WebMemo
Published by The Heritage Foundation

No. 1629
September 20, 2007

The Air Force's Cyber Command: Combating Electronic and Network Threats

Mackenzie M. Eaglen

The U.S. military remains extremely vulnerable in cyberspace. With threats ranging from Chinese espionage to improvised explosive devices, the U.S. Air Force has established a Cyber Command to improve both defensive and offensive capabilities. Congress and the President must fully support the effort to thwart America's adversaries in the cyber domain.

The Threat. Air Force Secretary Michael Wynne recently mused about ways in which potential enemies can harm the United States through cyber operations: Insurgents can use a radio transmitter or cell phone to detonate improvised explosive devices (the number one killer of U.S. forces in Iraq); drug traffickers can use satellite phones to obtain GPS coordinates for a nighttime cocaine drop; adversaries can steal U.S. money with a laptop computer and direct it to terrorist operations; foreign-government engineers can steal military technology to build radar or navigational jammers to counter American air superiority; and a hacker can crash military servers to disrupt operations, delay movement on the ground, and compromise command and control.

Secretary Wynne shows that adversaries' access to cyberspace is generally uncontested. Meanwhile, the Chinese military has devoted substantial resources toward computer warfare capabilities in recent years. Department of Homeland Security officials recently noted the exponentially rising number of suspicious Internet activities being reported by government agencies.

U.S. Air Force Cyberspace Command. The new Cyber Command is part of the Air Force's core mission. Beyond simply preserving Internet connectivity, securing cyberspace allows the military to launch precision weapons, destroy multiple targets simultaneously, collect infrared imagery, disrupt sensors, jam equipment to prevent remote bomb detonations, and keep forces around the globe informed and connected. According to recent Air Force doctrine, cyberspace and space-based capabilities allow the military to conduct global operations without leaving their permanent base in certain cases.

April's cyber attack on Estonia by Russian hackers highlighted the potential consequences for individuals and governments when Internet connectivity is lost. Like private citizens, U.S. federal agencies depend on the Internet for information and communication.

The National Strategy to Secure Cyberspace states, "spectrums of malicious actors can, and do, conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to America's critical infrastructures,

This paper, in its entirety, can be found at:
www.heritage.org/Research/NationalSecurity/wm1629.cfm

Produced by the Douglas and Sarah Allison
Center for Foreign Policy Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

economy, or national security." The strategy calls upon planners to improve coordination and capabilities for attack attribution and response and develop networks to detect and prevent cyber attacks as they emerge.

The 2006 Quadrennial Defense Review highlighted the need to create military capabilities to shape and defend cyberspace as well as maintain command and control capabilities that can survive electronic or cyber attacks.

This year's Air Force posture statement says the Cyberspace Command will "leverage, consolidate and integrate unique Air Force cyber capabilities and functions across the spectrum of conflict from peace, to crisis and war: command and control; electronic warfare; network warfare; and intelligence, surveillance and reconnaissance."

Strategy, Doctrine, Training, and Education. Air Force leaders are working diligently to create and codify the military's cyber strategy. Its recently released Irregular Warfare doctrine notes the expeditious value, increased situational awareness, and actionable intelligence provided by cyber capabilities that are well-suited for irregular warfare.

The Air Force is seeking to attain equally important offensive capabilities in cyberspace as well. Specifically, the irregular warfare doctrine states that a "computer network attack may hinder or disrupt insurgent operations, or at least require them to expend resources defending their cyberspace assets." This doctrine capitalizes on the numerous opportunities to directly target insurgents or to positively influence an online civilian population.

Lt. Gen. Robert J. Elder, Jr., in charge of standing up the Cyber Command, is currently developing a cyber concept of operations. He is also working in tandem with Air Education and Training Command to create for the military a professional cyber education and to establish a cyber career path with the associated training and development.

Military success in the 21st century requires the ability to deter, and protect from, cyber attacks and to strike at enemies in the cyber domain. Secretary Wynne summarized it best: "Without cyber dominance, operations in all of the other domains are in fact placed at risk."

Conclusion. The time is long overdue for the United States to do what is necessary to secure cyberspace. While the U.S. Strategic Command has overall responsibility for the military's cyber security efforts, all the services must invest the resources and attention necessary for developing offensive and defensive cyber capabilities. Air Force leaders have looked beyond the mission in Iraq and have started to prepare for the next conflict—which could involve the cyber domain.

Chief of Staff General Moseley has stated flatly that the Air Force needs an additional $20 billion annually to repair and replace aging aircraft. As the Air Force continues to plead for additional funding, Congress and the President must fully fund the Cyber Command in next year's defense budget. Policymakers must also support the effort to train professional cyber operators and provide them with a rewarding career path in the armed services.

—Mackenzie M. Eaglen is Senior Policy Analyst for National Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.