Assessing Five Cyber Incidents: Legal and Operational Perspectives on Response Options
Session Goals

• Assess if incident qualifies as an attack or the use of force against the United States.
• Identify military, intelligence, or diplomatic options for response.
• Decide what evidence is required to justify a military or covert response, including the application of force.
• Apply Laws of Armed Conflict: limits on collateral damage, proportionality, distinction.
Google

• Gmail searched for political information. Google proprietary technology exfiltrated.

• At least 30 other high tech companies are also hacked.

• Google had recently clashed with the Chinese government over censorship.

• Attacks were traced to computers at two campuses in China; consistent with China’s use of proxies.

• China did not respond to a US demarche
SIPRNET

• Unknown foreign opponent successfully placed malware on SIPRNET (CENTCOM). Malware could have disrupted data but was not triggered.
• Entry point is thumb drives given to Service members in Iraq.
• US was unable to remove the malware for several days.
• DOD says that the attack was perpetrated by a foreign intelligence service.
• Some blame Russia; Russia denies all.
**Stuxnet**

- Stuxnet caused physical damage that wiped out 20 percent of Iran’s nuclear centrifuges.
- The sophistication of the malware and its delivery suggests it was produced and deployed by a nation-state.
- Stuxnet was found on networks around the world (including the US) but only affected Iran.
- Stuxnet-like tools could be used against any critical infrastructure anywhere.
Electrical Grid Reconnaissance

• Military competitors probe the US electrical grid to map vulnerabilities for future use.
• There is no damage or exfiltration of data in these probes.
• Similar to satellite reconnaissance for targeting, but unlike satellites, involves virtual intrusions into US territory.
• Unclear if “leave-behinds” (“beacons,” “logic bombs”) are involved.
Defense Technology

• Hackers use phishing techniques in attempt to obtain data that would compromise authentication technology used by DOD and major defense contractors.
• The authentication data acquired is then used in an attempt to penetrate defense contractor networks to exfiltrate data on advanced weaponry.
• Based on forensic evidence, the companies suspect proxies acting on behalf of a foreign intelligence service in Asia
Reiteration of Session Goals

• Does the incident qualify as an attack or the use of force against the United States?
• What are the military, intelligence or diplomatic options for response?
• What evidence is required to justify a military or covert response, including the application of force?
• How do the Laws of Armed Conflict apply (limits on collateral damage, proportionality, distinction)?