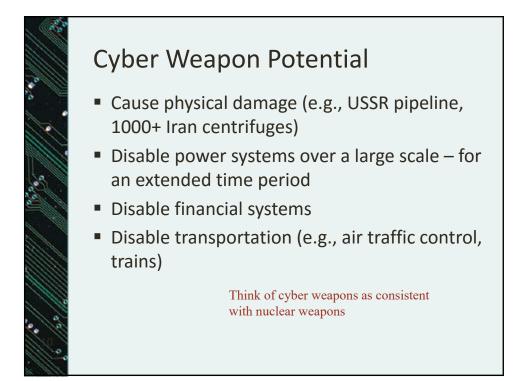




Definitions

- Politically motivated hacking to conduct sabotage and espionage
 - Cyber espionage obtaining secrets from individuals, rivals, governments, and enemies using illegal exploitation of computers, networks, and software
 - Cyber sabotage disruption of equipment such as power, water, fuel, communications and transportation

The Director of US National Intelligence defines cyber-sabotage as the top security threat to the United States







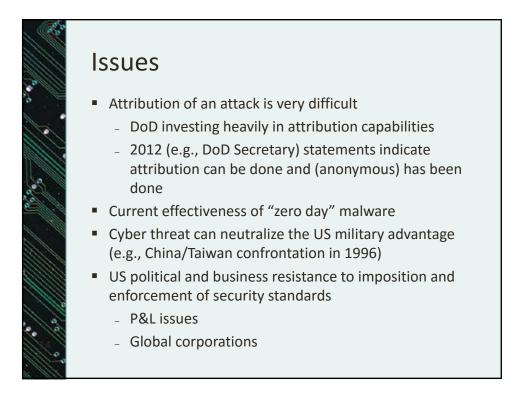


Examples

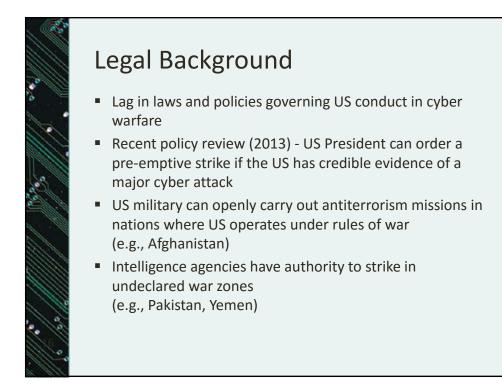
- 2009 reports of infiltration of US power grid (possibly only administrative systems)
 - By China and Russia (denied by China)
 - Left software that could potentially disrupt the grid
 - North American Electric Reliability Corporation issued a warning that grid is not adequately protected from cyber attack

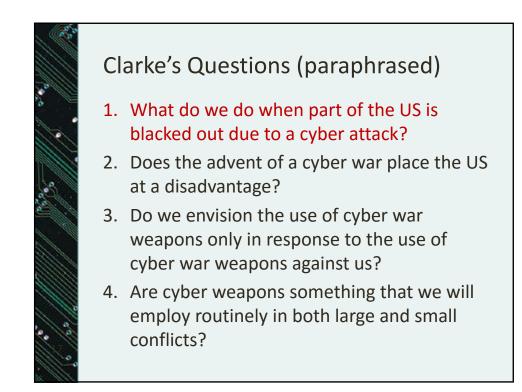
 2007 physical attack on Syria by Israel reported to be coordinated with a cyber attack on Syrian air defenses

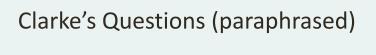
Corresponding page number:



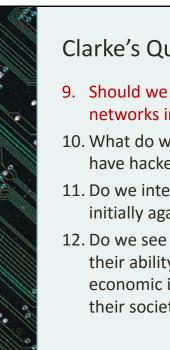


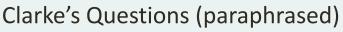




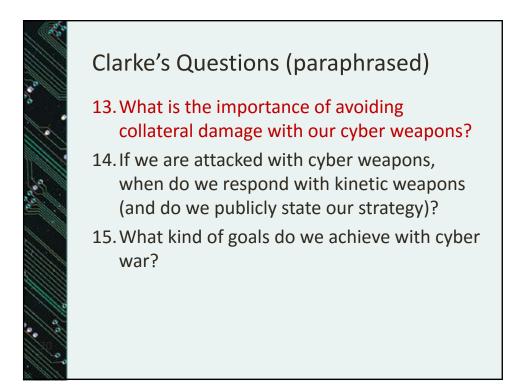


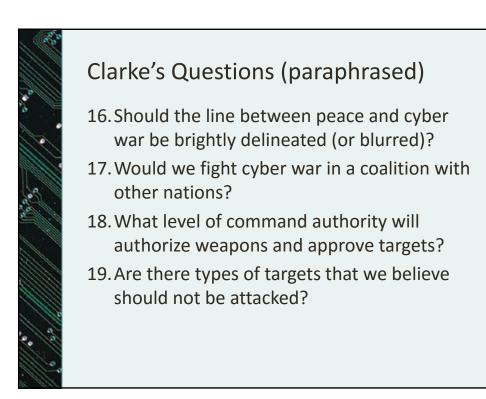
- 5. Will we plan to conduct a cyber war even when there is not a physical engagement?
- 6. Do we see cyberspace as another domain in which we must be militarily dominant?
- 7. How certain must we be to identify who attacked us before we respond?
- 8. Will we ever hide the facts when we attack with cyber weapons?

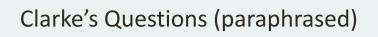




- 9. Should we be hacking into other nations' networks in peacetime?
- 10. What do we do if we find that other nations have hacked into our networks in peacetime?
- 11. Do we intend to use cyber weapons primarily or initially against military targets only?
- 12. Do we see the utility of cyber weapons being their ability to inflict destruction on the economic infrastructure of an enemy or on their society at large?

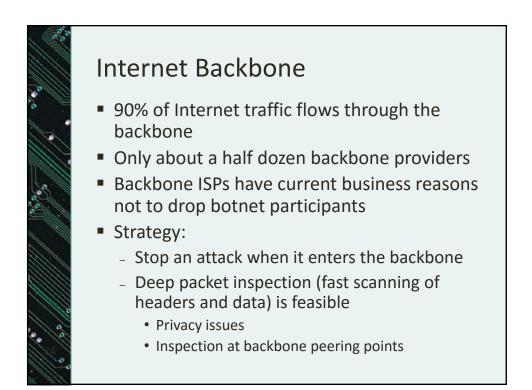






- 20. How do we signal our intentions in peacetime and in crisis? Can we use our cyber weapons as a deterrent?
- 21. If an enemy is successful in an attack, how does that affect our other military and political strategies?

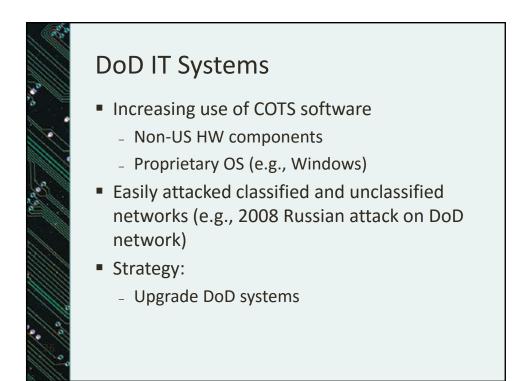


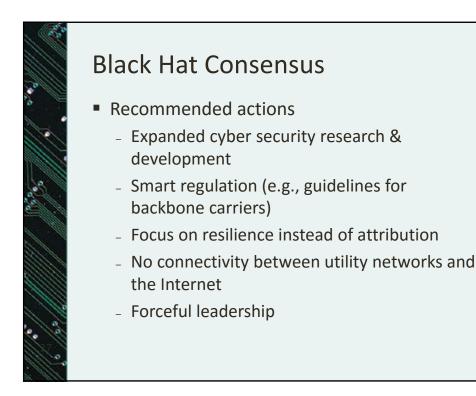


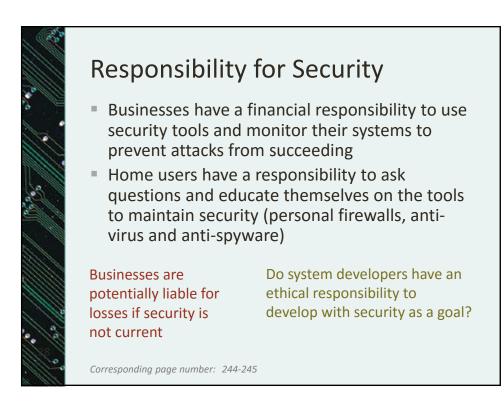


US Power Grid

- Department of Homeland Security announced that a US power station was crippled for weeks by cyber attacks
- Most of the US power grid is Internet connected (and increasing with development of Smart Grid)
- Audits show grid is easily attacked (some commands to components are not encrypted)
- Strategy:
 - Deep packet inspection on control grid interconnect
 - Encryption and authentication of control commands









The Law

Catching and Punishing Hackers

- 1984 Congress passed the Computer Fraud and Abuse Act (CFAA)
 - Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet
 - Under CFAA, it is illegal to access a computer without authorization
 - The USA PATRIOT Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems

Corresponding page number: 245

