



# **Cyber Security Professionals**

By: Gregg L. Zepp II  
CISSP, CEH, CPT, MCSA

# Cyber Security Professionals

## Security for Cyber Defense & Exploitation for Cyber Warfare

---

### ▶ Recon & Warfare Today:

- War conducted by land, sea, air, is often accompanied by attacks on the wire.
- Media warfare attacks have hit the governments of Georgia, Estonia, Lithuania, and this year, Kyrgyzstan. Media “cold war” and cyber terrorism is growing.
- According to Symantec, almost half of all DDOS attacks are targeted at the US. (Ref: UK’s “The Register” - [http://www.theregister.co.uk/2007/05/02/dos\\_trends\\_symantec/](http://www.theregister.co.uk/2007/05/02/dos_trends_symantec/))
- An article in the recent Spring 2009 IANewsletter from IATAC by COL John Surdu and LTC Gregory Conti calls for a new branch of the military dedicated only to Cyberwarfare.

### ▶ Cyber Security:

- Many critical systems are connected to networks with vulnerabilities, eventually leading to the internet. Defense of these critical systems, recon, and “back hacking” when they are attacked is crucial. We need better trained, highly skilled cyber security professionals / soldiers / warriors.

# Cyber Security Professionals

## Security for Cyber Defense & Exploitation for Cyber Warfare

---

### ► Cyber Security Professionals:

Training needs to be three-fold:

- 1. Industry Certifications:** Training for these exams provides quick exposure and practice of technologies and skill sets. Examinations offer some level of confirmation of acquired knowledge.
- 2. Long-term In-Depth Education:** Alliances with universities to establish in-depth courses within informational security areas. Learning must never end since technology is continually evolving. Degree enforce certifications and vice versa.
- 3. Mentoring and Practical Application:** When possible, junior engineers should work along side those more senior. Periods of practical application of new KSAs in simulated environments would further sharpen those recently trained.

# Cyber Security Professionals

## Security for Cyber Defense & Exploitation for Cyber Warfare

---

### ► Cyber Security Professionals:

End-to-End point information security can be achieved by securing 4 areas of technology:

1. **Networks** – securing hardware that controls traffic on the wire
2. **Hosts** – securing connected machines, handhelds, and other devices
3. **Software: Applications & Databases** – closing software vulnerabilities on the hosts and in network hardware
4. **Policy & Physical Security** – securing hardware through the use of physical security technology and policy creation & enforcement

# Cyber Security Professionals

## Network

- \* architectures
- \* hardware
- \* IOS
- \* protocols

- \* sniffing
- \* IDS/IPS
- \* traffic/protocol analysis
- \* attacking

## Host

- \* hardware
- \* server services
- \* operating systems

- \* OS hardening
- \* OS polley
- \* Forensics
- \* OS exploitation

## Application & Database

- \* languages: app & web
- \* scripting
- \* assembly
- \* SQL & other DB

- \* code exploitation
- \* code hardening
- \* reverse engineering

## Policy & Physical Security

- \* policy practitioner
- \* social engineering
- \* break-in artist

- \* govt regulation
- \* building security
- \* signal analysis
- \* surveillance

## Security Defensive & Offensive

# Cyber Security Professionals

## Domain 1: Networks

---

### ▶ Proficient in the following areas:

- Network typologies & LAN/WAN technologies
- Router, switch, bridge configurations ~ IOS
- Protocol analysis (TCP, IP, OSPF, BGP, EIGRP, RIP)
- Firewall practitioner

### ▶ Applicable areas of Security & Exploitation:

- Network sniffing & probing, Passive reconnaissance
- DNS, SNMP abuse / Breaking DMZs
- Traffic & protocol analysis / Covert channels / Session hijacking
- Penetration testing / hacking / back hacking
- Major Tools: Nessus, Nipper, RAT, Cisco-Bug,

### ▶ Suggested Industry Certifications:

- Network+ or Network 5, CNDA, GCED, CCNA, CCNA+Security, CCNP, EC-Council's NSA, ECSA

# Cyber Security Professionals

## Domain 2: Hosts

---

### ▶ Proficient in the following areas:

- OS hardening, OS policy configuration, Virtualization security
- OS Services expert, IIS & Apache, Cloud Taming
- Authentication Security (i.e., PKI), Password cracking
- File System Permissions & Encryption

### ▶ Applicable areas of Security & Exploitation:

- Host Forensics / Alternate Data Streams / Data Recovery / Antiforensics
- Overflows / Shellcode / Sockets
- Rootkit use & Kernel exploitation
- Circumventing Antivirus & IDS/IPS
- Major Tools: Nmap, Nessus, CoreImpact, Encase

### ▶ Suggested Industry Certifications:

- CompTIA's Security+, SANS GSEC, IACert's CPT, MCSE/MCSA+Security, EC-Council's CCI, CHFI, CEH, LPT

# Cyber Security Professionals

## Domain 3: Applications & Databases

---

### ▶ Proficient in the following areas:

- Branching statements, bytecode, identifying variables, web languages
- Kernel debugging, hashing functions, overflows, injections
- Malware, anti-debugger code, decompilers, disassemblers
- CWE/SANS Top 25 Most Dangerous Programming Errors (Jan 2009)

### ▶ Applicable areas of Security & Exploitation:

- Signature & Binary analysis, software vulnerabilities
- Rootkits, anti-rootkits, database injection tools, scripting (Python, Perl, Ruby)
- Reversing, Antireversing, Breaking Code Protections, Decompilation
- Malicious Crypto, web application security (OWASP)
- Major Tools: IDA Pro, SoftICE, OllyDbg, Dumpbin, Fortify, Metasploit

### ▶ Suggested Industry Certifications:

- ISC2's CSSLP, EC-Council's ECSP, CSAD, SANS GSSP Levels (C, Java, .Net)

# Cyber Security Professionals

## Domain 4: Policy & Physical Security

---

### ▶ Proficient in the following areas:

- Systems auditing, ISO standards, DIACAP, FISMA, DoD 8500, NIST 800-53
- Legal: fraud, e-security crimes, liability, policy, electronic records
- Defeating perimeter & physical security – hi-tech monitoring devices
- Break-in Specialist: defeating locks / bio security devices / social engineering

### ▶ Applicable areas of Security & Exploitation:

- Power grid security / SCADA systems / nuclear safety
- Aviation & Airport security
- Bio & Chemical response / HazMat info
- Communications/Cabling & Signal security
- Risk Assessment and Physical Security Surveys

### ▶ Suggested Industry Certifications:

- ASIS's CPP, PCI, PSP, ISACA's CISA, CISM, CGEIT, ISC2's CISSP, ATAB's CAS-IT, CAS-CTR, CAS-PSM, SANS (ISO Specialist, GSNA, GLEG)