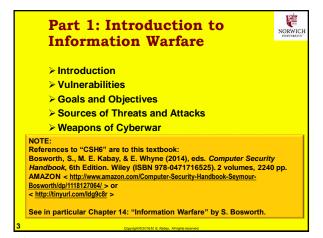
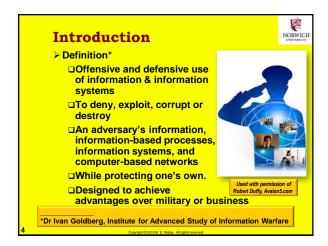
### INFOWAR: Introduction to Cyberwarfare

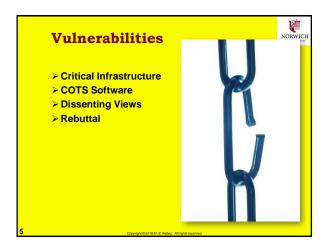
M. E. Kabay, PhD, CISSP-ISSMP

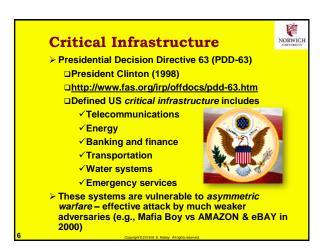
Professor of Computer Information Systems
School of Business & Management
College of Professional Schools
Norwich University

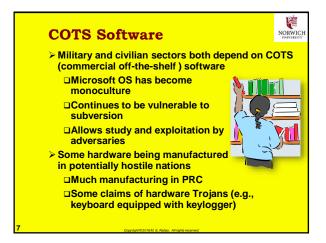


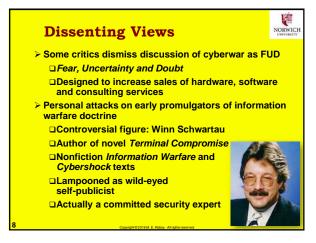


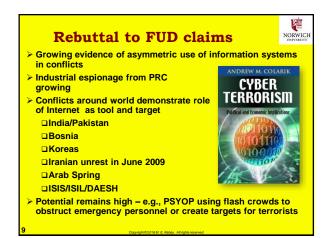




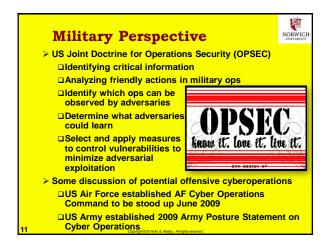






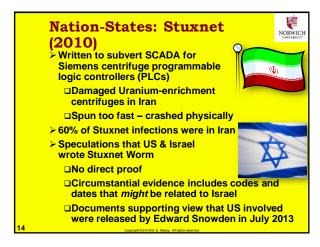


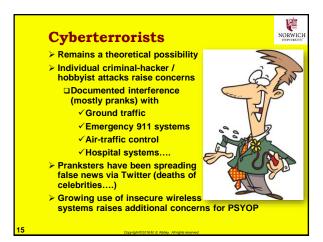


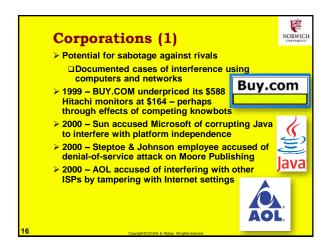




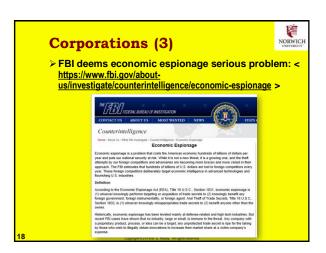










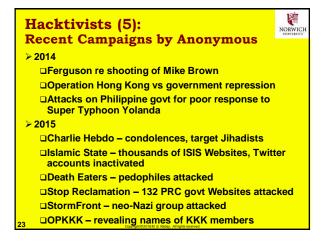


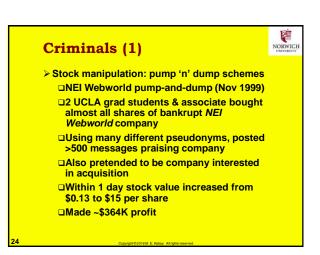


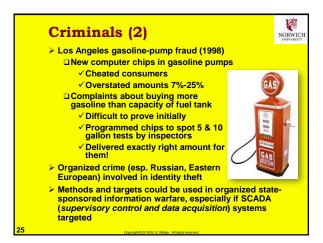


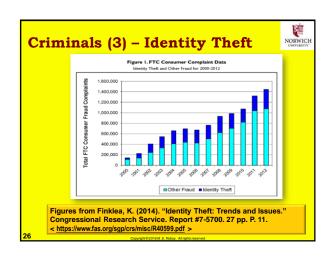


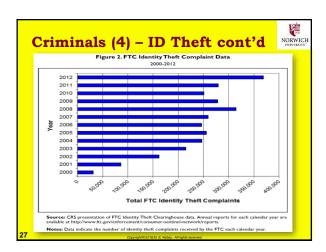


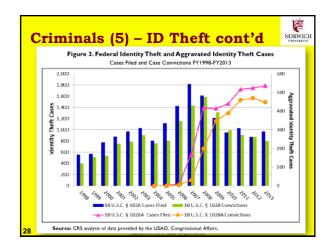


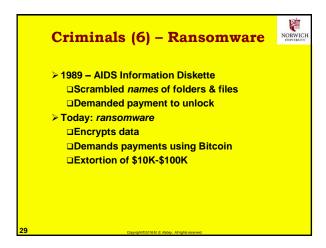


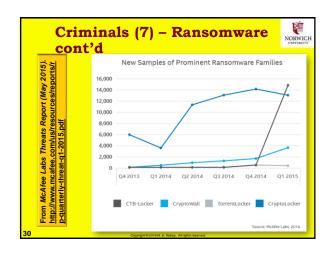




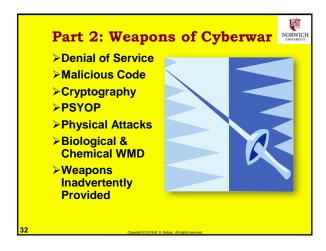


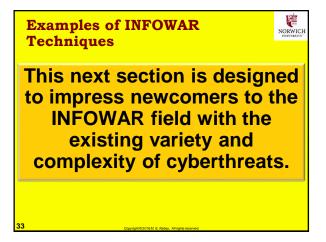


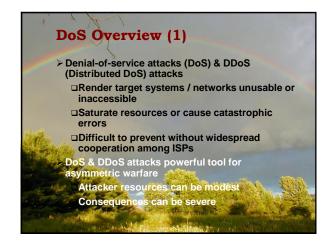


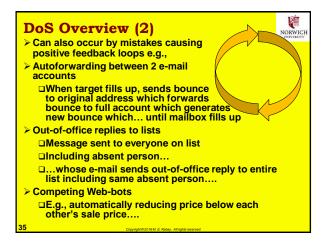


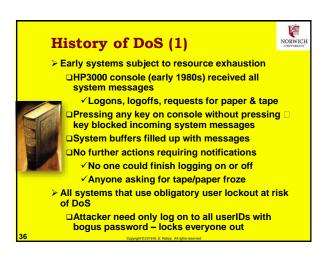






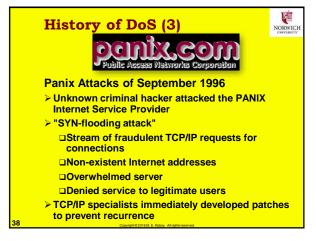


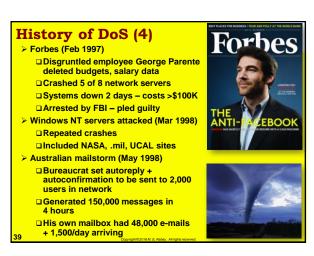


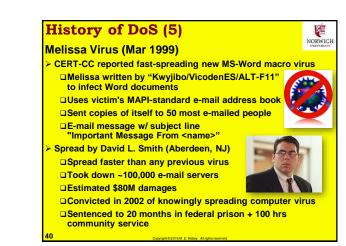


## History of DoS (2) > 1987-12: Christmas-Tree Worm | IBM internal networks | Grew explosively | Self-mailing graphic | Escaped into BITNET | Crashed systems | 1988-11: Morris Worm | Probably launched by mistake | Demonstration program | Replicated through Internet | -9,000 systems crashed or were deliberately taken off-line

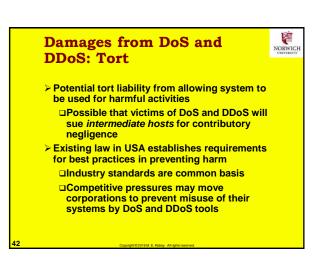
□Was about ½ to ¾ of Internet as it was then

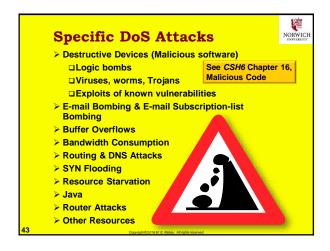


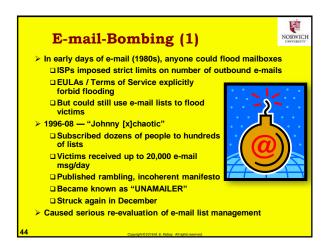


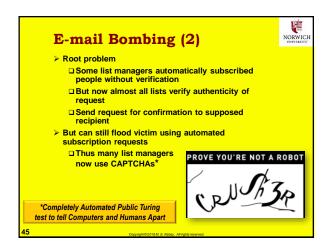


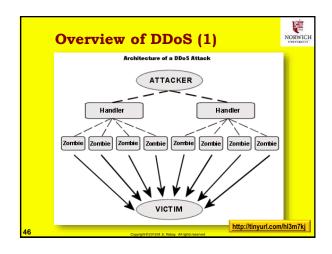


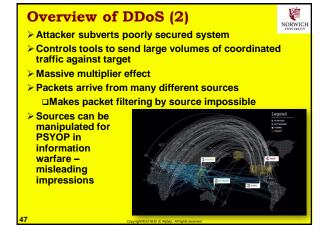


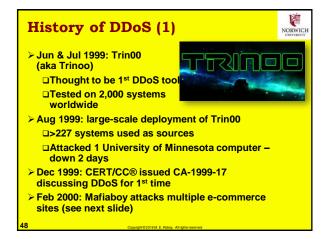


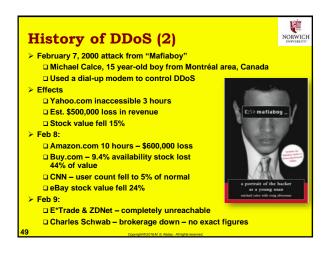


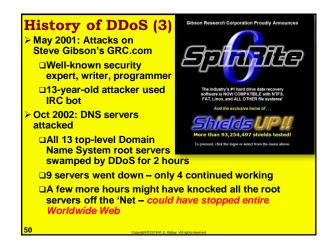


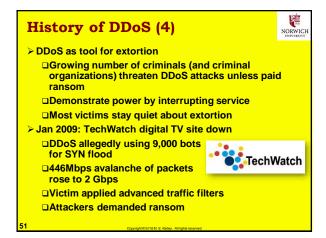




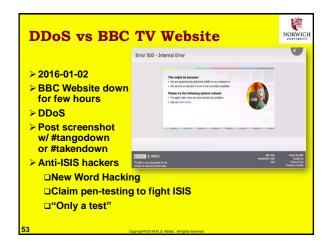








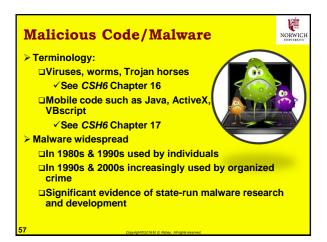


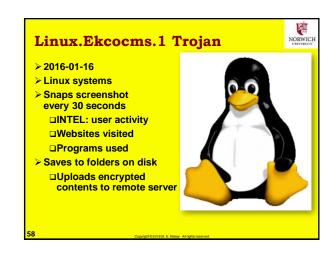




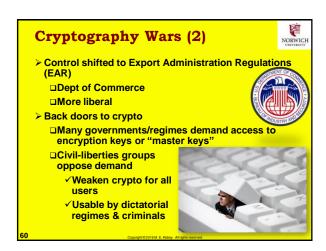


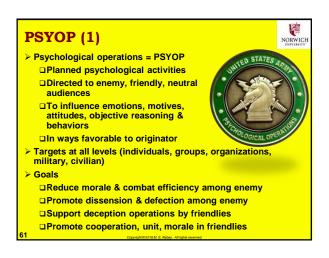


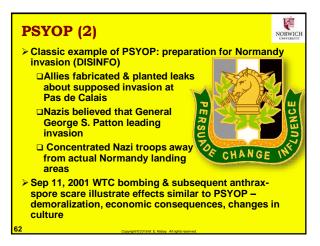


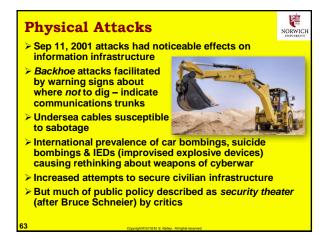










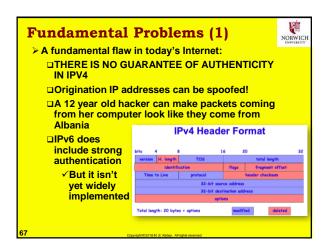


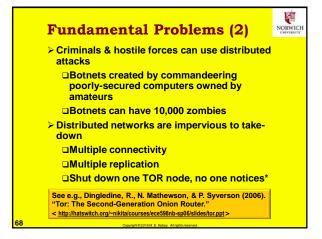


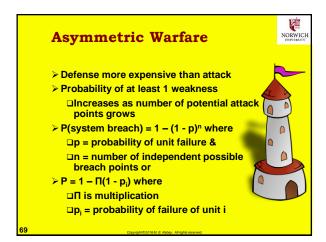


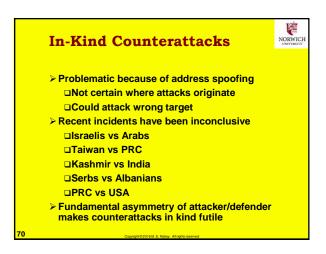


11



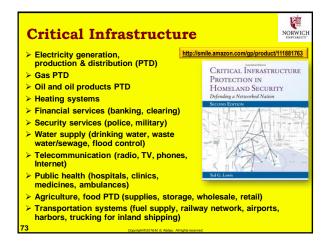




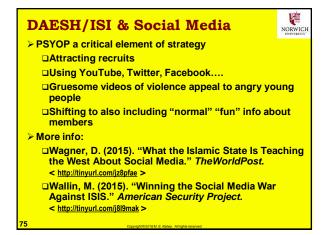






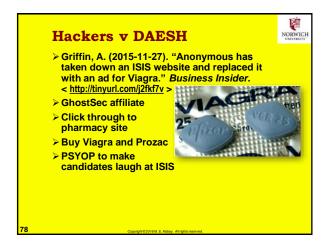




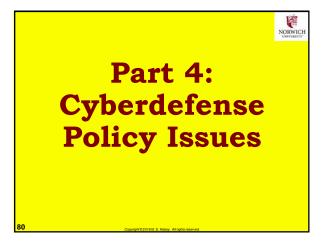


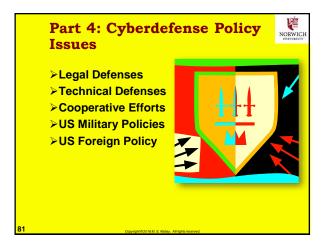






### What are the most effective measures for defending against cyberwarfare attacks? Are kinetic (conventional) warfare methods adequate / appropriate for reducing cyberattacks? How do we cope with the risk of attacking the wrong targets?







# Technical Defenses All the technical defenses used in protecting computers and networks against individual attack can be used in cyberdefense Entire contents of CSH6 apply to cyberwarfare defense Constant attention to evolving vulnerabilities and threats Special value for INTEL and COINTEL activities □Intelligence to track state and non-state actors e.g., infiltration, monitoring Internet chatter □Counterintelligence to identify spies and saboteurs



