

1. Record Nr.	UNINA9910786684903321
Autore	Blunden Bill
Titolo	Behold a pale farce : cyberwar, threat inflation, & the malware industrial complex // Bill Blunden, Violet Cheung
Pubbl/distr/stampa	Walterville, OR : , : Trine Day, , [2014] ©2014
ISBN	1-937584-81-X
Descrizione fisica	1 online resource (835 p.)
Disciplina	355.343
Soggetti	Information warfare Computer security - United States
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	CoverImage; Title Page; Copyright page; Dedication; Epigraph; Table of Contents; Media Massage; Firsthand Experience; The Public Relations Industry; Behold a Pale Farce; Organization; Acknowledgments; The Wonder of it All; Part I - Rampant Hyperbole; A Backdrop of Metaphors; Never Mind: False Alarm; The Madness of Crowds; An Electronic Pearl Harbor; A Cyber-Katrina; The Hiroshima of Cyberwar; A Cyber 9/11; Dissenting Voices; The Executive Responds; Stuxnet; Plan X; Presidential Policy Directive 20; Hacking Foreign Targets for Years; Oz the Great and Powerful; Our Frenemy in Asia A Plurality of ActorsRule of Law Breaks Down; The Internet's Frontier Town; Opposing Models for Reform; The Extent of China's Capabilities; Joined at the Hip; Both Sides Keep the Other in Business; The #1 Threat to Economic Security?; Cyberwar as a Misdiagnosis; Dialing 911; Looking Ahead; Part II - A Series of Unfortunate Events; Cybercrime; The Ecosystem; A Snapshot of Cybercrime; The TJX Hack; The Heartland Payment Systems Breach; The DarkMarket Sting; The RBS WorldPay Attack; The Return of the Analyzer; The Ballad of Max Butler; Sony under Siege; The FIS Breach; The Big Picture The Punch LineEspionage; Moonlight Maze; Titan Rain; Operation Byzantine Hades; GhostNet; Joint Strike Fighter Breach; Operation Aurora; Shadows in the Cloud; Night Dragon; RSA and SecurID; Operation Shady RAT; The Nitro Attacks; Targeting Certificate

Authorities; Operation Red October; Patterns Emerge; The Scope of U.S. Espionage; The Malware-Industrial Complex; Independent Operators; Spies Abound ...; But Some Groups Spy More Than Others; The Infrastructure; The Financial System; The Power Grid; The Telecoms; Aerospace; The Internet: Denial of Service Attacks; McAfee
The Internet: Manipulating TrafficThreat Inflation; Conflicts of Interest; Part III - The Futility of Offensive Solutions; The Quandary of Attribution; Achieving Anonymity Online; The Origins of Tor; The Folly of Attribution; Deterrence; Arms Control Treaties; Shades of Orwell; The Golden Age of Surveillance; The NSA's MUSCULAR project; Opting Into Surveillance; The DHS Monitors Social Media; Corporate Compliance; The Hemisphere Project; A Global Panopticon; Coda: Extorting Privacy; Part IV - The Road to Cyber-Security; The Origins of Cyber-Insecurity; A Layered Perspective; Exciting Causes
The Software DepressionPredisposing Causes; Remote Causes; Security for The 1%; Cyber-Security for The 99 Percent; Building Resilient Software; Echoes of Ken Thompson; International Cooperation; Managing Externalities; Catch-22; Strength in Numbers; The Hazards of a Misdiagnosis; Securitization In-Depth; Threat Inflation; The Folly of Deterrence; In Search of Enemies; American Hypocrisy; Subverting Attribution; Turning to Big Brother; Root Causes of Cyber-Insecurity; Cyber-Security for the 1%; Cyber-Security for the 99%; Index

Sommario/riassunto

This book presents a data-driven message that exposes the cyberwar media campaign being directed by the Pentagon and its patronage networks. By demonstrating that the American public is being coerced by a threat that has been blown out of proportion-much like the run-up to the Gulf War or the global war on terror-this book discusses how the notion of cyberwar instills a crisis mentality that discourages formal risk assessment, making the public anxious and hence susceptible to ill-conceived solutions. With content that challenges conventional no
