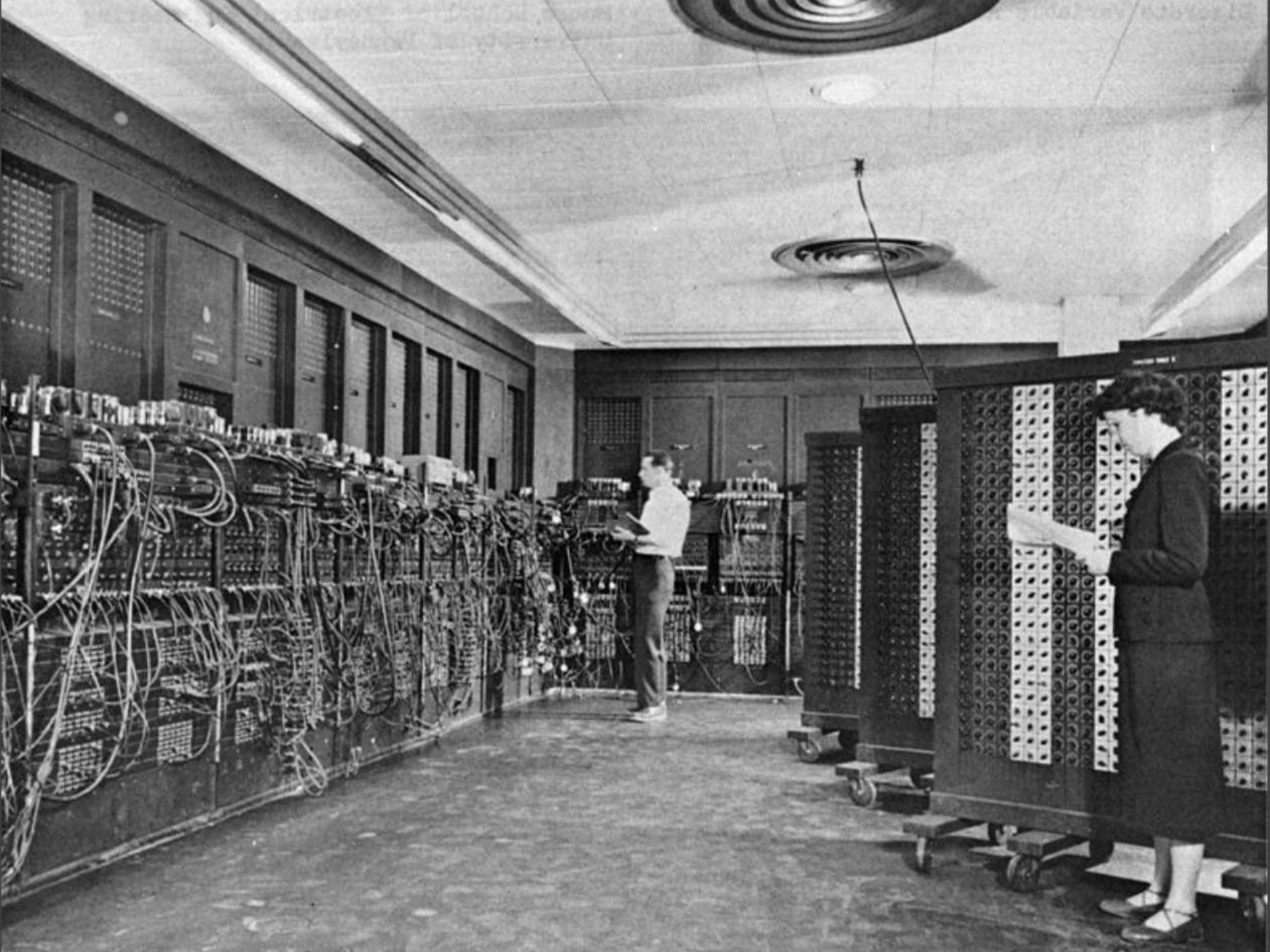
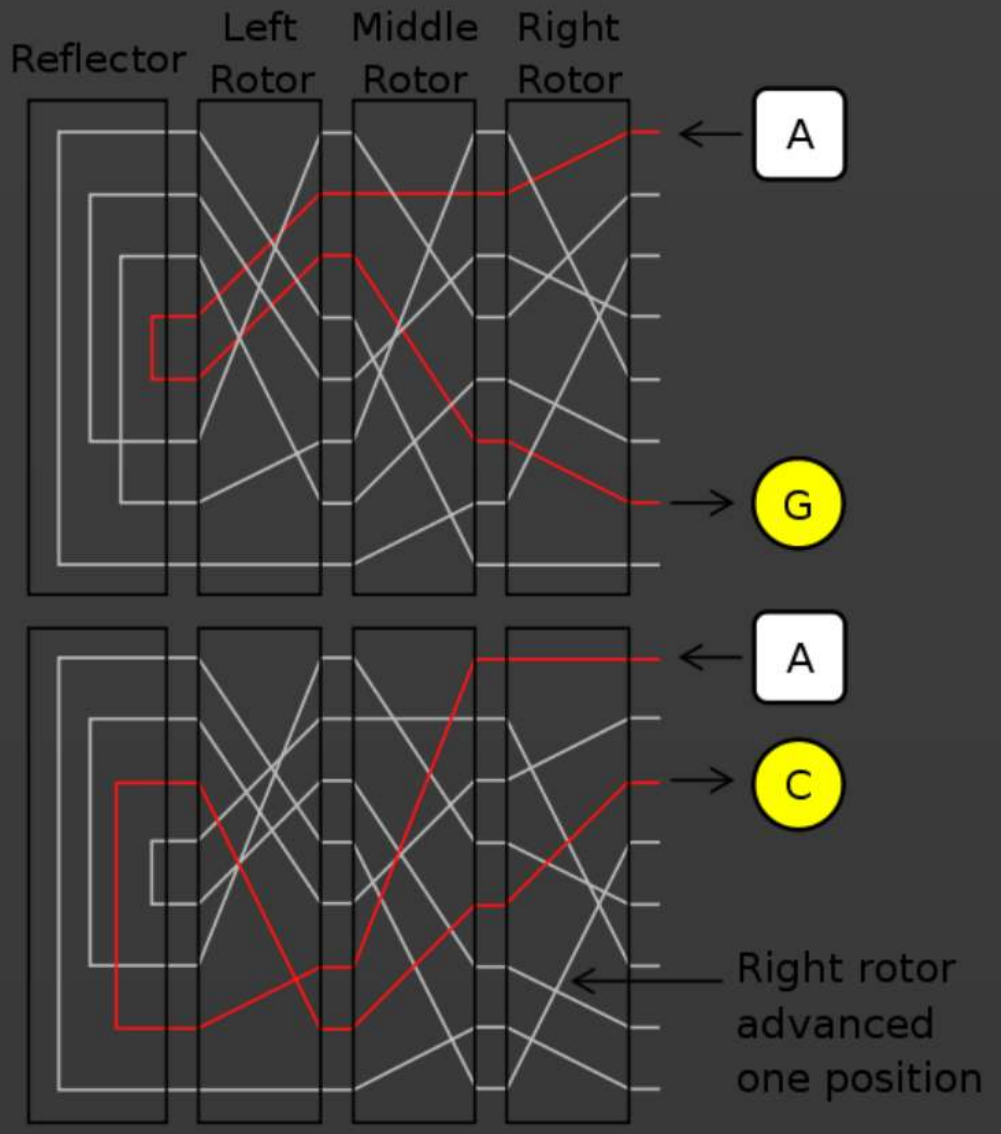
The Art of Cyberwar

Dr. Kenneth Geers

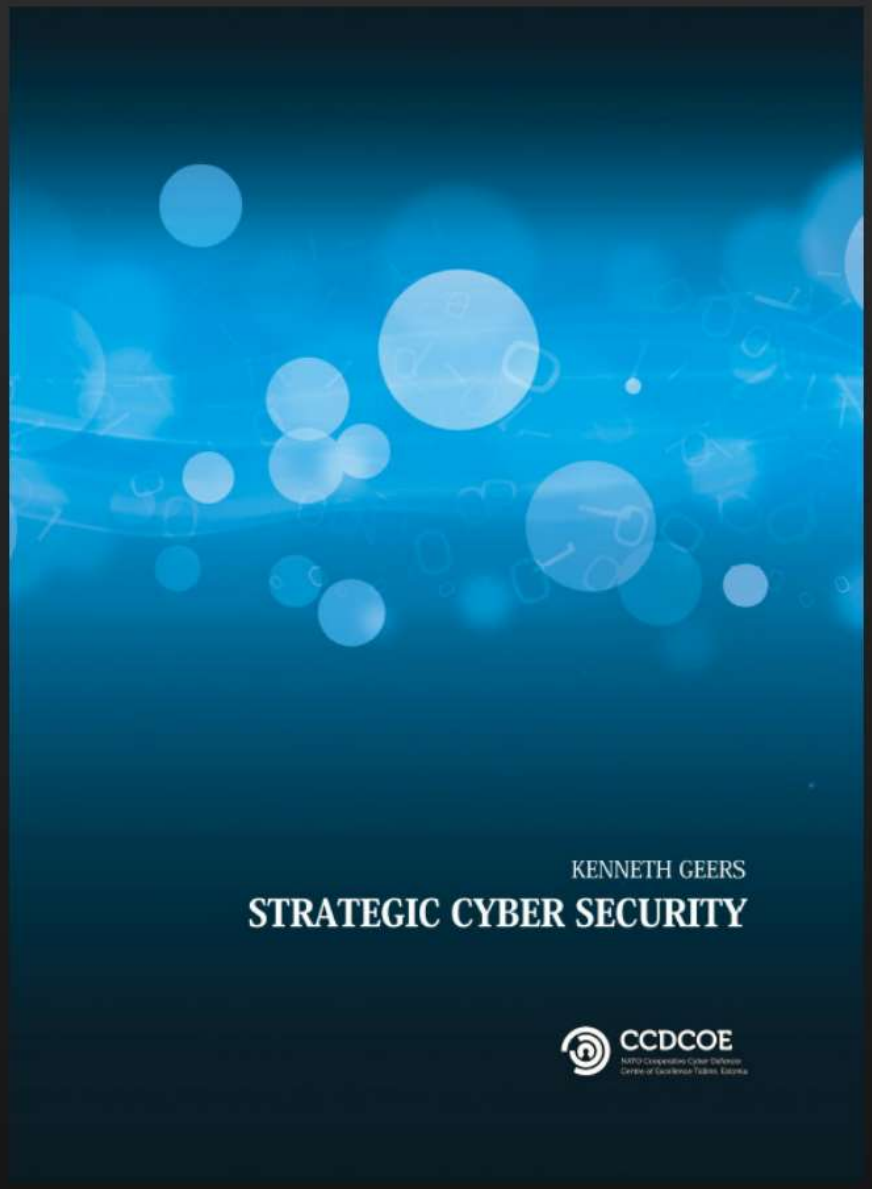
NCIS Cyber Subject Matter Expert




Bundesarchiv, Bild 183-2007-0705-502
Foto: Wakhar | 10. Dezember 1943


Reflector
Left Rotor
Middle Rotor
Right Rotor
A
G
A
C
Right rotor advanced one position

New York Times



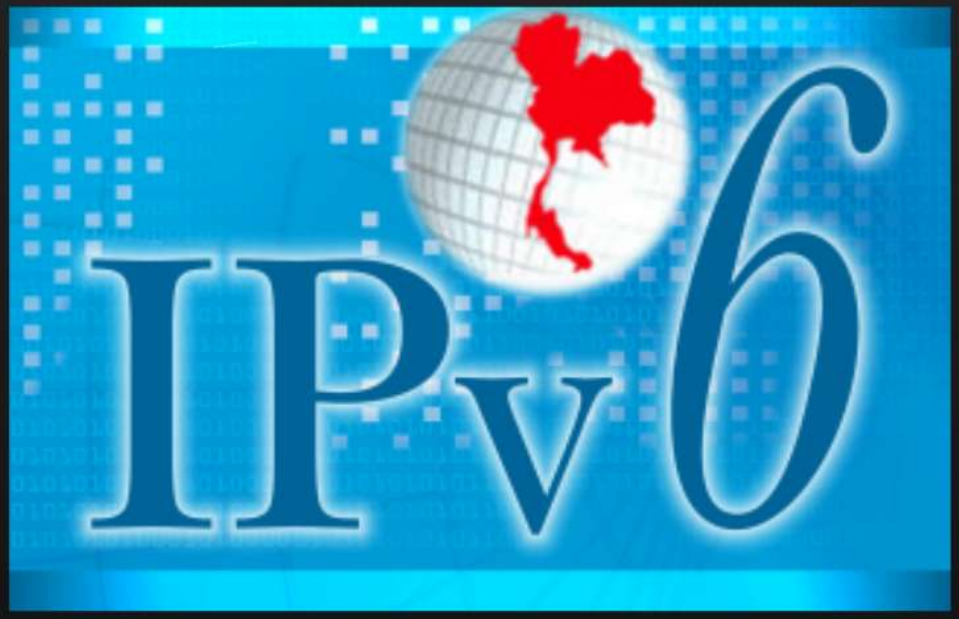
Free Download

Strategic Cyber Security

by Kenneth Geers

www.ccdcoe.org/278.html

Technology



Logic	1
Security	1
Attribution	1
Solution	0

Deterrence

	Deny	Punish
Capable	0	1
Communicate	0	1
Credible	0	0

Arms Control

Appeal	1
Assistance	1
Will	0
Prohibition	0
Inspection	0

Art of War

Objectivity	1
Training	1
Strategy	1
Tactics	1
Command	1
Battlefield	0

1. Environment

- Artificial, configurable
- Security vs freedom
- Code vs content

"The natural formation of the country is the soldier's best ally ... shrewdly calculating difficulties, dangers and distances constitutes the test of a great general."


ISAF REGIONAL COMMANDS
& PRT LOCATIONS
RC(N)
RC(W)
RC(C) Kabul
RC(E)
RC(S)
MeS
Konduz
Feyzabad
Meymana
Pol-e-Khomri
Panjshir
Nuristan
Qala-e-Naw
Herat
Bagram
Asadabad
Bamyan
Mether Lam
Chaghcharan
Wardak
Jalalabad
Ghazni
Gardez
Khowst
Tarin Kowt
Sharana
Farah
Qalat
Kandahar
Lashkar
Gah
ISAF PRT
PRT Lead Nation
Regional Command
KABUL

Updated 04 Feb 08

KFOR

HQ KFOR
THEATRE SUPPORT
~ 1700

MNTF (N)
~ 3000

MNTF (C)
~ 1800

MNTF (W)
~ 3000

MNTF (E)
~ 2400

MNTF (S)
~ 4000

~ 15,900 troops

24 NATO NATIONS

BEL 193	HUN 564	PRT 296
BGR 42	ITA 2567	ROU 147
CZE 435	LVA 19	SVK 135
DNK 305	LTU 32	EST 29
SVN 160	LUX 23	ESP 637
FRA 2269	NLD 6	TUR 752
DEU 2374	NOR 22	GBR 135
GRC 605	POL 320	USA 1456

10 NON-NATO NATIONS

ARM 34	IRL 279
AUT 561	MAR 213
AZE 34	SWE 331
FIN 391	CHE 209
GEO 182	UKR 184


MINISTERIUM FÜR STAATSSICHERHEIT

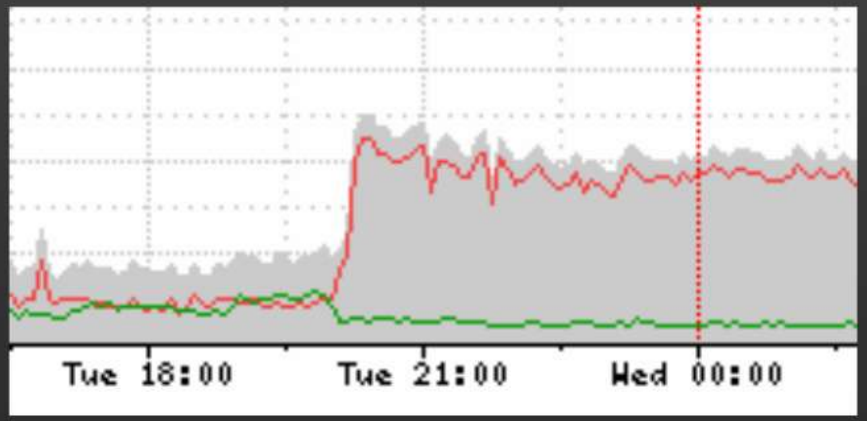
2. Proliferation

- Blinding speed
- 0 Day
- Defend classes of attacks

"The Art of War teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

Estonia 2007: after

<



Georgia 2008: during

=

Arab Spring: before

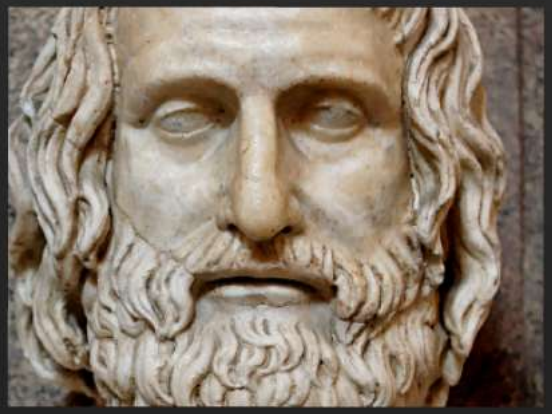
#Tunisia
#Egypt
#Libya
#Yemen
#Syria
?

<

3. Proximity

- Connectivity not geography
- Air, sub, S Forces
- App, OS, compiler, HW
- Seizing cyber ground

"The general is skillful in attack whose opponent does not know what to defend; he is skillful in defense whose opponent does not know what to attack."



مُحَمَّدٌ ﷺ

New Pen

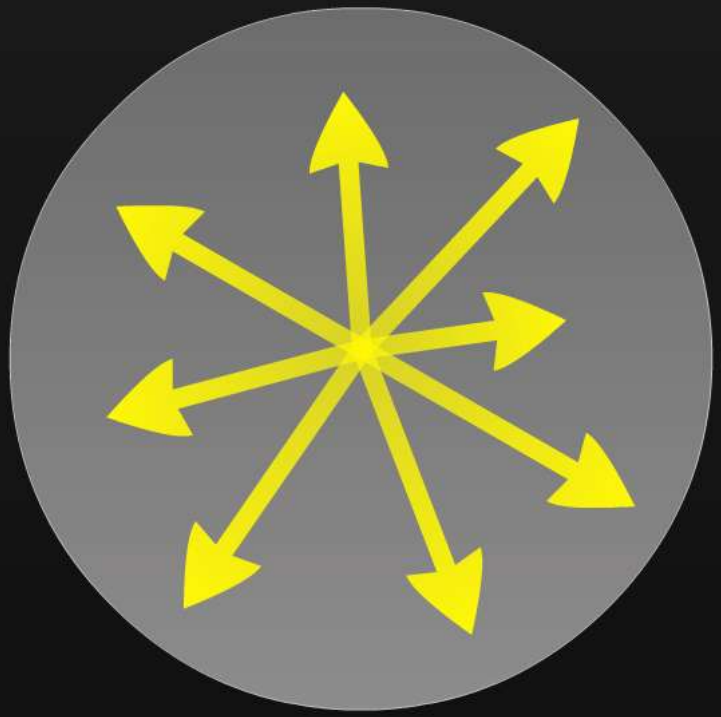
New Sword

```
#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
```

Wikileaks

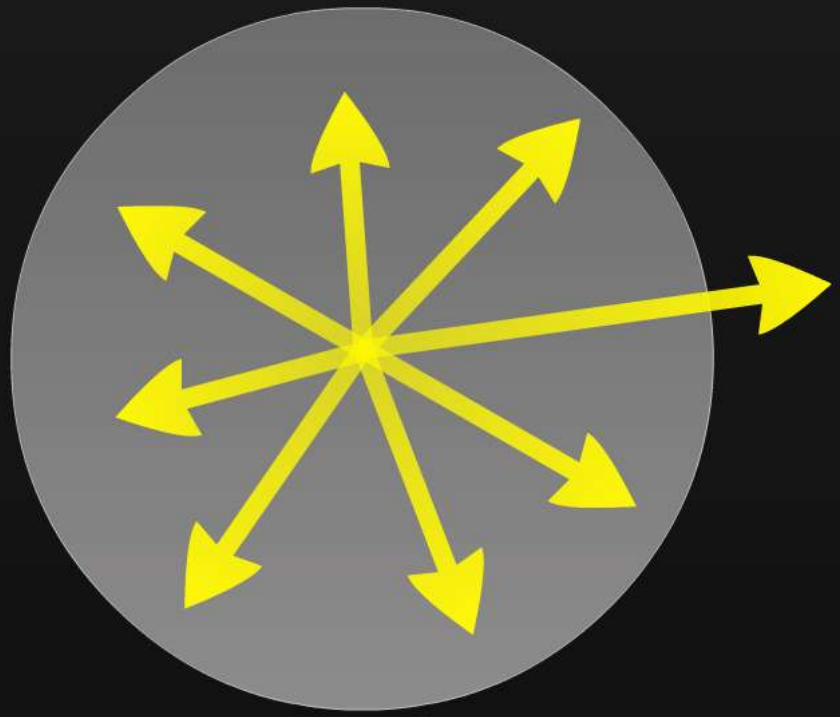
Stuxnet

Information Space



Wikileaks

Attack Space

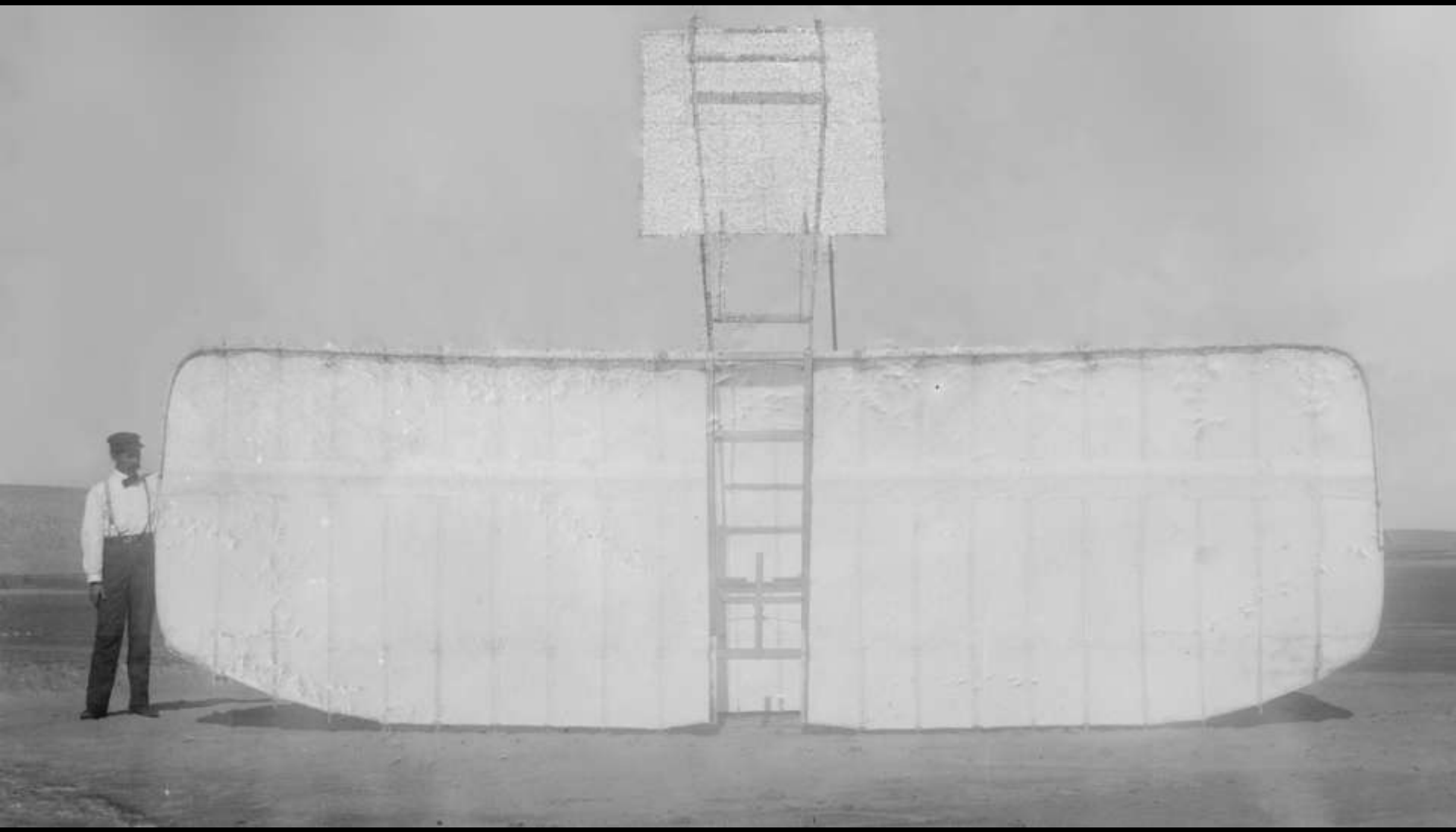


Stuxnet

4. Unpredictability

- Change w/o warning
- Must pull trigger to know
- Home-field advantage

"The general who is skilled in defense hides in the most secret recesses of the earth."



5. Advantage

- Old: size, strength
- New: network, anonymity
- Tactical to strategic advantage

"Rapidity is the essence of war: take advantage of the enemys unreadiness ... unexpected routes ... unguarded spots."

Syria


U.S. GOVERNMENT

إلى الشعب السوري : إن العالم يقف معكم ضد النظام الوحشي لبشار الاسد. أعرفو أن الوقت والتاريخ . إلى جانبكم -- الطغاة يستخدمون العنف لأن ليس لديهم أي شيء آخر . و كلما زاد عنفهم. كلما أكثر هشاشة اصبحو. نحيي تصميمكم على أن تكملوا سلمياً في مواجهة وحشية النظام . ونعجب استعدادكم لتحقيق العدالة و ليس الانتقام. سوف يسقط جميع الطغاة . وبفضل شجاعتكم... بشار الأسد هو التالي.

الى الجيش السوري : أنت مسؤول عن حماية الشعب السوري. وكل من يأمرك بقتل النساء والأطفال والمسنين يستحق أن يحاكم بتهمة الخيانة. لا يمكن لأي عدو خارجي أن يلحق الضرر بسوريا بقدر ما قام به بشار الاسد. دافعوا عن بلدكم - انتفضوا ضد النظام - مجهول

To the Syrian people: The world stands with you against the brutal regime of Bashar Al-Assad. Know that time and history are on your side - tyrants use violence because they have nothing else, and the more violent they are, the more fragile they become. We salute your determination to be non-violent in the face of the regime's brutality, and admire your willingness to pursue justice, not mere revenge. All tyrants will fall, and thanks to your bravery Bashar Al-Assad is next.

To the Syrian military: You are responsible for protecting the Syrian people, and anyone who orders you to kill women, children, and the elderly deserves to be tried for treason. No outside enemy could do as much damage to Syria as Bashar Al-Assad has done Defend your country - rise up against the regime! - Anonymous

Syria 1982 … Syria 2012

"…cut all telephone and road communication with the city … exact details … incomplete … no reporters" NYT

6. Flexibility

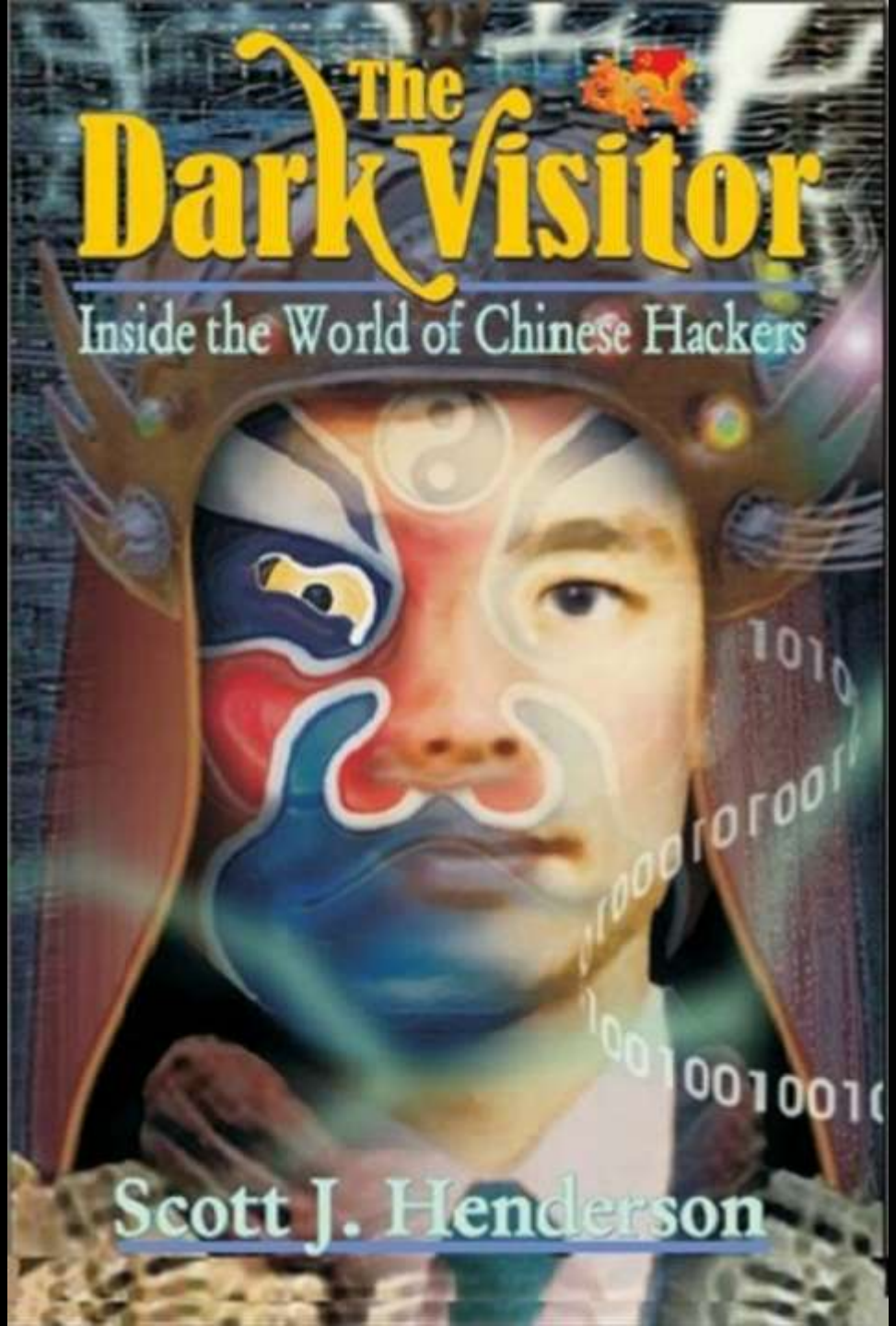
- Espionage: Golden Age
- Destruction: STXNT
- Most powerful: propaganda

"There are five ways of attacking with fire: burn soldiers in their camp; burn stores; burn baggage trains; burn arsenals and magazines; hurl dropping fire amongst the enemy."

ЧЕЧЕНСКАЯ РЕСПУБЛИКА ИЧКЕРИЯ
ЧЕЧЕНПРЕСС
Государственное информационное агентство
RUSSIAN TURKISH ENGLISH

Professor U.Ezhiev's sons kidnapped

On the night of 9 March 2003, in Staropromislov district of the Chechen capital Grozny, the Russian servicemen kidnapped two brothers Ezhaevs - Ruslan and Arby Umalatovich. Certain details of the incident have become known today.


The Dark Visitor
Inside the World of Chinese Hackers
Scott J. Henderson

INTERNATIONAL
Herald Tribune
THE GLOBAL EDITION OF THE NEW YORK TIMES
Europe

Cyberwar and real war collide in Georgia

By John Markoff

Published: August 13, 2008

Weeks before bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace.

Jose Nazario of Arbor Networks in Lexington noticed a stream of data directed at Georgian government sites with the message: "win+love+in+Rusia."

2346.98

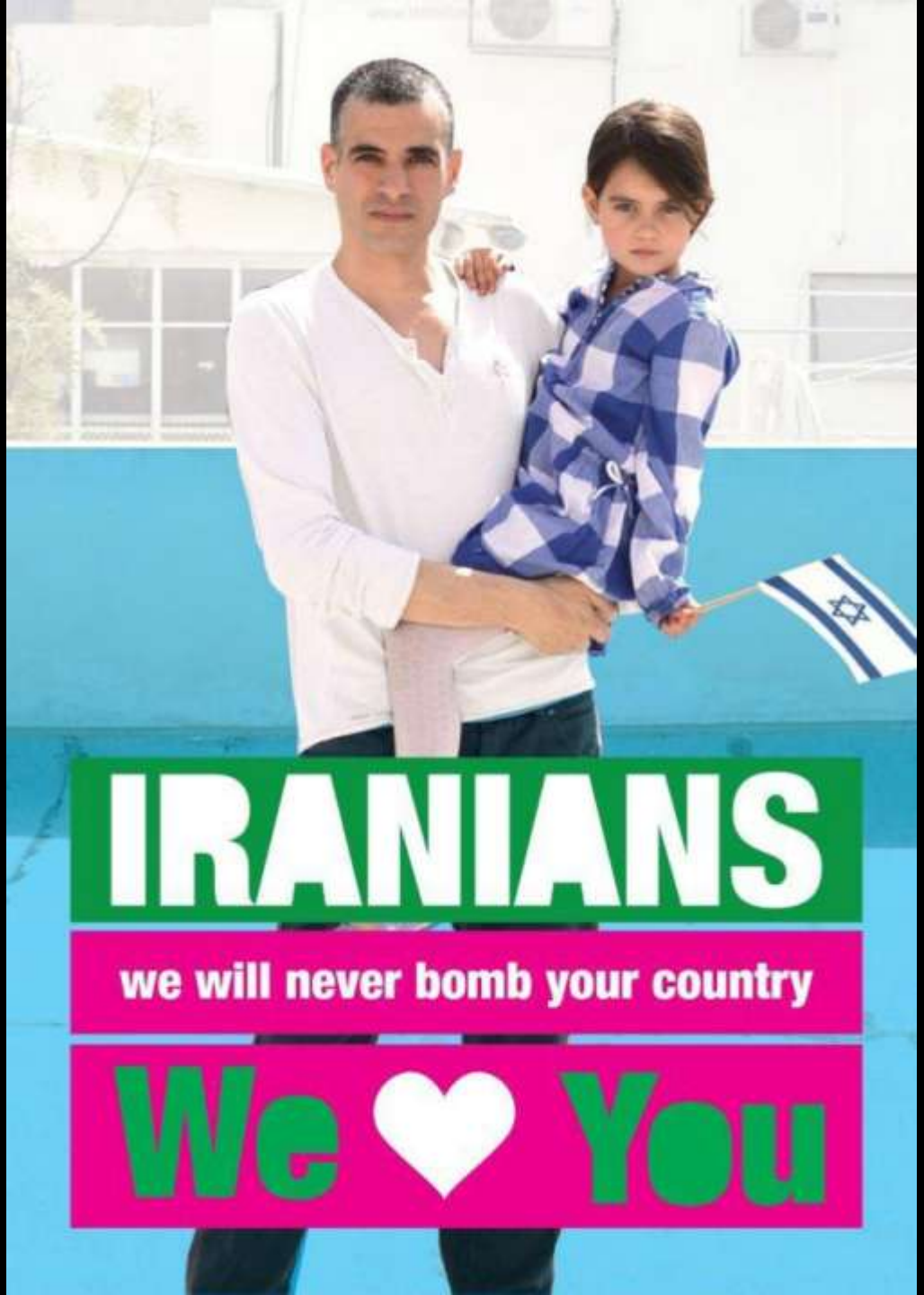
64.89


WENGER

7. Attribution

- Deterrence, retaliation: low credibility
- Ease of entry = rising numbers
- Real cyberwar, ID should be clear

"A wise general makes a point of foraging on the enemy ...
one cartload of the enemy's provisions is equivalent to twenty of one's own."


IRANIANS
we will never bomb your country
We ♥ You

8. Quiet

- Covert cyber war
- Retaliation in meatspace
- Proportionality
- Private sector vs nation-state

"O divine art of subtlety and secrecy ... we learn to be invisible ... inaudible ... we can hold the enemy's fate in our hands."

INSIDE THIS WEEK: TECHNOLOGY QUARTERLY

The Economist

JUNE 2ND–8TH 2012 Economist.com

The horror in Houla

How to save Spain

Time to buy European stocks?

Squeezing out the doctor

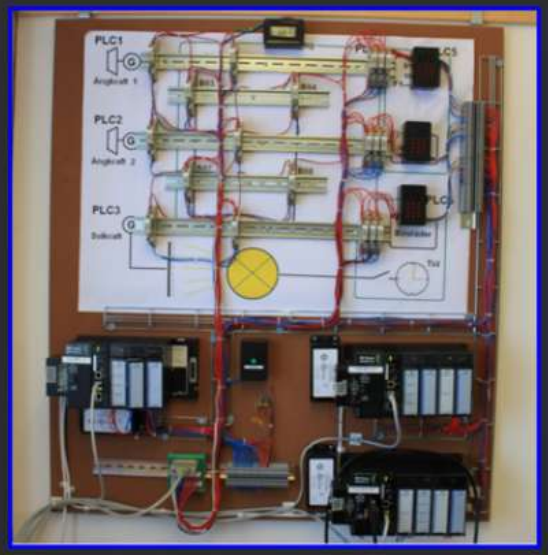
In praise of misfits

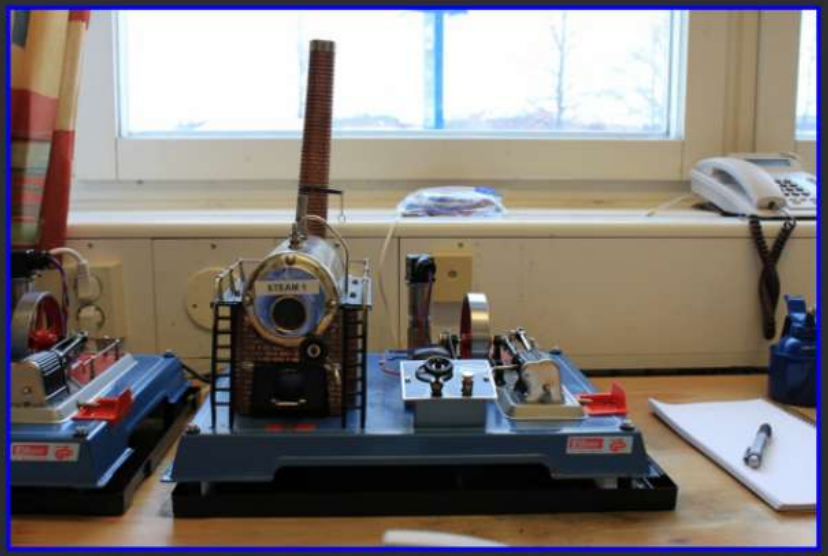
Morals and the machine

Teaching robots right from wrong


MANGA ENTERTAINMENT PRESENTS A MAMORU OSHII FILM GHOST IN THE SHELL BASED ON THE ORIGINAL MANGA BY MASAMUNE SHIROW
AT A CINEMA NEAR YOU FROM DECEMBER 8TH
GHOST IN THE SHELL
IT'S FOUND ITS VOICE.... NOW IT NEEDS A BODY
FEATURING "ONE MINUTE WARNING" BY PASSENGERS (BRIAN ENO + U2)

NATO Cyber Centre - War Gamez





9. Subjectivity

- Cyber defense immature
- BDA calculations
- Effects-based evaluation

"If you know the enemy and know yourself, you need not fear the result of a hundred battles."

Cyber Battalion

- Intelligence = Intelligence
- HUMINT = HUMINT (Social Engineer)
- Special Forces = Special Forces
- Combat Engineer = Software Developer
- Infantry = Network Penetrator
- Tents = Clients, Servers
- Weapons = Information

10. Morality

- Few inhibitions: no dead humans
- Future target: civilians
- End-state: war or peace?

"Supreme excellence consists in breaking the enemy's resistance without fighting."

"The best thing of all is to take the enemy's country whole and intact."

Just War

Just cause	1
Last resort	1
Competence	1
Necessity	1
Probability	1
Distinction	1
POW ethics	1
Proportionality	1
Prohibition	0
Declaration	0
Surrender	0

Confidence Building Measures

1. Non-aggression pact
2. Int'l administration
3. Transparent log files
4. World CERT
5. Joint investigations

The Art of Cyberwar

Dr. Kenneth Geers

NCIS Cyber Subject Matter Expert