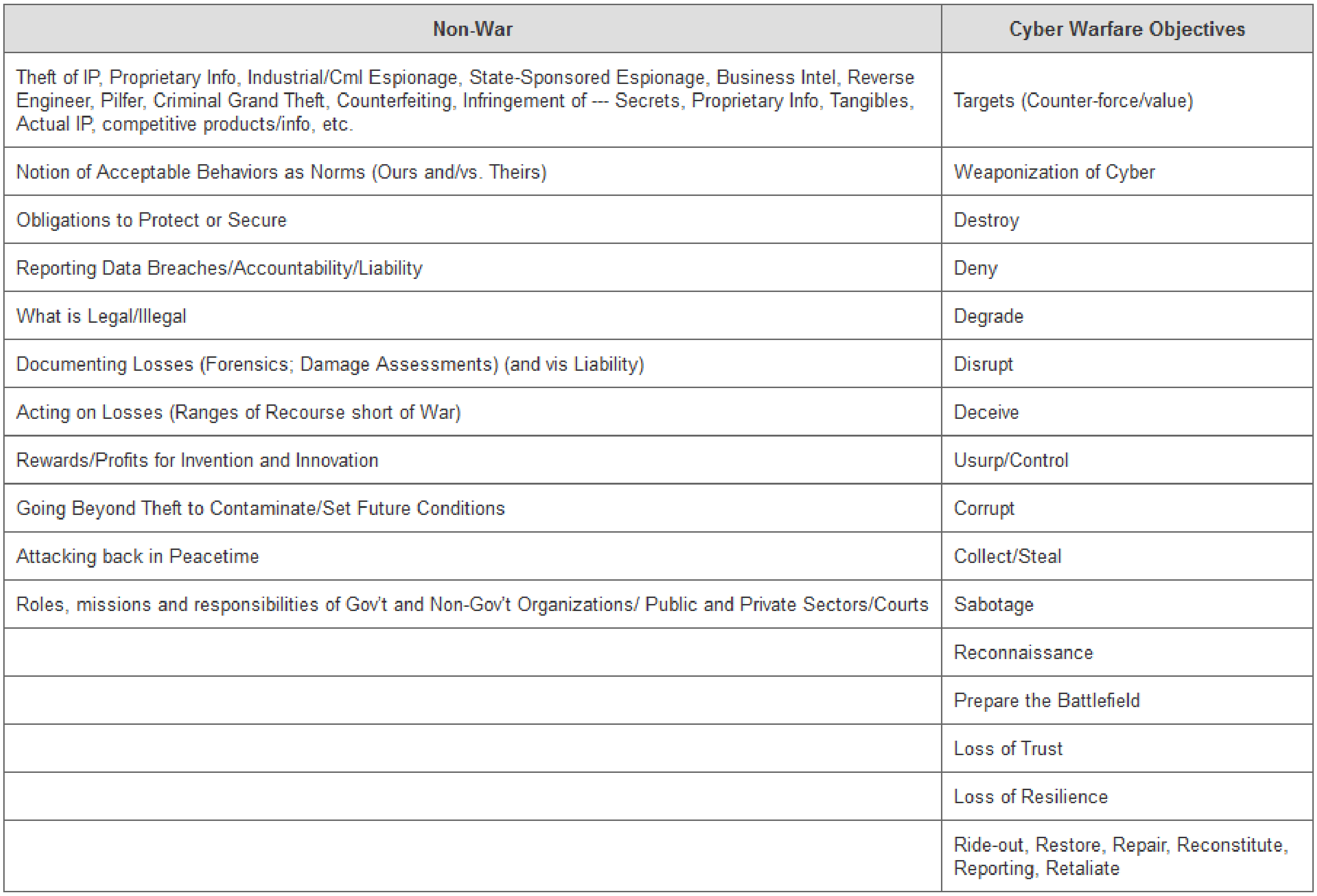
Session 4: Political, Military and Industrial Espionage (Thursday, 2:45 – 4:15 PM)
Roundtable: Catherine Lotrionte (co-moderator), William (Bill) Studeman (co-moderator), Nigel Inkster, Sean Kanuck

Stimulating Words and Phrases:



Non-War	Cyber Warfare Objectives
Theft of IP, Proprietary Info, Industrial/Cml Espionage, State-Sponsored Espionage, Business Intel, Reverse Engineer, Pilfer, Criminal Grand Theft, Counterfeiting, Infringement of --- Secrets, Proprietary Info, Tangibles, Actual IP, competitive products/info, etc.	Targets (Counter-force/value)
Notion of Acceptable Behaviors as Norms (Ours and/vs. Theirs)	Weaponization of Cyber
Obligations to Protect or Secure	Destroy
Reporting Data Breaches/Accountability/Liability	Deny
What is Legal/Illegal	Degrade
Documenting Losses (Forensics; Damage Assessments) (and vis Liability)	Disrupt
Acting on Losses (Ranges of Recourse short of War)	Deceive
Rewards/Profits for Invention and Innovation	Usurp/Control
Going Beyond Theft to Contaminate/Set Future Conditions	Corrupt
Attacking back in Peacetime	Collect/Steal
Roles, missions and responsibilities of Gov't and Non-Gov't Organizations/ Public and Private Sectors/Courts	Sabotage
	Reconnaissance
	Prepare the Battlefield
	Loss of Trust
	Loss of Resilience
	Ride-out, Restore, Repair, Reconstitute, Reporting, Retaliate

Some notional round table questions:

1. Does (Big) Cyber Conflict generally conform and map into the current normative wartime Laws of Armed Conflict (LOAC) and peacetime domestic and international law as currently written?
2. How is Peacetime Theft of IP done by a State/State Sponsored Patriot from a norms point of view legally different then State sponsored Espionage?
3. Discuss possible ranges of normative types of recourse and responses against countries who pervasively engage in theft of IP?
4. Since Cyber is a new and evolving field, what is the status of aligning EU and U.S. data breach reporting approaches, and how could these relate to corporate liability and marketplace concerns?
5. Since cyber conflict in peace and war is a new and poorly understood threat spectrum, discuss whether we can expect any new/different other future norms for cyber? Could

there ultimately be arms control-like engagements and negotiations re use of cyber that have norms implications?

6. Why isn’t it a norm to aggressively pursue low to mid-end criminals, hackers, DDOS, owners and renters of BOTNets, criminals/privateers, and to cooperate on solutions which better help with attribution and prosecution of such criminals?
7. Could forms of active defense and attack-back become an accepted norm area, and under what conditions?
8. Could it be an acceptable norm that one country can justify cyber attacks in peacetime against other countries because their State does not like the policies and behavior of the target State?