
Cryptography and Information Warfare

January 29, 1997

Dr. Gerald L. Kovacich, CFE, CPP, CISSP

Phone: 310-948-0739

e-mail address: [jkovacich@atdc.northgrum.com](mailto:jkovacic@atdc.northgrum.com)

NORTHROP GRUMMAN



Three Waves of Information Warfare (IW)

- **Agricultural**
 - Sticks & Stones
- **Industrial**
 - Blitzkrieg and Nuclear Weapons
- **Information**
 - Computers/Telecommunications
 - Surveillance/Precision Strike
 - Advanced Battle Management

Information Warfare, as defined by the US Defense Information Systems Agency (DISA)

- “actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and protecting our information and information systems.”

Working Definition Drawn From DOD Sources



- Offensive - to deny, corrupt, destroy, or exploit an adversary's information, or influence his perception,
- Defensive - to safeguard ourselves and allies from similar action,
- Exploitative - to exploit available information in a timely fashion, in order to enhance our decision/action cycle and disrupt the adversary's cycle.

Progressive Hostilities and Cryptography

- Intelligence Collection
- Diplomatic Action
- Economic Segregation
- Military Preparedness
- War

Information Warfare

- Information Age Warfare
 - ⑦ Warfare by Intelligent Weapons
 - ⑦ Integrated Battle Management
- Information Systems Warfare
 - ⑦ Hackers/Phreakers
 - ⑦ Cyberwar

Sophistication and Vulnerabilities

- **US Vulnerable to First and Second Wave Nations' IW Attacks**
- **First and Second Wave Nations Less Vulnerable to US IW Attacks**

● Haiti - Somalia - Iraq - China - Russia

Crypto (Exploit and Protect)

- **Defined as: The encrypting of US and allies' information so it is not readable by those who do not have a need-to-know; the decrypting of the information of adversaries to be exploited for the prosecution of information warfare.**

Crypto and IW Challenge

- Protects communications except when secure datalinks can't meet the needs of the IW warriors, then any links are used to communicate
- The challenge is to ensure flexible encryption capabilities available to meet the needs
- Encrypted communications will be impacted by adversary's use of IW-related techniques to deny use of the links, e.g. spamming

Crypto and IW Challenge

- More complex due to more powerful and sophisticated computers
- Broken easier for the same reason - more powerful and sophisticated computers

The Chinese Example

- Chinese believe all its citizens are soldiers in time of need
- More capitalism has brought more Western support in the form of technology
- More businesses and more citizens beginning to own computers
- How much computer power will it take to break encrypted messages if the power of more than 50 million Pentium-plus computers were attacking the problem?

SUMMARY

- IW Defense requires use of cryptography
- IW Offense requires breaking adversaries code
- A new type of war, but old type of protection methods
- The difference - the technology applied