
  - IAEA inspector: 2,000 Natanz centrifuges broken

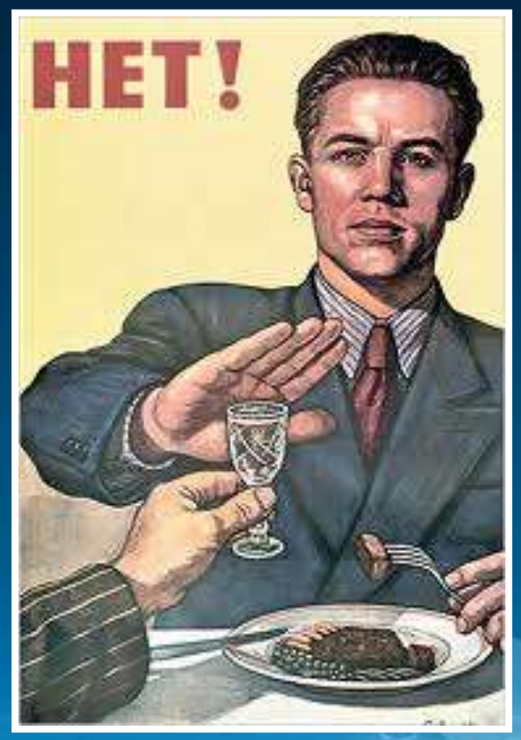
Implications for Infrastructure

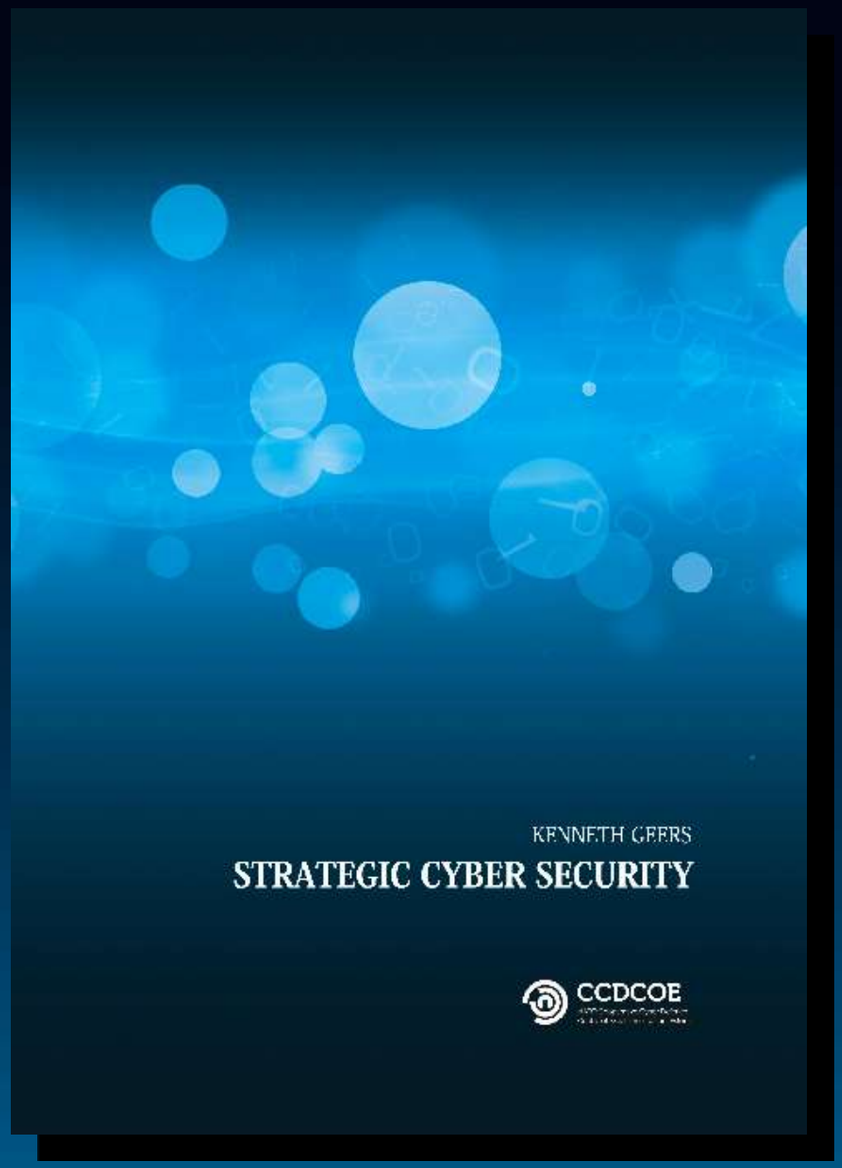
- Professional hackers
  - Physical damage of military significance
    - Without casualties, collateral damage, wider war?
- Vigilance required in peacetime
  - Strategic hacking requires long-term subversion

Mitigation Strategies



孫子兵法





Strategic Cyber Security

Kenneth Geers

NCIS Cyber SME

Free download:

ccdcoe.org/278.html

References

Broad, William J., Markoff, John & Sanger, David E. “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *New York Times* (15 Jan 2011).

Burns, John F. & Somaiya, Ravi. "WikiLeaks Founder on the Run, Trailed by Notoriety," *New York Times* (24 Oct 2010).

Chen, Thomas M. “Stuxnet, the Real Start of Cyber Warfare?” *IEEE Network*, Nov/Dec (2010).

Fisk, Robert. *Pity the nation: the abduction of Lebanon*, Nation Books (2002).

Friedman, Thomas. *From Beirut to Jerusalem,* Macmillan (1991).

Geers, Kenneth. *Strategic Cyber Security*. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia (2011).

References

"Iran has tricked us." *Der Spiegel* website (2 OCT 11)

"Leak of Military Documents." ROK Editorial Dong-A Ilbo Online (3 OCT 11)

Ludlow, Peter. "WikiLeaks and Hacktivist Culture." *The Nation*, 25-26 (4 Oct 2010).

Nicolas Falliere, Liam O Murchu, and Eric Chien. "W32.Stuxnet Dossier" Version 1.4 Symantec Security Response (Feb 2011).

O'Loughlin, John, Witmer, Frank D. W., Linke, Andrew M. & Thorwardson, Nancy. "Peering into the Fog of War: The Geography of the WikiLeaks Afghanistan War Logs, 2004–2009." *Eurasian Geography and Economics* 51(4) 472–495 (2010).