Homeland Security / Cyber Security
Autumn 2005

Course Project ("White Paper") Assignment, and Topic Suggestions

Version 5: November 2

White Paper (~55%): Teams of 3-5 students will provide a comprehensive report describing a particular threat, assessing possible losses in the event of an attack, assessing current vulnerabilities, presenting possible responses, and evaluating the cost-effectiveness of each. The report should be **a well-written, thoughtful, coherent analysis, 20-30 pages in length**. (Stop writing when you have nothing left to say on your topic! The goal is to produce something interesting, not to fill pages!)

Due date: The White Paper will be due **by class (6:30 p.m.) on Wednesday December 7**.

Team formation and structure, and topic selection: If you like, you may use your "Red Team Project" grouping. Or you may form a new team – perhaps utilizing the Wiki to coalesce around a topic. Each team should include at least one "policy" student. Although each team can structure itself as it desires, our recommendation is that each team divide the topic into sub-topics ("chapters" of the report) with each team member (or a small group of team members) acting as the "lead author" for that portion. (However, all team members should review and suggest changes for the entire report – the overall report must be "smooth and integrated" – not a "staple job" on 3-5 independent sections.) Please send the TA (Jeff Bigham) a list of team members, a one-page description of your topic, and a one-page description of how you intend to divide the work, by **5 p.m. on Friday November 11**. **Do not wait until the last minute** – we are happy to help engineer teams, but **we want to have the process completed by Friday November 11**. Once teams are formed and topics selected, a specific instructor will be designated as the "mentor" for each team.

Exceptions: The team structure described above is intended as the norm. If you have a special situation, contact one of the instructors.

Possible topics: Don't feel limited by these! If you have an idea, run with it! Interact with us over the next week as you refine your topic ideas.

Nuclear Weapons: What does the history of state programs teach us about the problem? Current Non-proliferation status. Nuclear forensics (traceback). Cargo screening. References: Glasstone, *Effects of Nuclear Weapons.*

Chemical Weapons: History. Technology. Barriers to entry. Options. Cost-Benefit. References: Croddy, *Chemical and Biological Warfare.*

Biological Weapons: History. Traditional Technology. Genetic Engineering. Barriers to entry. Defense Options. Cost-Benefit. References: Alibek, *Biohazard*; Guillemin, *Biological Weapons.*

Radiological Weapons: History. Practicality. Defense Options. Cost-Benefit. [The references here are thin. Steve Maurer could probably get people started but this is a real research project.]

Privacy and Data: How Is It Done? Is Total Information Awareness Possible? What would the costs and benefits be for a typical citizen? References: Whitaker, *The End of Privacy*, Monomonier, *Spying With Maps.*

Encryption Policy: Echelon. How Good Is Al Qaeda's computer security? Could new commercial products make Al Qaeda's job easier – do export controls make sense? References: Keefe, *Chatter; 9-11 Commission Report; NRC CSTB Cyber Security report.*

Open Source and Cybersecurity: Does open source software have inherent security advantages/disadvantages? What is the evidence? Note: this is not a religious topic, it is a technical one!

Interrogation & Torture: International Law. Domestic Law. US Army & CIA Policy and Practices. Israeli Policy. What Qualifies as Torture? Is Torture Reliable? What is the ethical case for and against different interrogation methods? References: Dershowitz, *Why Terrorism Works*, Solzhenitsyn, *Gulag Archipelago*, Mackey, *Interrogator's War.*

State-Sponsored Hacking: Press coverage of rumored China, N. Korea and US programs. What are the bottlenecks for today's hackers? Can a large, well-funded team overcome these constraints? What damage could they plausibly cause?

Cyberterrorism: What are threats of cyberterrorism? Compare these threats with more traditional CBNR threats. How is cyberterrorism different? How real is cyberterrorism? Will Al Qaeda launch a cyberattack?

Cybersecurity and National Infrastructure: Trace the historical dependency of national critical infrastructure on cyber infrastructure. To what extent does that expose critical infrastructure to terrorism attack via cyberattacks? Perhaps choose a specific infrastructure, such as the electrical power grid, as your focus of study.

Cybersecurity and Law: What is the history of prosecution of cybersecurity attacks? How does current and proposed law relate to current and future attacks? What is the current state of the art in forensics, evidence, and attestation? What gaps remain between law and policy, and ability to prosecute? How will evolution in law change kinds, extent, and frequency of cyber attacks? What categories of activity should be illegal? How should existing law be changed? What is the state of the art in Cyberforensics? What are the issues and challenges with attacks across political borders (state, national, international)?

Cyber Criminal Activity: Trace history of cyber criminal activity, evolution from intrusion to botnets as platforms for global criminal activity. Profile the evolution of attackers, targets, defenders, vulnerabilities, threats, and goals of attacks. Where are the trends pointing?

Liability: What are the liability issues surrounding vulnerabilities in software and hardware? What are the implications of regulation and shifts in liability? Who should be regulated (who is the lowest cost provider?) Compare/contrast with other technology industries where liability has had more impact (e.g., medicine, communication).

Education, Exploits, Cyberculture: Should universities teach people to hack? Should university researchers try to break commercial encryption? Should they publish if they succeed? Are exploits a nuisance or a useful corrective? Can we imagine a better system than exploits? Are existing norms and sanctions suitably adaptive? Should community members report colleagues who break the rules? When we teach people how to exploit software vulnerabilities (as we did in this course), we are effectively training people to exploit; when we announce vulnerabilities as warnings (both before and after patches have been created), we are effectively creating targets of those systems that have not installed patches; when we post exploit software, we are effectively providing the mechanism for a broader group of people to launch cyber attacks. At the same time, the historical track record of most vendors is that they do not take vulnerabilities seriously until exploits are demonstrated; additionally, "security through obscurity" has a long history of not working. Perhaps compare/contrast with policy and implications of training, education, development of traditional CBNR technology (e.g., CBNR labs and weapon stockpiles) – technology mainly based on scarce expensive assets.

Offense vs. Defense: While this class has primarily focused on cyber security from a defensive standpoint, the line between defense and offense is frequently blurred. Several security vendors have championed "strike back" capabilities, and organized overloading of sites advertised via spam are commonplace. In yet another example, some experts have proposed (and even created) "white worms" that exploit extant security holes to gain access to vulnerable machines and either fix them or alert their users about the threat. At the same time, unclear legal footing has often stymied law enforcement attempts to respond effectively to massive host compromises (e.g., million-node botnets). Consider the potential technical and legal issues around "offensive" cyber-defense on the Internet. It what situations might it be possible, in which might it be legal, and are there interesting intersections or "grey areas" that may be emerging?