



Live-Fire Exercise:  
*Baltic Cyber Shield 2010*

Kenneth Geers

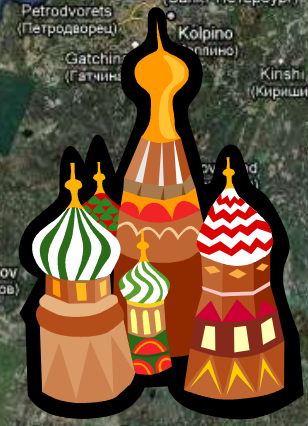
Naval Criminal Investigative Service (NCIS)

Cooperative Cyber Defence Centre of Excellence (CCD COE)

# Overview

- May 10-11, 2010
- **International cyber defense exercise (CDX)**
- CCD CoE / Swedish National Defence College
- Six Blue Teams
  - Northern European gov, mil, priv sec, acad
- Red Team
  - 20 friendly hackers
- Scenario
  - Cyber terrorists vs power generation companies

# Baltic Sea



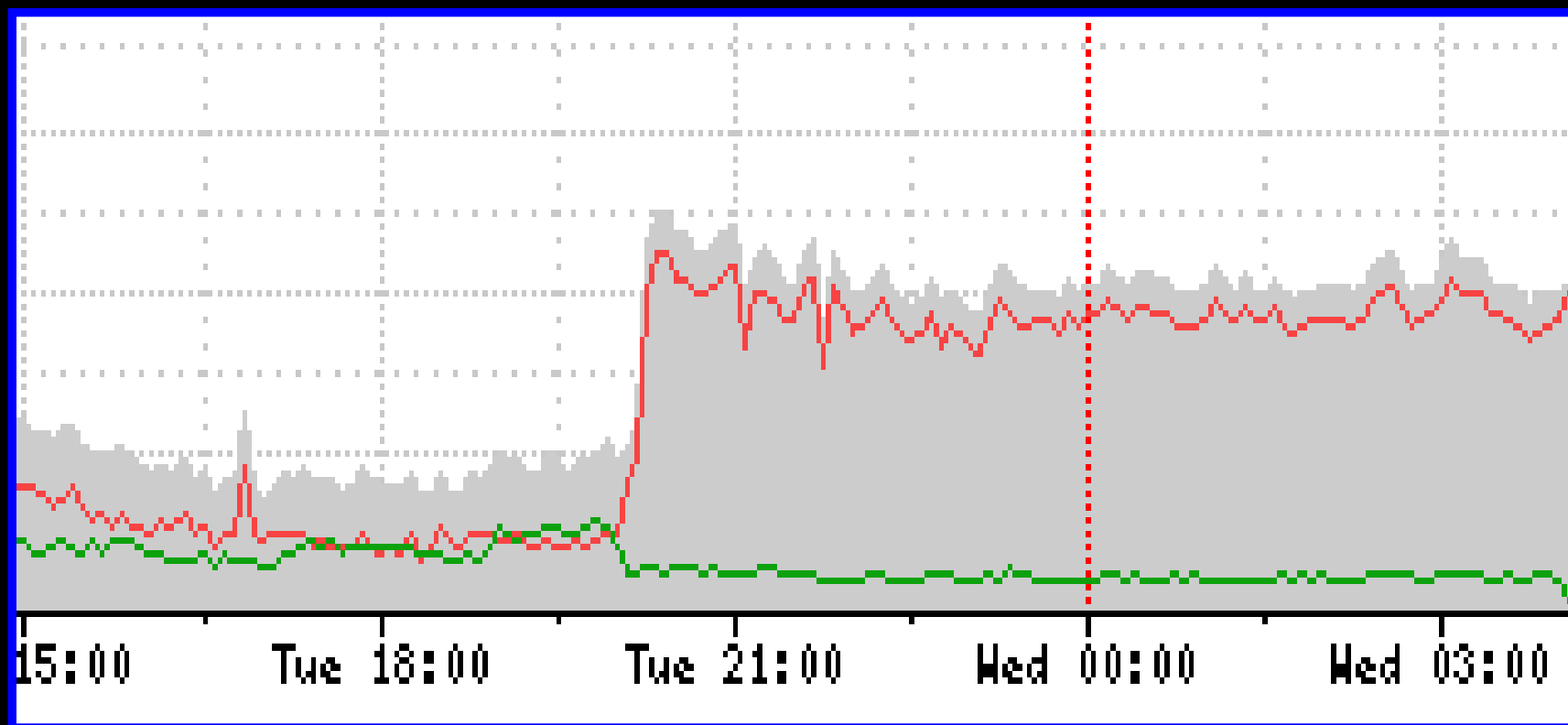
# Tallinn, Estonia



# 2007: Street Disturbances



# 2007: Cyber Attack



# CCD CoE



# Introduction

- **Are cyber attacks a threat to national security?**
  - Cyber terrorism, cyber warfare
- Expert opinions
  - Dismissive to apocalyptic
- What would the targets be?
  - Electricity, water, air traffic control, stock exchange, national elections...



# Trends

- National critical infrastructures increasingly connected to the Net
- Custom IT systems replaced with less expensive, off-the-shelf Windows and UNIX
- Traditionally closed networks (eg SCADA) not designed for resiliency
- OS familiarity may facilitate hacking

# Nat'l Security Thinking

- Cyber attacks: better understanding required
  - Some real-world case studies
  - Much information lies outside public domain
  - No wars yet between two Internet-enabled militaries
- **Must be able to simulate cyber attack and defense in a laboratory**

# Moving Target

- Realistic CDXs are a challenge
  - Must simulate adversary, friendly forces, even the battlefield
  - Conclusions may be valid for a short time
- IT, hacking are complex and dynamic
  - Rapid proliferation of computing devices, processing power, user-friendly hacker tools, practical encryption, Web-enabled intelligence collection

# Half-Life

- The military and computers...
  - Train tank drivers, pilots
  - Simulate battles, campaigns, complex geopolitical scenarios
- **How well can a sim model the real world?**
- Failure factors
  - Poor intelligence, miscalculations, incorrect assumptions, scoring system, political considerations
  - 2002: \$250 million Millennium Challenge

# Cyber Defense Exercise

- Robust CDX requires team-oriented approach
  - **Blue Team**: friendly forces
  - **Red Team**: hostile forces
  - **Green Team**: technical infrastructure
  - **White Team**: game management

# Blue Team

- Real-life system administrators and computer security specialists
  - Primary targets for instruction
- Goal
  - Defend network confidentiality, integrity, and availability (CIA) vs hostile RT
  - Scoring: automated and/or manual system

# Red Team

- The cyber attacker
  - BCS: “cyber terrorist”
- Goal
  - *Undermine CIA of BT networks*
- Tactics
  - On virtual battlefield, almost no limitations
- “White box” vs “black box” testing
  - The question of prior knowledge

# White Team

- **Manages and referees CDX**
  - Writes game scenario, rules, scoring system
  - Makes in-game adjustments
  - Tries to prevent cheating
    - EX: firewall rule detrimental to game and/or unrealistic?
  - Declares the “winner”



# Green Team

- **Designs, hosts network infrastructure**
  - In-game ISP
  - Records traffic for post-game analysis
  - Manages automated scoring
- Virtual machine technology
  - Possible with few resources, but...
  - Sim powerful adversary = many resources
    - EX: RT plan should indicate money, manpower
- VPN technology
  - Teams can log in from anywhere

# Scenario

- **Helps determine strategic significance**
- Estimate resources and cost
  - Lone hacker, org, nation-state?
    - Can a lone hacker be a nat'l sec threat?
- Out-of-the-box thinking
  - Always helpful
- Can only real-world attacks change threat perception?

# Cyber War Philosophy

- Cyber warfare is not traditional warfare
  - Tactical victories: reshuffling of bits
  - Any real-world effects?
- Cyber attack
  - Not an end in itself
  - **Extraordinary means to many ends**
    - Espionage, DoS, identity theft, propaganda, infrastructure manipulation, ?

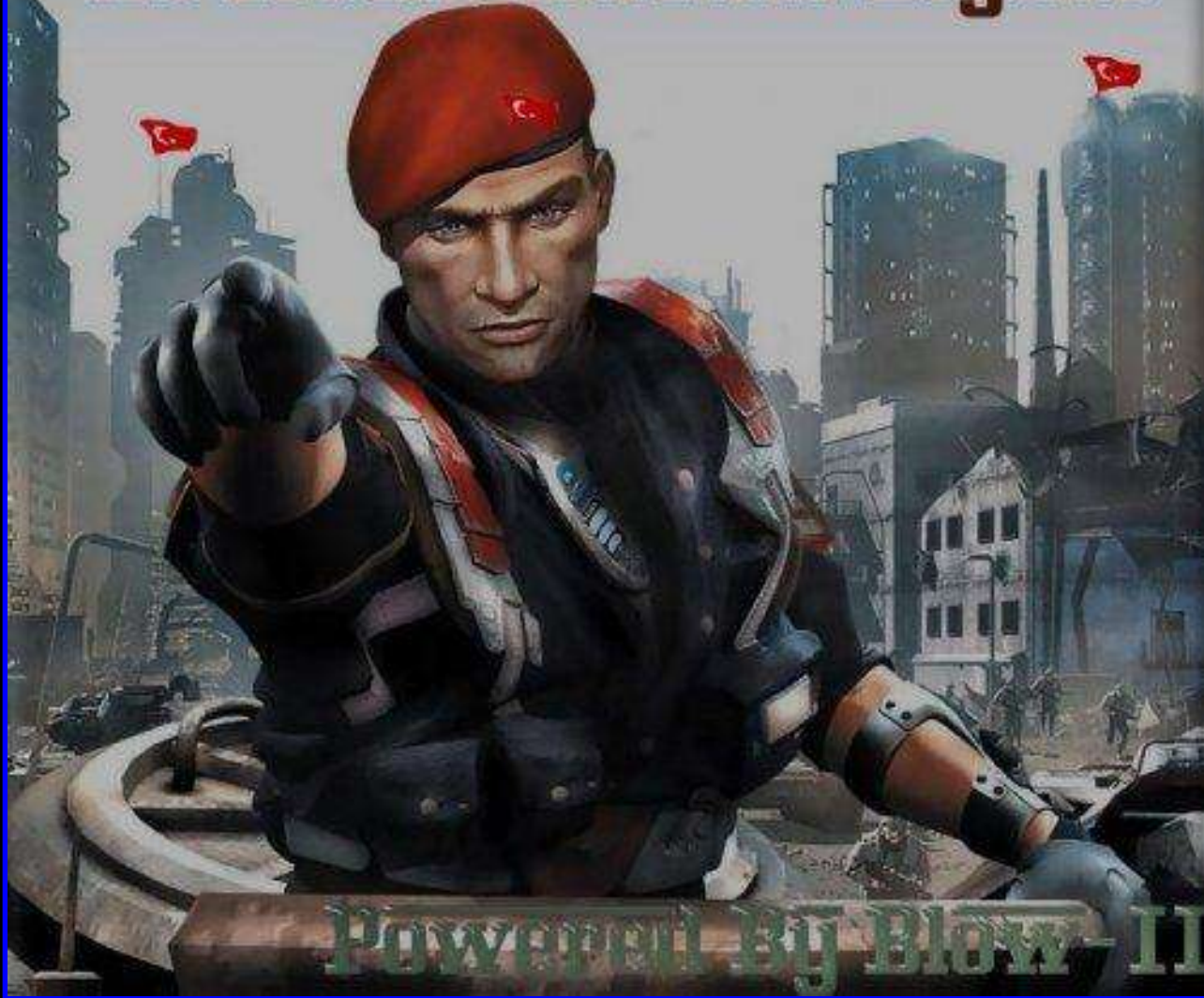
# The Art of (Cyber) War

Sun Tzu said: There are five ways of attacking with fire. The first is to burn soldiers in their camp; the second is to burn stores; the third is to burn baggage trains; the fourth is to burn arsenals and magazines; the fifth is to hurl dropping fire amongst the enemy.



[www.hizbulla.org](http://www.hizbulla.org): October 25, 2000

Ne Mutlu Turkum Diyene



Powered by Blow-IT



Γ.Η.Σ.

GREEK HACKING SCENE



# The New York Times

July 1, 2008

## Hackers Tag Lithuanian Web Sites With Soviet Symbols

By SARA RHODIN

MOSCOW — Hackers attacked about 300 Web sites in [Lithuania](#) over the weekend, with Soviet symbols and anti-Lithuanian slogans, officials said Monday.







*The Chinese hackers advocate the freed*

*We merely make the safe examination*

*Invades the Personnel*

*江南劍书生, FruNylsE, Shnog , LnSang, HnBin , Ploiy*

WIRED

TECH BIZ : IT 

## 'UFO Hacker' Tells What He Found

Nigel Watson  06.21.06

The search for proof of the existence of UFOs landed Gary McKinnon in a world of trouble.

After allegedly hacking into NASA websites -- where he says he found images of what looked like extraterrestrial spaceships -- the 40-year-old Briton faces extradition to the United States from his North London home. If convicted, McKinnon could receive a 70-year prison term and up to \$2 million in fines.



**Ministry of  
Health**



ZIMBABWE



**and Child  
Welfare**

---

**Command Tribulation Ownz your b0x**

**Jesus loves you**







# 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."

-  E-Mail Article
-  Listen to Article
-  Printer-Friendly
-  3-Column Format
-  Translate
-  Share Article

# Electronic Pearl Harbor?



July 19, 2010



**WIRED** SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> HOW-TO

Sign In | RSS Feeds

# THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

## SCADA System's Hard-Coded Password Circulated Online for Years

By [Kim Zetter](#) July 19, 2010 | 5:29 pm | Categories: [Cybersecurity](#)

A sophisticated new piece of malware that targets command-and-control software installed in critical infrastructures uses a known default password that the software maker hard-coded into its system. The password has been available online since at least 2008, when it was posted to product forums in Germany and Russia.



# Strategic Thinking

1. The Internet is vulnerable
2. High return on investment
3. Inadequacy of cyber defenses
4. Plausible deniability
5. Growing power of non-state actors
6. ?

# CDX: Goals

- RT vs BT
  - Credible simulation of net attack and defense
  - Acquisition / prevention of *unauthorized access*
- Real-world impact
  - Political / military results?
  - Zip, minor annoyance, or national security crisis?



# Nation-State Simulation

- **Mil / gov agencies are “full-scope” actors**
  - Much more than computer hacking
  - Deep well of nat’l IT expertise
    - Crypto, prog, debug, vuln discovery, agent-based systems, etc
  - Supported in turn by experts in other disciplines
    - Natural sciences, physical security, supply chain, continuity of business, social engineering, etc

## EX: Sandia Nat'l Labs

- Robust RT
  - Kills: mil installations, oil companies, banks, electric utilities, e-commerce firms
  - Specialize in hidden vulns in complex environmts
    - Obscure infrastr interdep in specific domains
- Former chief
  - “Our general method is to ask system owners: ‘What's your worst nightmare?’ and then we set about to make that happen”

# CDX history

- Every CDX is unique
  - Good and bad
  - IT evolves too quickly
  - Too many variables in cyberspace
- Both lab-based and real-world
- Cyber defenders may / may not be warned

# Eligible Receiver (1997)

- 35 NSA personnel
  - “North Korean” hackers
  - Target: U.S. Pacific Command
- J. Adams in *Foreign Affairs*
  - “human command-and-control system” infected with “paralyzing level of mistrust”
  - “nobody in the chain of command, from the president on down, could believe anything”
- Also revealed that many nat’l critical infrastr vulnerable to cyber attack

# Water Security

- 2006: Environmental Protection Agency
  - **Could a hacker poison the water supply?**
  - Sandia vuln assessm't: distrib plants serving >100,000
    - 350 such facilities = too many!
    - Thorough analysis: 5 sites
    - Risk Assessm't Methodology for Water (RAM-W)

# International CDXs

- **Internat'l architecture, internat'l responsibility**
- 2006 DHS Cyber Storm
  - Scen: non-state “hacktivists”
  - Gov collab w/ private sector
- 2008 Cyber Storm II
  - Scen: Nation-state
  - Cy / phys attacks: coms, chem, RR, pipe infra
- **2009 CDX: remote, mountainous Tajikistan**
  - U.S., Taj, Kazakhstan, Kyrgyzstan, Afghanistan

# Baltic Cyber Shield

- 10-11 May 2010
  - 7 northern European countries
  - 6 national BTs
  - 20-hacker internat'l RT
- “Live-fire” CDX
  - Unscripted battle
  - Malicious code both authorized and encouraged
    - Within virtual battlefield

# Inspiration

- U.S. National Collegiate Cyber Defense Competition
- International Cyber Defense Workshop (ICDW)
- UCSB International Capture the Flag (iCTF)
- Annual U.S. military CDXs
- **CCD COE-SWE CDX, Dec 2008**



# BCS 2010 Scenario

- Exploration of “cyber terrorism”
- Target: power supply company
  - CII / SCADA infrastructure
- Blue Teams
  - SIT: sec insp failure / insider fears
  - Hired-gun, Rapid Response Team
- Red Team
  - Attacks should intensify throughout CDX

# BCS Goals

1. Hands-on BT training in CII defense
  - *Cyber Defense* Exercise
2. Highlight international nature of cyberspace
  - Technical, institutional, legal, political, etc
3. Improve future CDXs
  - “Lessons learned”
  - Survey

# White Team

- CCD CoE Tallinn, SNDC Stockholm
- **Scoring criteria**
  - Based on network CIA
    - Office infrastructure , external services
  - **+ BT points**
    - Thwarted attacks, “business requests,” innovative strategies and tactics
  - **– BT points**
    - Criticality of system, service, compromise
    - Admin/Root, SCADA PLC

# Green Team

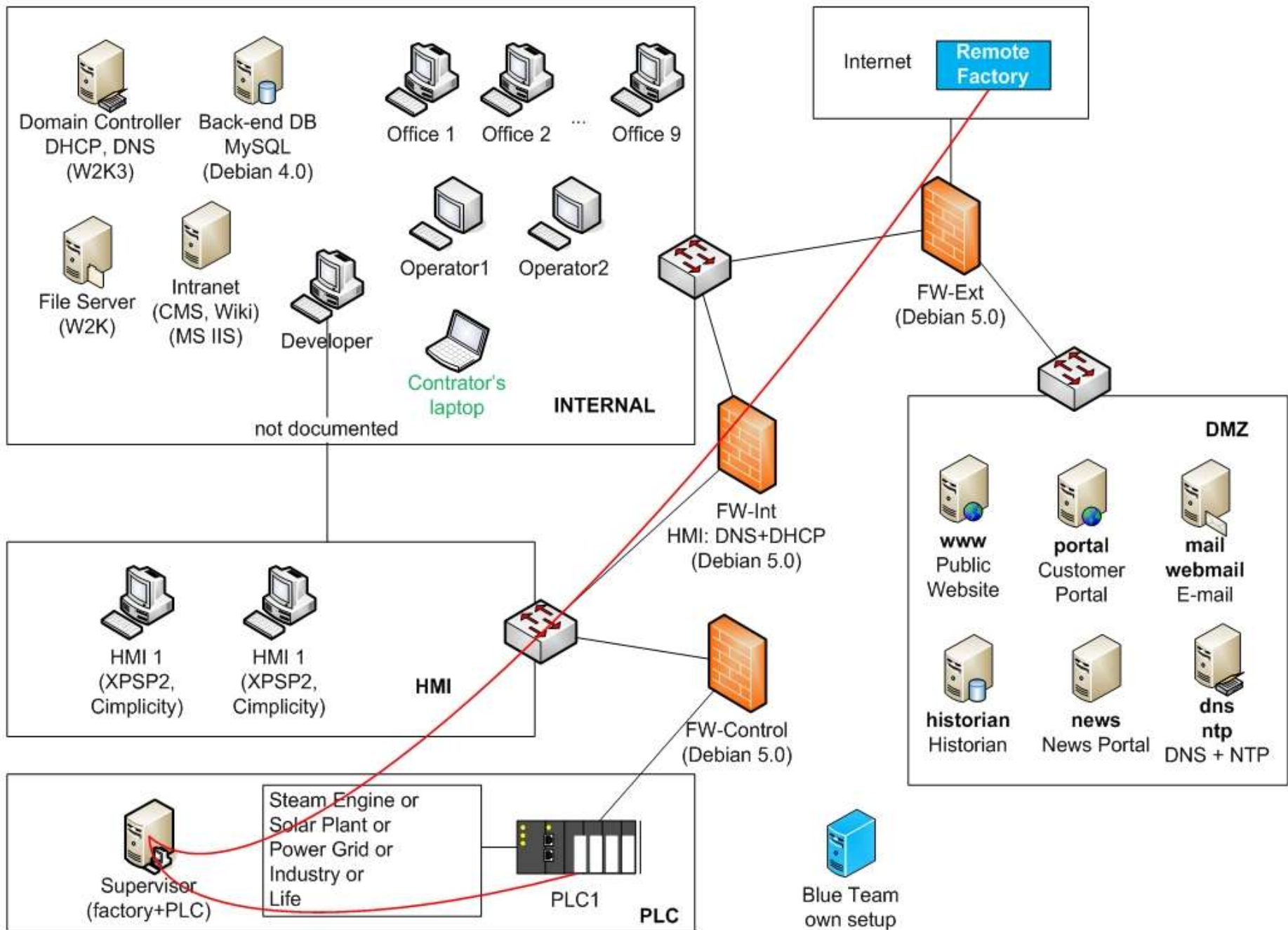
- **Swedish Defence Research Agency (FOI)**
  - Linköping, Sweden
  - Hosted most CDX infrastructure
  - 9 racks, 20 physical servers each
  - BT nets designed by GT & WT
- 12 miniature factories
  - Each:1 butane flame to “detonate”
- RT / BTs accessed game via OpenVPN

# Blue Teams

- 6 BTs
  - 6-10 personnel each
  - Northern Euro gov, mil, priv sec, academia
- **Network: identical, pre-built, fairly insecure**
  - 20 physical PC servers, 28 virtual machines
  - 4 VLAN segments: DMZ, INTERNAL, HMI, PLC
  - Many elements unpatched, vuln, misconfig, poor paswrds, keys, some pre-planted malware

# Game Environment

- 2x 2.2GHz Xeon processors
- 2 GB RAM
- 80 GB HDD
- 2 10/100Mbit Ethernet interfaces
- VMware Server 2.0.2 on Gentoo Linux
- 2 segments: management / game



# BCS SCADA

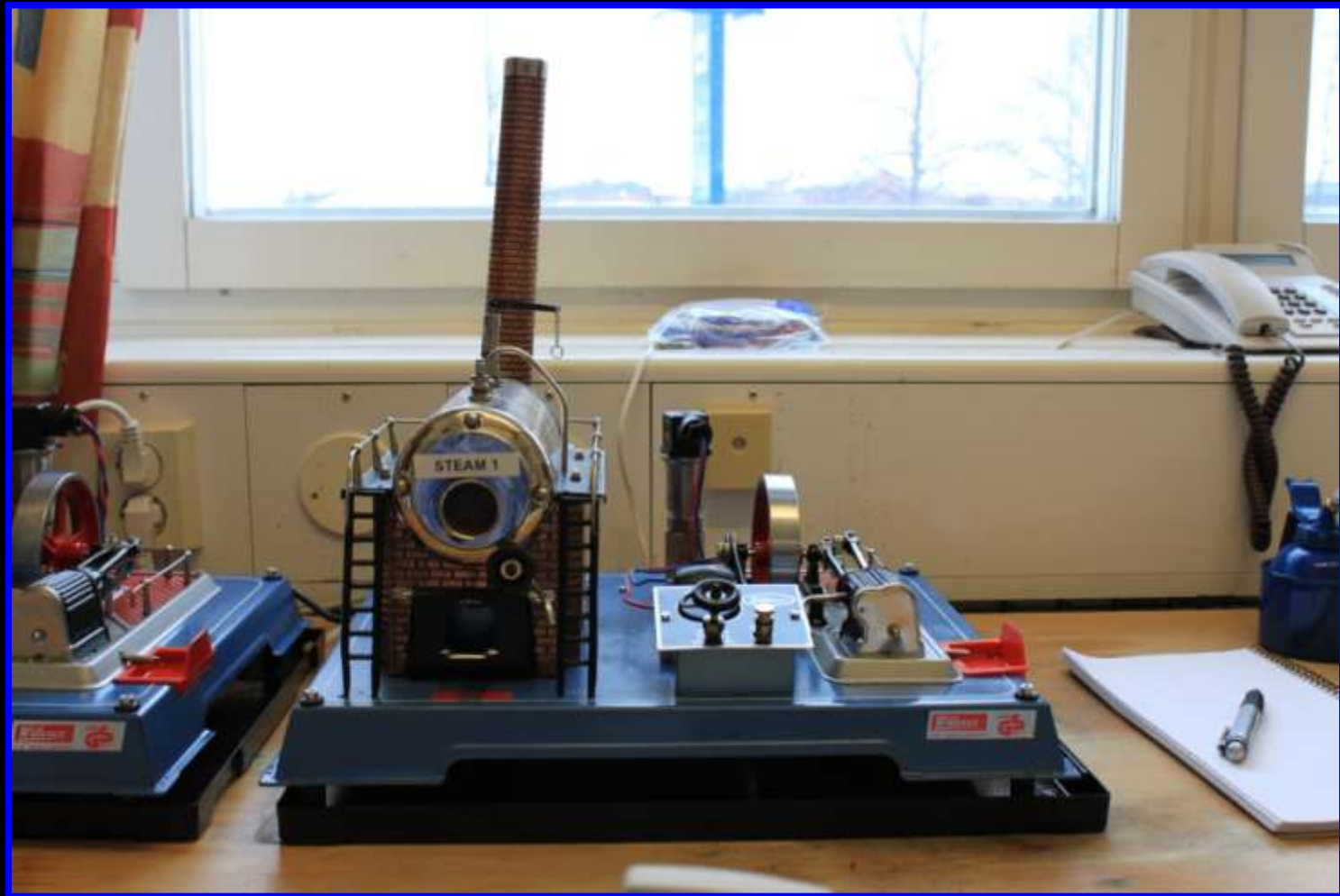
- Sim: power generation company
  - Production, management, distribution
  - GE PLCs
  - Cimplicity HMI terminals
  - Historian databases
- 2 model factories per BT net



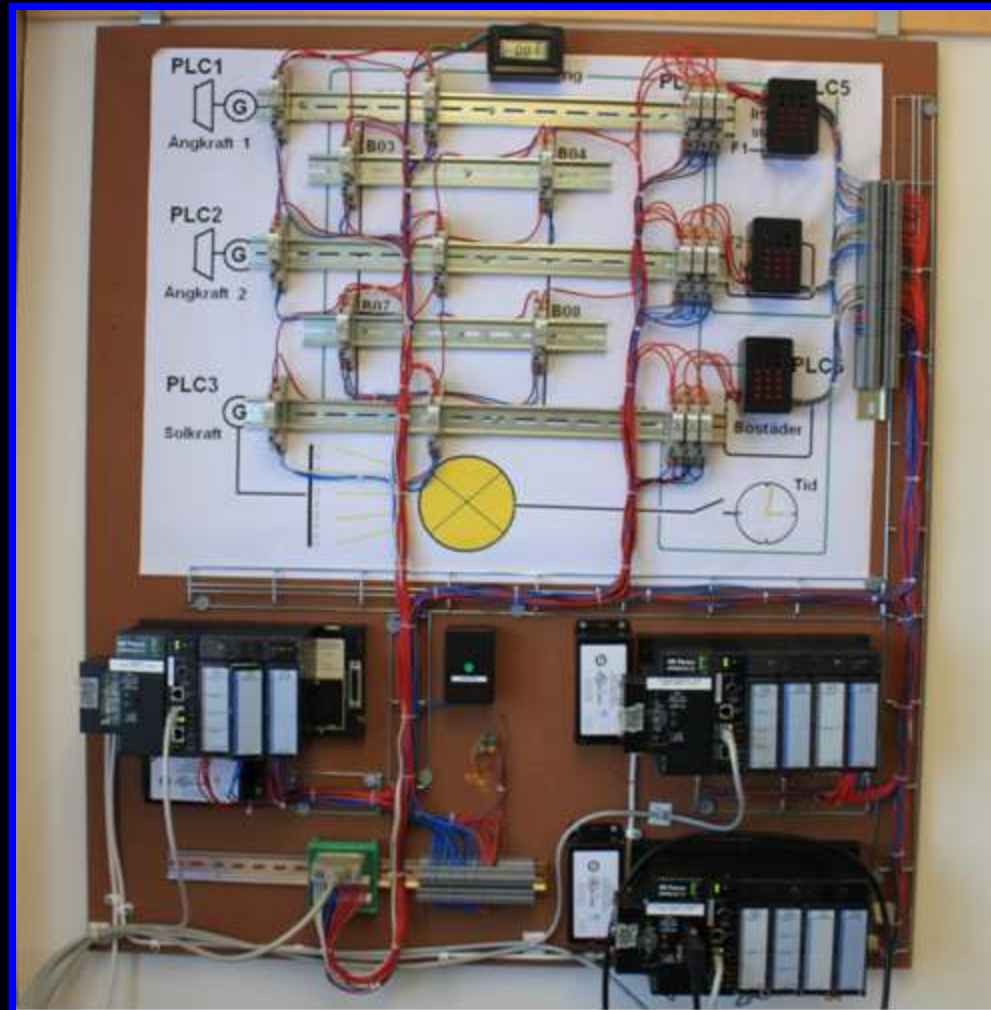
# Model Factories



# Model Steam Engine



# GE PLC



# Hardening the Network

- BTs did not have prior access to CDX environment
  - Given somewhat outdated network docs
- **Could install / modify existing SW**
  - Min #, type of apps & services required
  - Offensive BT cyber attacks prohibited
    - Vs RT or other BTs

# Red Team

- 20 volunteer angry environmentalist h4x0r5
  - Attacks should begin slowly, intensify
  - No limit on hacker tools & techniques vs BTs
  - Could not attack CDX infrastructure
  - Attacks confined to CDX environment
- Internally, four sub-teams
  - “Client-side,” “fuzzing,” “web app,” “remote”
- Early CDX access, sim prior recon

# Visualization

- Network topography
- Traffic flows
- Chat channels
- Team workspaces
- Observer reports
- Terrestrial map
- **Scoreboard**





2010-05-10 04:54:00  
2010-05-10 04:49:04



Flows Identities Ports Topology

### Red + Scoring



### Factories

Blue1 Factory Blue2 Factory Blue3 Factory Blue4 Factory Blue5 Factory Blue6 Factory



### IPX

### White



### Blue1

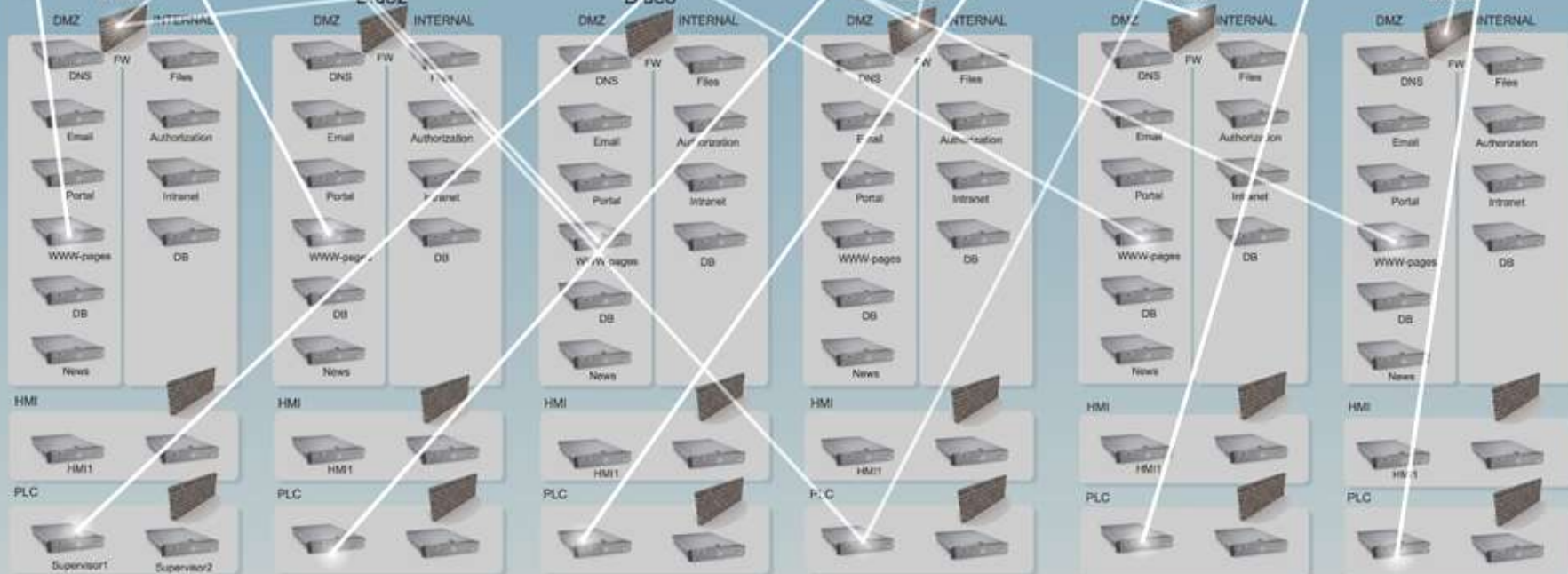
### Blue2

### Blue3

### Blue4

### Blue5

### Blue6







2018-2019  
CCDCOE

# RT Campaign

- **Four phases**
  1. Declaration of war
  2. Breaching the castle wall
  3. Owning the infrastructure
  4. Wanton destruction

# Declaration of War

- Hacker ultimatum
  - RT must deface each BT website
  - “Cease operations & convert to green power...”
    - “...or face crippling cyber attack!”
  - Extremist environmental organization
    - “K3 c1b3r w4rf4r3 d1v1s10n”
  - RT defaced 5 of 6 sites w/in 30 minutes

# Phase One

- WT allowed RT to compromise only:
  - 1 server in each BT DMZ
  - 1 INTERNAL workstation
- Still, RT created steady stream of incident reports
  - EX: in 1 hour, RT had live A/V feed from BT workspace
  - WT had trouble scoring all incidents

## Phase Two

- RT: compr as many DMZ / INTERNAL as possible
  - First day: 42 kills, incl web, email servers
  - MS-SQL SCADA rept server
- Historical CDX challenge
  - Balanced, sustained RT pressure on all BTs
  - WT directive: for each vuln, all BT sys checked
- For Red Team, was BCS config too easy?
  - Maybe not: 2 BTs kept RT out of INTERNAL nets

# Phase Three

- Steal BT “crown jewels”
  - Human Machine Interface (HMI)
    - Power management
    - SCADA infrastructure
- RT claimed only limited victories
  - Only 1 of 12 model factories set on fire
    - Intentional or accidental?

# 1300Z: Boom!



# diff: RT vs State Actor

- RT did not understand factory processes
  - How to blow them up?
- Hypothesis
  - The one factory blown up was due to fuzzing attack vs Modbus protocol
- More RT / GT communication, training could help



## Phase Four

- “Wanton destruction”
  - Attack / destroy any BT system
  - Desperate attempt to cause max taret dmg
- Not a wise CDX decision
  - RT DoS’d previously conquered systems
    - EX: Custom-config Cisco router DoS
  - Prevented WT from accurately scoring game

# Vulns and Exploits

- RT compromised 80 BT computers
- Publicly-known vulns
  - MS03-026, MS04-011, MS06-040, MS08-067, MS10-025, flaws in VNC, Icecast, ClamAV, SQUID3
- Hacked web applications
  - Joomla and Wordpress
  - SQL injection, local / remote file inclusion, path traversal, XSS vs Linux / Apache / Mysql / PHP

# Vulns and Exploits 2

- Account cracking, online brute-forcing, DoS with fuzzing tools, password hash dumps, “pass-the-hash,” Slowloris vs Apache, NTP daemon and Squid3 web proxy DoS, SYN flood
- Backdoors: poison ivy, Zeus, Optix, netcat, custom-made code; Metasploit used to deploy reverse backdoors
- Crontab changes: eg, drop firewall rules
- **One zero-day client-side exploit for most browsers**

## And the Winner is...

- Essential services moved to custom-built, higher-security virtual machine
  - NTP, DNS, SMTP, WebMail
- Domain Controller: IPsec filtering
- “Out-of-band” communications
  - Did not trust in-game e-mail
- Preexisting malware found and disabled
- After initial MS-SQL loss, no Conf/Integ points lost

# Successful BT Strategies

- **Linux**
  - AppArmor, Samhain, custom short shell scripts
- **Windows**
  - AD group policies, CIS SE46 Computer Integrity System, KernelGuard, central collection of logs
- **All OSs**
  - White/blacklisting, IP blocking/black hole routing

# Goals Met? 1

## 1. Successful “live fire” CDX

- BTs tasted defense of CII / SCADA
- “Cyber terrorist” scenario explored
- Very little down-time reported

## 2. International composition of teams

- >100 personnel, >7 countries
- Numerous cross-border relationships strengthened

# Lessons

- **More WT manpower**
  - Coms, scoring, observation, adjudication
  - 1 WT per BT, 2 WT for RT (trust issues)
- **One pre-CDX “mechanics” day**
  - Strength-test all connectivity, bandwidth
  - Make rules and scoring crystal clear
- “Dumb users” req’d or no client-side attacks
  - Wasted browser 0-day (affected SCADA sim)

## Lessons 2

- **No VMWare Server Console**
  - Too big, too slow, too particular
- **BTs should have some net admin rights**
- Authoritative team leaders from start
  - Big project = some clashing agendas, egos
- Lawyer on WT
- No “wanton destruction” phase



# Final Thought

- CDX challenges  $\approx$  real world challenges
  - IT
    - Complicated, dynamic, polymorphic, evolving
    - Defenders may not see same attack twice
  - Intangible nature of cyberspace
    - Victory, defeat, battle damage can be highly subjective
    - *Sub Rosa* Cyber War

# Estonian Cyber Defense League



# References

- Adams, J. (2001). "Virtual Defense," *Foreign Affairs* 80(3) 98-112.
- "Air Force Association; Utah's Team Doolittle Wins CyberPatriot II in Orlando." (2010, Mar 10). *De-fense & Aerospace Business*, p. 42.
- Bliss, J. (2010, Feb 23) "U.S. Unprepared for 'Cyber War', Former Top Spy Official Says," *Bloomberg Businessweek*, online.
- Caterinicchia, D. (2003, May 12) "Air Force wins cyber exercise." *Federal Computer Week*, 17(14), p. 37.
- Chan, W. H. (2006, Sep 25). "Cyber exercise shows lack of interagency coordination." *Federal Computer Week*, 20(33) p. 61.
- "Cyber War: Sabotaging the System." (2009, Nov 8). 60 Minutes: CBS.
- Geers K. (2010). "The challenge of cyber attack deterrence." *Computer Law and Security Review* 26(2) pp. 298-303.
- Geers, K. (2008, Aug 27). "Cyberspace and the Changing Nature of Warfare." *SC Magazine*.
- Gibbs, W. W. (2000). "RT versus the Agents." *Scientific American*, 283(6).
- Goble P. (1999, Oct 9). "Russia: analysis from Washington: a real battle on the virtual front." *Radio Free Europe/Radio Liberty*.
- Gomes, L. (2003, Mar 31). "How high-tech games can fail to simulate what happens in war." *Wall Street Journal*.
- Gorman, S. (2009, Aug 17) "Cyber Attacks on Georgia Used Facebook, Twitter, Stolen IDs." *Wall Street Journal*.
- "International cyber exercise takes place in Tajikistan." (2009, Aug 6). *BBC Monitoring Central Asia*. (Avesta website, Dushanbe)

# References cont'd

- Keizer, G. (2009, Jan 28). "Russian 'cyber militia' knocks Kyrgyzstan offline." Computerworld.
- Lam, F., Beekey, M., & Cayo, K. (2003). "Can you hack it?" Security Management, 47(2), p. 83.
- Lawlor, M. (2004). "Information Systems See Red." Signal 58(6), p. 47.
- Lewis, J.A. (2010) "The Cyber War Has Not Begun." Center for Strategic and International Studies.
- Libicki, M. (2009). "Sub Rosa Cyber War." *The Virtual Battlefield: Perspectives on Cyber Warfare*.
- Meserve, J. (2007, Sep 26). "Sources: Staged cyber attack reveals vulnerability in power grid." CNN.
- Orr, R. (2007, Aug 2). "Computer voting machines on trial." Knight Ridder Tribune Business News.
- Preimesberger, C. "Plugging Holes." (2006). eWeek, 23(35), p. 22.
- "Remarks by the President on Securing our Nation's Cyber Infrastructure." (2009). The White House: Office of the Press Secretary.
- "Tracking GhostNet: Investigating a Cyber Espionage Network." (2009). Information Warfare Monitor.
- Verton, D. (2003) "Black ice." Computerworld, 37(32), p. 35.
- Verton, D. (2002). *The Hacker Diaries: Confessions of Teenage Hackers*. New York: McGraw-Hill/Osborne.
- Wagner, D. (2010, May 9). "White House sees no cyber attack on Wall Street." Associated Press.
- Waterman, S. (2008, Mar 10). "DHS stages cyberwar exercise." UPI.
- "'USA Today' Website Hacked; Pranksters Mock Bush, Christianity." (2002, JUL 11). Drudge Report.



Live-Fire Exercise:  
*Baltic Cyber Shield 2010*

Kenneth Geers

Naval Criminal Investigative Service (NCIS)

Cooperative Cyber Defence Centre of Excellence (CCD COE)