

Technology in the Next War

New kinds of technology assisted hostile events

- Insurgencies
 - Iraq (cell phones trigger IADs)
- Terrorist attacks
 - 9/11/2001 (multiple, coordinated events, overwhelm responders)
 - Mumbai November 2008 (use of cell phones, GPS, google maps, to coordinate attacks)
- Cyber attacks
 - As the infrastructure of nation states becomes increasingly dependent on computer networks
 - Russia attacks the breakaway republic of Georgia
- Theft of Nuclear materials

Mumbai terrorists

- Used GPS to navigate to their attack points
- Used voice over internet and satellite phones for Command and Control
- Used Google Earth to familiarize themselves with the targets and the best approaches to them.
- VoIP is increasingly popular with criminals and terrorists – hard to tap and track.
 - Controllers in Pakistan, service providers in New Jersey and Austria.

Russia and Georgia

- “The Russians conducted a cyber-attack that was well coordinated with what Russian troops were doing on the ground.” (AvWeek, May 18, 2009)



Objectives of a cyber attack device

- Capture expert knowledge but keep humans in the loop.
- Quantify results so that the operator can put a number against choices.
- Enhance execution by creating a tool for the non-expert that puts material together and keeps track of it.
- Create great visuals so missions can be executed more intuitively.

Rochlin says,

- “Clearly when the human in the loop is not fully part of it, what is more desperately wanted is some reflective and digestive time.” (1997:167)

The next targets?

- Communications networks
- Data bases
- Supervisory control and data acquisition (SCADA) networks
 - These control things like nuclear power plants, power grids, waterworks, chemical plants, pipelines...

Tooth and Tail?

- Inexpensive high/low tech tooth
- Short inexpensive tail
- Willingness to sacrifice combatants