

1. Record Nr.	UNINA9910220108903321
Autore	Molander Roger C
Titolo	Strategic information warfare [[electronic resource]] : a new face of war // Roger C. Molander, Andrew S. Riddile, Peter A. Wilson
Pubbl/distr/stampa	Santa Monica, CA, : RAND, 1996
ISBN	1-282-45126-X 9786612451263 0-8330-4846-5
Descrizione fisica	1 online resource (115 p.)
Altri autori (Persone)	RiddileAndrew S WilsonPeter A. <1943->
Disciplina	355.343
Soggetti	Information warfare Strategy
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"National Defense Research Institute." "Prepared for the Office of the Secretary of Defense."
Nota di contenuto	Cover; PREFACE; CONTENTS; FIGURES; TABLES; SUMMARY; ACKNOWLEDGMENTS; Chapter One - WHAT IS "STRATEGIC INFORMATION WARFARE?"; INTRODUCTION; STUDY BACKGROUND; DEFENSE-ORIENTED TASKING FROM OASD(C3I); Chapter Two - METHODOLOGY; THE "DAY AFTER . . ." EXERCISE METHODOLOGY; THE EXERCISE DESIGN PROCESS; EXERCISE HISTORY; Chapter Three - THE CHANGING FACE OF WAR; Chapter Four - DEFINING FEATURES OF STRATEGIC INFORMATION WARFARE; LOW ENTRY COST; BLURRED TRADITIONAL BOUNDARIES; PERCEPTION MANAGEMENT; STRATEGIC INTELLIGENCE; TACTICAL WARNING AND ATTACK ASSESSMENT; BUILDING AND SUSTAINING COALITIONS Chapter Five - ISSUES OF STRATEGIC INFORMATION WARFARE RISK ASSESSMENT; NATIONAL MILITARY STRATEGY; NATIONAL SECURITY STRATEGY; U.S. GOVERNMENT ROLE; Chapter Six - CONCLUSIONS; LEADERSHIP: WHO SHOULD BE IN CHARGE?; RISK ASSESSMENT; GOVERNMENT'S ROLE; NATIONAL SECURITY STRATEGY; NATIONAL MILITARY STRATEGY; ADDITIONAL READING: THREATS AND VULNERABILITIES; Appendix A - METHODOLOGY; Appendix B -

SUMMARY OF GROUP DELIBERATIONS FOR STEP THREE; Appendix C -
EXERCISE

Sommario/riassunto

Future U.S. national security strategy is likely to be profoundly affected by the ongoing, rapid evolution of cyberspace--the global information infrastructure--and in particular by the growing dependence of the U.S. military and other national institutions and infrastructures on potentially vulnerable elements of the U.S. national information infrastructure. To examine these effects, the authors conducted a series of exercises employing a methodology known as the Day After ... in which participants are presented with an information warfare crisis scenario and asked to advise the president on