

Cyberdyne Systems wins Air Force "botnet" contract

6/17/2008 — **ROME, N.Y.** (AFP) — The Air Force Research Laboratory's Information Directorate has awarded a \$95,137,560 contract to Cyberdyne Systems Corp. of Sunnyvale, Calif., to develop a botnet that enhances computer network security and provides for national defense.

The three-year agreement is a follow-on to an award to develop a "World Infrastructure Security Environment (WISE) Berkeley Open Infrastructure for Network Computing (BOINC)" middleware system that links all Air Force desktop & laptop computers in a "grid computing" infrastructure. That work was funded at Congressional direction under the federal Small Business Innovative Research program, with research focusing on utilizing **autonomous software agents** previously developed by Cyberdyne Systems.

"The goal of this research will be to develop technology to provide a more comprehensive, secure network environment," said Miles Bennett Dyson, head of Cyberdyne special projects and the program manager for the creation of an Air Force botnet. "We will provide software, testing and evaluation reports and demonstrations of the intended evolutionary 'version 2.0' of the WISE-BOINC concept."

"The WISE-BOINC program contemplates providing near-term technology solutions to the improvements of information assurance efforts, as well as researching long-term, innovative compumetric warfare solutions to information security concerns," Mr. Dyson explained.

"While initially intended to assimilate Air Force and other Department of Defense systems in pursuit of classified grid computing projects, the technology developed under this program will most likely be transitioned to a variety of commercial applications that can leverage the unused computing power on corporate networks without regard to nation-state boundaries."

The concept of a military-run botnet was conceptualized by and will also be supervised by Colonel Charles W. Williamson III, the Staff Judge Advocate for the Air Force Intelligence, Surveillance and Reconnaissance Agency at Lackland AFB, Texas. "Hackers often use botnets to generate spam," Col. Williamson explained, "but their real strength lies in their ability to generate massive amounts of Internet traffic and direct it against a small number of targets. This is called a distributed denial of service (DDOS) attack. The effect is that the target computers are cut off from the Internet."

Col. Williamson explained that a botnet is a truly devastating force multiplier. "Because communication is often a computer's main purpose, a compromised computer might as well be a rock. While preparation and money can help target computers defend themselves, once under attack, they have little ability to recover."

According to Col. Williamson, the Cyberdyne contract includes a clause that says civilian computers will not be infected or enslaved as "zombies" under the control of an Air Force botnet. "We can build enough power over time with our own [government] resources," he said, using "computers attached to the Nonsecret Internet Protocol Network (NIPRNet). Once the system reaches a level of maturity, it can [autonomously] add other .mil computers, then .gov machines" at the direction of the National Command Authority.

Col. Williamson also assured that the contract with Cyberdyne will "protect against fratricide by having filters to prevent attacks against .mil, .gov or registered allied addresses, unless specifically overridden" by the National Command Authority. He stressed that other countries have nothing to fear so long as their citizens' computers and their corporate networks don't participate in an attack against the United States. "A U.S. defensive DDOS attack on a neutral country, or on multiple neutral countries, will certainly require the U.S. to explain itself," he declared. This is a situation the National Command Authority would never want to be in.

While all military weapons can, and do, sometimes kill "collateral" civilians, Col. Williamson assured that an Air Force botnet will not "kill someone" if the weapon misfires against a hospital or an emergency services network. "The risk of this occurring is overblown," he explained. "Hospitals and emergency services already need backup plans in case of many exigencies from natural causes, including the types of power and



Search

search Air Force Lin >>>

> Advanced Search

Week In Photos: 11/24/06



Featured AF Links

[AF 60th Anniversary](#)
[AF Bandstand Player](#)
[AF Posture Statement](#)
[AF Media Center](#)
[AF Mission](#)
[AF Senior Leadership](#)
[AF Symbol](#)
[Airman Magazine](#)
[Biographies](#)
[BRAC 2005](#)
[Deployed Newspapers](#)
[Fact Sheets](#)
[Senior Viewpoints](#)
[Senior Leader](#)
[Soundbites](#)
[Week in Photos Gallery](#)
[Why I Serve](#)

Specials



Blue Summit Videos



AF Cyber Command

Letter to Airmen
CSAF Vector

New Viewpoints



How We Fight Video



AF 60th Anniversary

Other Links

[AAFES](#)
[AF Crossroads](#)
[AF Personnel Center](#)

communications outages that a [botnet-created] DDOS could cause. Also, target preparation in cyberspace can create no-strike lists just like the physical world," which would exclude hospitals, fire departments, police stations, etc.

In the final analysis, the Air Force needs Cyberdyne Systems to build an effective botnet, Col. Williamson asserted. "We cannot afford to let adversaries maneuver in that domain uncontested," he concluded. "The af. mil botnet brings the capability to help defeat an enemy attack or hit him before he hits our shores."

- [AF Crossroads](#)
- [AF Personnel Center](#)
- [AF Portal](#)
- [Air Force OneSource](#)
- [Army](#)
- [Citizen Airman](#)
- [DECA](#)
- [Defense Link](#)
- [Employer Support to the Guard and Reserve](#)
- [Freedom of Information Act \(FOIA\)](#)
- [Join the Air Force](#)
- [Marine Corps](#)
- [Multi-National Force - Iraq](#)
- [Navy](#)
- [No Fear Data](#)
- [Civil Air Patrol](#)
- [Airmen Voting Website](#)