

Red Team Project Meetup

Launch and Hack Night

“The term ‘cyber’ is cool”

-- No one ever

κυβερνάω (kubernao)




https://commons.wikimedia.org/wiki/File:Official_Portrait_of_President_Reagan_1981.jpg



<https://www.reaganlibrary.gov/sites/default/files/archives/photographs/large/c8087-8a.jpg>

WarGames' and Cybersecurity's Debt to a Hollywood Hack



From left, Dabney Coleman, Matthew Broderick and Ally Sheedy in "WarGames" (1983). The film led to the nation's first directive about computer security. MGM

By Fred Kaplan

Feb. 19, 2016

Movies rarely influence public policy, but Washington's policies on cyberattacks, computer surveillance and the possibility of cyberwarfare were directly influenced by the 1983 box-office hit "[WarGames](#)."

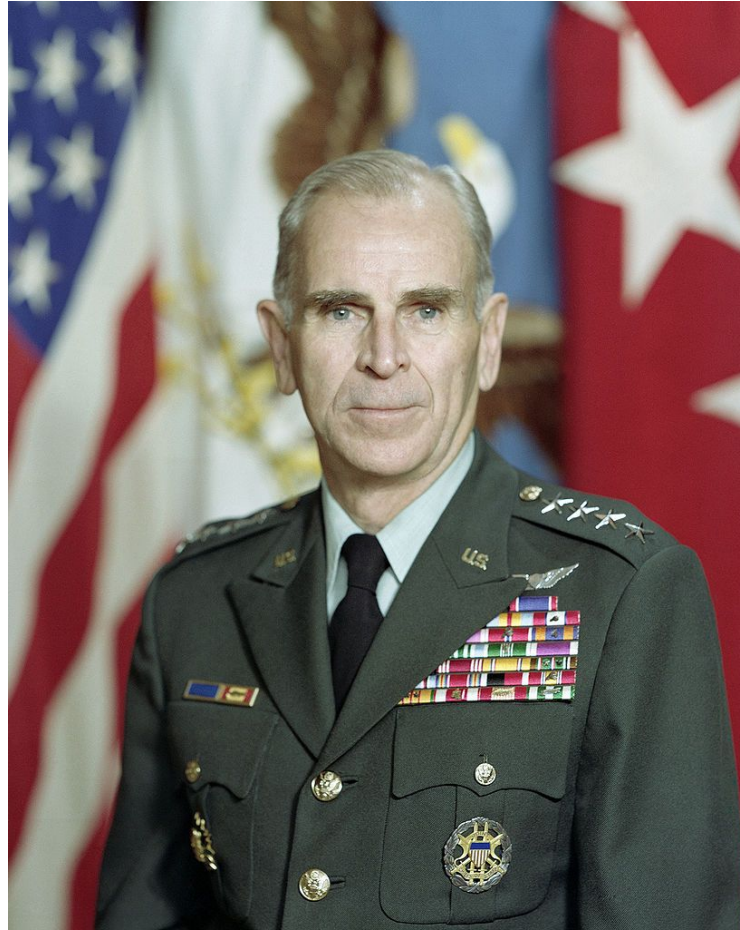
Subscribe for \$1 a week. SEE MY OPTIONS

Dark Territory

The Secret History of Cyber War

Fred Kaplan

ISBN-13: 978-1476763262



https://commons.wikimedia.org/wiki/File:Gen_John_Vessey_Jr.JPG

~~CONFIDENTIAL~~

THE WHITE HOUSE

UNCLASSIFIED

WASHINGTON

September 17, 1984

~~CONFIDENTIAL~~
UNCLASSIFIED

National Security Decision
Directive Number 145

NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY (U)

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation. (U)

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities. (U)

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns

12/7/92
Declassified/Released on
under provisions of E.O. 12958
by S. Tuley, National Security Council

UNCLASSIFIED

~~CONFIDENTIAL~~
UNCLASSIFIED

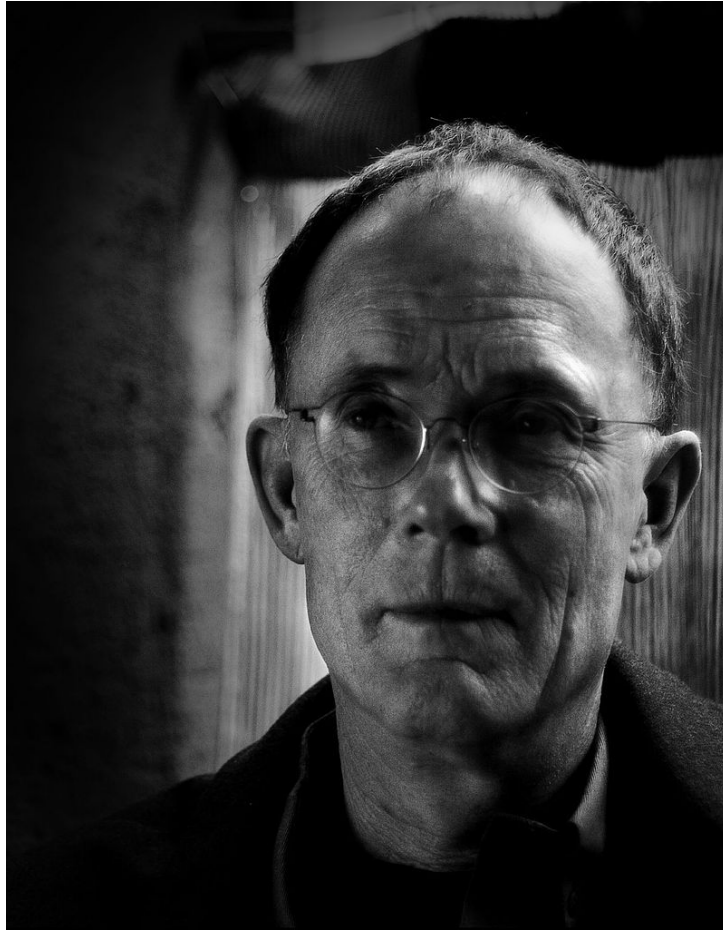
~~CONFIDENTIAL~~

CRITICAL FOUNDATIONS

PROTECTING AMERICA'S
INFRASTRUCTURES

The Report of the
President's Commission
on Critical Infrastructure Protection





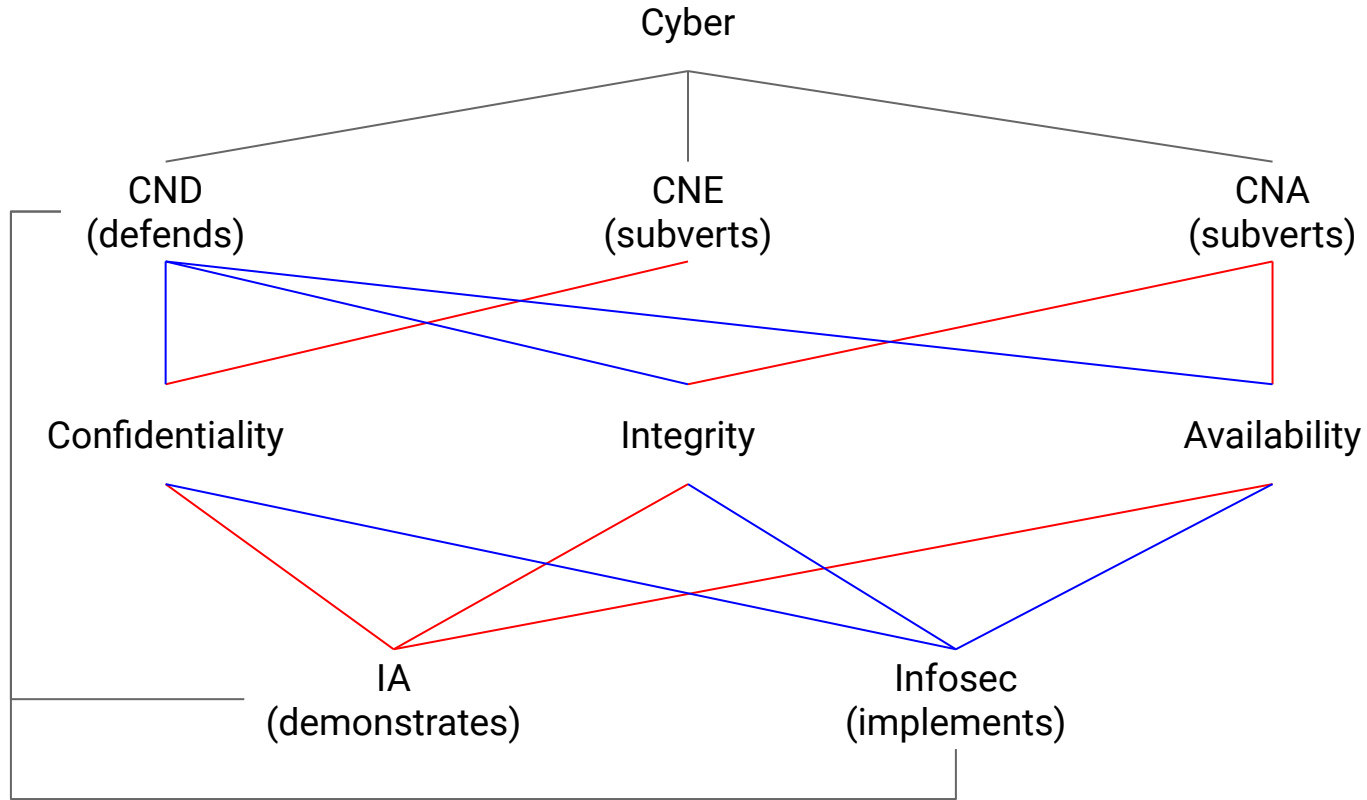
https://commons.wikimedia.org/wiki/File:William_Gibson_60th_birthday_portrait.jpg

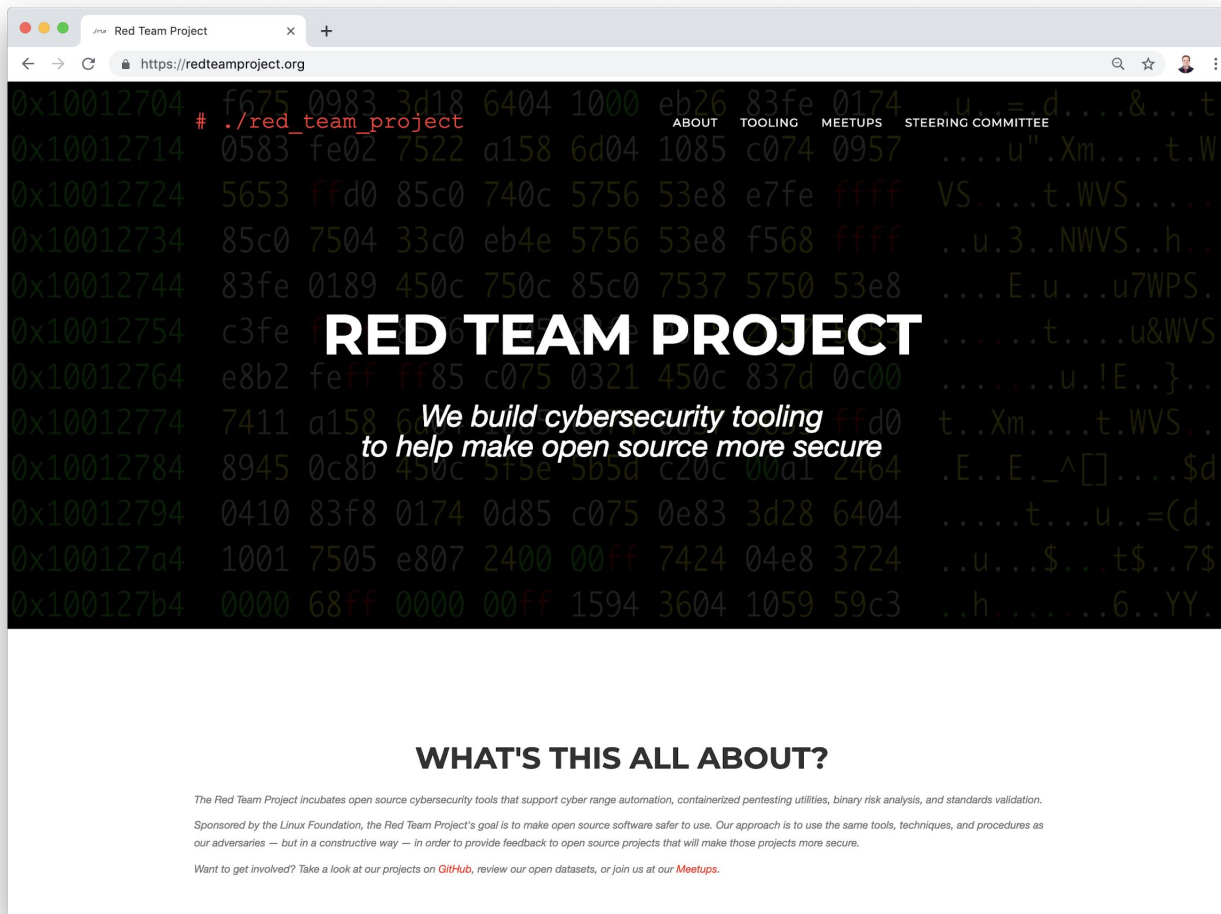
INFORMATION OPERATIONS INTEGRATION INTO JOINT OPERATIONS (NOTIONAL)						
Core, Supporting, Related Information Activities	Activities	Audience/ Target	Objective	Information Quality	Primary Planning/ Integration Process	Who does it?
Electronic Warfare	Electronic Attack	Physical, Informational	Destroy, Disrupt, Delay	Usability	Joint Operation Planning and Execution System (JOPEs)/ Targeting Process	Individuals, Governments, Militaries
	Electronic Protection	Physical	Protect the Use of Electro-magnetic Spectrum	Security	JOPEs/Defense Planning	Individuals, Businesses, Governments, Militaries
	Electronic Warfare Support	Physical	Identify and Locate Threats	Usability	Joint Intelligence Preparation of the Battlespace(JIPB)/SIGINT Collection	Militaries
Computer Network Operations	Computer Network Attack	Physical, Informational	Destroy, Disrupt, Delay	Security	JIPB/JOPEs/Targeting Process	Individuals, Governments, Militaries
	Computer Network Defense	Physical, Informational	Protect Computer Networks	Security	JOPEs/J-6 Vulnerability Analysis	Individuals, Businesses, Governments, Militaries
	Computer Network Exploitation	Informational	Gain Information From and About Computers and Computer Networks	Security	JIPB/Targeting Process	Individuals, Governments, Militaries
Psychological Operations	Psychological Operations	Cognitive	Influence	Relevance	JOPEs/Joint Operation Planning	Businesses, Governments, Militaries
Military Deception	Military Deception	Cognitive	Mislead	Accuracy	JOPEs/Joint Operation Planning	Militaries
Operations Security	Operations Security	Cognitive	Deny	Security	JOPEs/Joint Operation Planning	Businesses, Governments, Militaries
Supporting Capabilities	Information Assurance	Informational	Protect Information and Information Systems	Security	JOPEs/J-6 Vulnerability Analysis	Businesses, Governments, Militaries
	Physical Security	Physical	Secure Information and Information Infrastructure	Usability	JOPEs/Defense Planning	Businesses, Governments, Militaries
	Physical Attack	Physical	Destroy, Disrupt	Usability	JOPEs/Joint Operation Planning	Governments, Militaries
	Counterintelligence	Cognitive	Mislead	Accuracy	JIPB/Human Intelligence Collection	Governments, Militaries
	Combat Camera	Physical	Inform/Document	Usability, Accuracy	JOPEs/Joint Operation Planning	Governments, Militaries
Related Capabilities	Civil Military Operations	Cognitive	Influence	Accuracy	JOPEs/Joint Operation Planning	Governments, Militaries
	Public Affairs	Cognitive	Inform	Accuracy	JOPEs/Joint Operation Planning	Businesses, Governments, Militaries
	Public Diplomacy	Cognitive	Inform	Accuracy	Interagency Coordination	Governments

Figure I-3. Information Operations Integration into Joint Operations (Notional)



https://commons.wikimedia.org/wiki/File:Seal_of_the_United_States_Cyber_Command.svg





Red Team Project - Focus Areas



Cyber Range Automation



Binary Risk Quantification



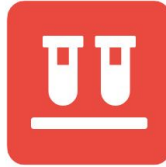
Standards Advancement

Red Team Project - Tooling



Linux Exploit Mapper

LEM scans a Linux system for local exploits and maps them to known exploit code.



Exploit Curation

LEM-mapped exploits are **curated**, i.e., tested for efficacy and ease-of-use using a variant of the STRIDE scoring mechanism



cyber-range-target

An Ansible role called **cyber-range-target** is used to deliberately downgrade OS packages to a version vulnerable to a given CVE



Red Container

Red Container offers containerized pentesting tooling, which can be launched from whole OSES or containerized environments like Kubernetes



Training Labs

Cyber range **training scenarios** that automatically launch and configure the cyber range via Deployment Manager and Ansible



Compliant

Automatically apply DISA STIG settings to OS instances

Red Team Project - Meetups



Featured Speaker

Come hear luminaries from the offensive security community. (Washington, DC)



Hack Nights

Learn how to use the Red Team Project tooling, contribute to our GitHub projects, and help us curate exploits. (Washington, DC)



Def Con 27

Going to Def Con? We'll be there, so let's hang out! (Las Vegas, NV)

Lab