1. Record Nr. UNINA9910219977703321

Autore	Libicki Martin C
Titolo	Crisis and escalation in cyberspace / / Martin C. Libicki
Pubbl/distr/stampa	Santa Monica, CA : , : RAND, Project Air Force, , 2012
ISBN	0-8330-7679-5 0-8330-7680-9
Descrizione fisica	1 online resource (279 p.)
Disciplina	358.4/141
Soggetti	Information warfare - United States Escalation (Military science) Cyberspace - Security measures Crisis management - Government policy - United States Cyberterrorism - Prevention Conflict management Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"Prepared for the United States Air Force." "Approved for public release; distribution unlimited."
Nota di bibliografia	Includes bibliographical references (pages 163-172).
Nota di contenuto	Avoiding crises by creating norms -- Narratives, dialogues, and signaling -- Escalation management -- Strategic stability -- Conclusions and recommendations for the Air Force -- Introduction -- Some hypothetical crises -- Mutual mistrust is likely to characterize a cyber crisis -- States may have room for maneuver in a cyber crisis -- A note on methodology -- Purpose and organization -- Avoiding crises by creating norms -- What kind of norms might be useful? -- Enforce laws against hacking -- Disassociate from freelance hackers -- Discourage commercial espionage -- Be careful about the obligation to suppress cyber traffic -- How do we enforce norms? -- Confidence-building measures -- Norms for victims of cyberattacks -- Norms for war? -- Deception -- Military necessity and collateral damage -- Proportionality -- Reversibility -- Conclusions -- Narratives, dialogue, and signals -- Narratives to promote control -- A narrative framework for cyberspace -- Victimization, attribution, retaliation, and aggression

-- Victimization -- Attribution -- Retaliation -- Aggression -- Emollients: narratives to walk back a crisis -- We did nothing -- Well, at least not on our orders -- It was an accident -- This is nothing new -- At least it does not portend anything -- Broader considerations -- Signals -- Ambiguity in signaling -- Signaling resolve -- Signaling that cyber combat is not kinetic combat -- Conclusions -- Escalation management -- Motives for escalation -- Does escalation matter? -- Escalation risks -- Escalation risks in phase -- Escalation risks for contained local conflicts -- Escalation risks for uncontained conflicts -- Managing proxy cyberattacks -- What hidden combatants imply for horizontal escalation -- Managing overt proxy conflict -- The difficulties of tit-for-tat management -- The importance of pre-planning -- Disjunctions among effort, effect, and perception -- Inadvertent escalation -- Escalation into kinetic warfare -- Escalation into economic warfare -- Sub rosa escalation -- Managing the third-party problem -- The need for a clean shot -- Inference and narrative -- Command and control -- Commanders -- Those they command -- Conclusions -- Implications for strategic stability -- Translating sources of cold war instability to cyberspace -- What influence can cyberwar have if nuclear weapons exist? -- Can cyberwar disarm another state's nuclear capabilities? -- Can cyberwar disarm another states cyberwarriors? -- Does cyberwar lend itself to alert-reaction cycles? -- Are cyberdefenses inherently destabilizing? -- Would a cyberspace arms races be destabilizing? -- Misperception as a source of crisis -- Side takes great exception to cyberespionage -- Defenses are misinterpreted as preparations for war -- Too much confidence in attribution -- Too much confidence in or fear of pre-emption -- Supposedly risk-free cyberattacks -- Neutrality -- Conclusions -- Can cyber crises be managed? -- A. Distributed denial-of-service attacks -- B. Overt, obvious, and covert cyberattacks and responses -- Can good cyberdefenses discourage attacks? -- Bibliography -- Figures -- Figure 1: Alternative postures for a master cyber narrative -- Figure 2: Sources of imprecision in tit for tat -- Figure 3: An inadvertent path to mutual escalation -- Figure A-1: Configuring networks to limit the damage of DDoS attacks -- Table -- Overt, obvious, and covert cyberattacks and responses.

Sommario/riassunto

The chances are growing that the United States will find itself in a crisis in cyberspace--the escalation of tensions associated with a major cyberattack, suspicions that one has taken place, or fears that it might do so soon. Such crises can be managed by taking steps to reduce the incentives for other states to step in, controlling the narrative, understanding the stability parameters of the crises, and recognizing escalation risks.