Is the Pen still mightier than the Sword?

Kenneth Geers
NCIS Cyber Subject Matter Expert
Reconsidering an Adage
Long-range weapons
“…cut all telephone and road communication with the city.”

“Exact details ... Incomplete. No reporters”
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

Wikileaks

Stuxnet
The new Pen

WikiLeaks
The Chinese hackers advocate
We merely make the safe escape
Invades the Person

Owned by cDC
www.cultdeadcow.com
The last shall be first
Whom do you trust?
Outliers

Miyazaki 8.299

Van Damme 4.805
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

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

// Data declarations
extern int dword_10001c0[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, _DWORD, _DWORD); // weak
extern int (__stdcall *dword_1000218a)(__DWORD, _DWORD, _DWORD, _DWORD, _DWORD); // weak
extern int dword_1000218e; // weak
extern int dword_10002192; // weak
extern int dword_10002196; // weak
extern int (__stdcall *dword_1000219a)(__DWORD); // weak
extern int HWND window_1000215c; // weak
```
Context
The First Cyber War(s)
## Military Grade

1. Infrastructure test
2. 1<sup>st</sup> 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
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:
cdccoe.org/278.html
References


References

“Iran has tricked us.” Der Spiegel website (2 OCT 11)

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

