Panel 4: Law of Armed Conflict (LOAC) and Rules of Engagement (RoE) in Cyberspace
(Thursday, 15:00-16:45)

Chair: Duncan Hollis.
Panel members: Amy Gordon, Eric Jensen, Neil Rowe, Hardin Tibbs, and Jody Westby.

As militaries increase their presence in cyberspace, significant questions have emerged over (a) how the existing Law of Armed Conflict (LOAC) applies to military cyber activities, (b) what rules of engagement (RoE) militaries will adopt for those activities, and (c) whether new LOAC rules are necessary to deal with critical infrastructure's reliance on cyber-based systems. The panel will explore whether and how the LOAC applies even where it contains no cyber-specific rules. It will also examine the relative gaps and challenges that exist in translating into the cyber context the LOAC's three main principles – *necessity* (allowing only acts necessary to accomplish legitimate military objectives); *distinction* (requiring militaries to distinguish between civilian and military objects and to only direct operations against military objectives); and *proportionality* (prohibiting force in excess of what's necessary to accomplish military objectives

Questions guiding panel prepared remarks:

I. Applying the Law of Armed Conflict (LOAC) to Cyberspace

1. Can the LOAC apply? As a general matter, how strong is the consensus that the LOAC applies to incidents and operations that militaries undertake in cyberspace?
   a. What are the implications of China's apparent resistance to applying the LOAC to cyberspace? Do they have any credible legal arguments that exempt them even though the LOAC is presumed to apply to all new methods and means of using force?

   b. Can we apply the LOAC with any degree of certainty to military operations in cyberspace where there is so much uncertainty on questions of legal thresholds (which is the focus of Panel 3)?

   c. How does the technical attribution problem impact the LOAC's application? Presumably, the LOAC will both constrain and facilitate how militaries behave in cyberspace. But, without technical attribution, can victims ever invoke the LOAC where the exact perpetrator may remain anonymous, and where it's difficult to know if the attacker is a State, an entity under a State's "effective control", a non-State actor, or one or more individuals?
2. How does the LOAC Apply? Assuming the factual and legal thresholds for applying the existing LOAC rules are surpassed, how should States and their militaries translate the existing LOAC into cyberspace?

   a. What is the Tallinn manual and how does it seek to answer this question? What is the best case for the manual's impact on the development of cyber-specific LOAC norms? Is it a Lieber Code for cyber? Conversely, what is the worst case scenario for its impact?

Could it lead to conflicting assumptions about the relevant permissibility of certain cyber operations or generate unintended escalation of conflicts?

b. Should the Tallinn manual be the exclusive vehicle for translating the existing LOAC to cyberspace? Should other vehicles be considered alongside this effort such as legal negotiations or allowing state practice to set the standards for behavior?

c. What are the most pressing "open questions" about the existing LOAC's application to cyberspace? Of the three main principles for how military operations must be conducted – distinction, necessity and proportionality – which one needs the most attention and why? Are there other LOAC rules that deserve similar (or greater) priority – such as those on combatants, neutrality, or blockades?

d. Who will hold non-state actors accountable for LOAC breaches and how will they do so?

e. Can we actually identify how the LOAC applies in practice -- for example, assuming the LOAC applied to Stuxnet (admittedly, a debatable proposition) is there any degree of certainty as to its consistency with those rules?

II. Developing Rules of Engagement (RoE):

1. Can States develop effective RoEs in the cyber environment where the technological capacity and application may not be known and, even if known, is subject to near constant evolution?
2. Should cyber-RoEs be developed in the usual classified fora? What is gained by keeping such RoE's classified? What costs or risks are associated with keeping them secret?

III. Proscribing Attacks on Cyber-Based Critical Infrastructure and the Potential for Other New Rules

1. Is a proscription of cyber attacks on critical infrastructure covered by the existing LOAC? If not, should the LOAC be elaborated to include such a proscription? Which critical infrastructure, if any, warrants protection and in what order of priority (electrical grids, telecommunications networks, banking and financial systems, oil and natural gas delivery systems, etc.)?

2. How would a proscription of attacks on cyber-based critical infrastructure be implemented, assuming anonymous actors might still desire to pursue such attacks? Is legal deterrence possible in the absence of catching those who violate the proscription?
3. Is there a need to revise current legal standards to ensure they do not limit State action in responding (whether unilaterally or collectively) to some such cyber catastrophe. Are there lessons from other domains (such as the debate over the Global Initiative against nuclear terrorism) that might inform this inquiry?