Marty Lyons
marty@cs.washington.edu
CSE P590 TU
White paper topic proposal
11 November 2005

Proposal:

Traditional systems of national protection include national legal policies, international law, federal charters and principles of government organization, and policing and military defenses. Many of these systems rely on behavior and action of an individual or group in a manner which can be handled through standard protective mechanisms, such as powers of arrest and trial.

As the non-traditional threats of terrorism and non-state actors emerge, a new type of combatant challenges our traditional methods of maintaining a free and civil society. This amorphous group benefits from acting outside the standard rules of international charters and bodies (such as the United Nations).

Nation-states have for their own national protection and competitive advantage maintained national intelligence agencies. Typically well funded and with expertise in diverse fields, the organizations can act as both an agent of international influence as well as "defense without weapons".

Both of these groups share one common characteristic in the desire to work in near or absolute secrecy. The benefit of taking the long-term view and investment in technology, training, and personnel to achieve desired goals separates these organizations from the more strategic political realm and the more tactical state or military one.

Some groups are now cross-pollinating, and we consider nation-states such as North Korea or Iran representing both a recognized political entity, as well as potentially acting in furtherance of more non-traditional goals. Additionally, specialists "for hire" from failing states such as the former Soviet Union are working in conjunction with both groups, often in areas of high impact such as weapons research and production.

The widespread availability of international telecommunications and computing acts as an economic leveler in that even an under-funded adversary can use these instruments as the basis of an offensive strategy. In many instances, the value and gain from the non-physical attack may be greater than that carried out using more traditional means, with the possibility of discovery, prevention, or prosecution marginalized.

I propose to review the impact that a well-funded state actor (such as an intelligence agency) or an independent group (such as a rogue or terrorist) could have on a national level by using digital technologies. In particular, could an attack impact the national readiness of defense systems, intelligence and police agencies, and government? What type of defenses and policies are required to prevent or limit such an attack, and at what cost and complexity? Are there methods that could place the general public at great risk, using digital techniques as the "weapons" of delivery?

Team:

As approved by Prof. Lazowska on 2 November 2005, I'll be doing this project on my own, and therefore the work is not being divided amongst a group.