Panel 4: Law of Armed Conflict (LOAC) and Rules of Engagement (RoE) in Cyberspace

Law has long proscribed (and permitted) various means and methods of warfare. The modern Law of Armed Conflict (LOAC) emerged from U.S. President Abraham Lincoln's 1863 *General Orders No. 100, Instructions for the Government of the Armies of the United States in the Field.* Those rules – originally drafted outside the U.S. Government by Columbia Professor Francis Leiber – regulated how the Union army would engage its Confederate adversary. They did so on a non-reciprocal basis, providing minimum standards of behavior independent of Confederate military actions, an approach the LOAC still employs. Today, that LOAC rests on three fundamental principles:

- ***Necessity*** (allowing militaries to engage in only those 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 military uses of force in excess of those necessary to accomplish military objectives).

The LOAC extends these principles to *all* means and methods of attack, allowing the law to adapt when new technologies emerge such as air power or nuclear weapons.

With an increasing military presence in cyberspace, significant questions have emerged on *whether* and *how* the LOAC applies to State-sponsored cyber operations. The panel addressed these questions while also asking *if* the LOAC needs *new* cyber-specific norms.[1]

I. Can the LOAC Apply to Cyberspace?

There was unanimity on the question of whether, as a general matter, the LOAC applies to incidents and operations that militaries undertake in cyberspace. The resistance of one State – China – to this position was noted, prompting a discussion of its rationale for doing so. One view ascribed Chinese resistance to the fact that so much of what is happening in cyberspace lies below the level at which the LOAC applies. Others, however, characterized China's position as a categorical objection to linking the LOAC to all cyber incidents and operations. From an international law perspective that categorical position is difficult to sustain given the LOAC rule requiring its application to every new situation or technology employed by military actors. As the so-called "Martens Clause" emphasizes, the absence of a cyber-specific provision on the use of information technology in an armed conflict does not mean that such technology is automatically permitted; any use of information technology for military operations requires the same levels of planning and analysis applicable in more conventional contexts.

A similar consensus emerged on the importance of legal thresholds for applying the LOAC. Any LOAC discussion is unlikely to have much practical relevance without a clear understanding on *when* its rules apply (similar clarity is needed for the thresholds at which point a cyber operation constitutes a use of force). Workshop participants acknowledged that the LOAC may be triggered when cyber operations are used in concert with conventional armed attacks, but it could also apply where a cyber operation in isolation constitutes an "armed

[1] Although the Panel title references "Rules of Engagement (RoE)", the discussion never reached that given the robust LOAC discussion among the panelists and other participants.

attack." There is a real risk, however, that militaries and other actors will adopt different assumptions as to which cyber operations constitute armed attacks and which do not. Thus, a victim might view the LOAC to clearly apply to the same cyber operation that its perpetrator assumed was permissible espionage or merely subject to domestic criminal law(s).

Given the importance of thresholds, there was support for further work on the LOAC's operation along two dimensions. **First**, several participants advocated a project that would **generate a typology of cyber technologies and operations** to inform further analysis of the LOAC's application. **Second**, a call was made to **have specialized cadres of lawyers – those with expertise in both cyber and the LOAC –** work out in more detail how to interpret and apply the LOAC in cyberspace.

II. How does the LOAC Apply?

This second project has already begun. In August 2012, a group of legal experts, acting in their personal capacities (albeit with support from NATO's Cooperative Cyber Defence Centre of Excellence) generated the **Tallinn Manual**; a set of rules for the use of force and the LOAC in cyberspace. The Manual took three years to develop with the express mission of identifying what the existing LOAC cyberspace rules *are*, not merely what the rules *should be*. It is hoped that the Tallinn Manual may clarify how the LOAC works in cyberspace by addressing at least five critical topics:

(i) What constitutes direct participation in hostilities, thereby delineating what civilians can (and cannot do) with respect to military cyber operations;
(ii) What types of cyber events can constitute "attacks" including those impacting computer functionality;
(iii) How the principle of neutrality applies to cyber operations;
(iv) Whether and how those deserving special protections under the LOAC (e.g., the Red Cross) must identify themselves in cyberspace; and
(v) How to treat non-State actor cyber operations and incidents.

It was recognized that **the Tallinn manual is meant to start the discussion of the LOAC's application, not to end it**. Others will need to enter the conversation and further cooperation is essential. Various vehicles for such cooperation were considered. Several participants emphasized **the importance of considering informal methods** alongside the more formal UN or treaty-making processes that have dominated the discussion to date. Useful precedents include the Global Initiative for Countering Nuclear Terrorism or the Proliferation Security Initiative. Others emphasized the need to **move the discussion beyond a purely LOAC framework** to ensure consideration of the impact of military cyber operations on civilian populations even if they clearly do not qualify as attacks in the LOAC sense. A call was also made to ensure that **ethical considerations** are part of the analysis alongside the legal ones under discussion.   Finally, the **reality of power** was acknowledged and the likelihood that Great Powers are going to be unwilling to agree to be constrained by anything they do not want to be constrained by.

Workshop participants also recognized that the architecture of existing technology has a significant impact on how the LOAC applies to cyber operations. Most notably, **the problem of attribution** continues to complicate the application of existing LOAC rules, most of which depend on being able to identify the attacker. Where the attacker's identity is unclear, it becomes difficult to know if the LOAC or some other legal regime (e.g., domestic criminal law) applies. It was noted that new forensic tools are increasing the chances of technical attribution. But, even if one identifies the computer system or network from which an attack originates, difficulties remain in identifying who actually entered the keystrokes. Workshop participants emphasized the **strategic implications** of this anonymity as there are trade-offs in terms of strategic signaling if actors choose to remain anonymous. It was suggested that at least one European State is preparing to publicly acknowledge future cyber operations by its military, although it would not do so for those of its secret service.

Similar concerns were raised about **the demonstrated unpredictability of cyber operations**; even the most carefully planned operation (e.g., Stuxnet) may have significant cascading effects. Given this reality, more work is needed to translate the LOAC's existing prohibition on State use of **indiscriminate weapons** to cyber incidents and operations.

In terms actually applying the LOAC to specific issues, workshop participants had a wide-ranging and robust discussion. Four issues were particularly prominent:

- **First**, **workshop participants were sharply divided on how the LOAC (and the *jus ad bellum)* apply to the *Stuxnet* virus**. Some participants believed it was neither a use of force nor an "armed attack" as that term is used in the LOAC. Others were just as insistent that Stuxnet crossed both thresholds, with further differences of opinion on its legality under either regime. Furthermore, it was noted that the Stuxnet incident itself may set a precedent since Iran's reaction may limit the ability of future victims to invoke the UN and LOAC frameworks, limiting their avenues for relief to domestic criminal law and export control regimes.

- **Second**, participants examined **whether the distinction between counterforce (force-on-force) and countervalue (society-on-society) targeting decisions extends to cyberspace**. At present, individuals, corporations, and other non-governmental groups are frequently victims of cyber operations, but the effects almost always fall short of those to which the counterforce/countervalue distinction applied historically. The LOAC itself, moreover, does not make that distinction, adopting the principle of proportionality instead, where civilian collateral damage is adjudicated in terms of the military objective achieved (and perhaps based on who wins the conflict). Workshop participants did, however, express support for using an "**effects test**" to assess individual cyber operations and their legality. At the same time, questions were raised about whether there might be **a gap in the LOAC** if it permits militaries to pursue counter-value operations against civilian populations in precise, but bloodless ways. It was noted that, even if military cyber operations target civilian populations in ways that do not rise to the level of an attack (which would be prohibited by the principle of distinction), a separate LOAC provision prohibiting the terrorization of the population does restrict what militaries can do vis-à-vis civilian targets.

- **Third**, **participants discussed the liability and neutral status of a State that owns or funds networks (e.g., onion routing) used by a second State for military purposes (e.g., targeting insurgent forces or populations).** Participants noted that if the second State's activity was simply intelligence gathering, it would not trigger the LOAC in contrast to a scenario where the technology was a component part of an attack itself. Similarly, the level of the first State's involvement matters; international law does not make States responsible for simply funding activities nor can a State's corporations pull it out of neutrality. But, a State is responsible for its own actions as well as those of proxies under its overall or effective control. Furthermore, States remain free to apply their domestic criminal laws to proxies where they have jurisdiction to do so, as well as to "patriotic" hackers who are not controlled by the State itself.

- **Fourth**, in a variation on the State responsibility discussion, **workshop participants discussed increasing activity by private actors whose technology implicates LOAC questions**, namely corporations who develop (and sell) technology that foreign militaries may use. Participants discussed State export control laws and the issue of what technology should be openly available in commercial contexts. In addition, participants discussed the possibility that corporations themselves may play a role in responding directly to cyber-attacks with counter-attacks of their own.

III. Potential New Norms for the LOAC in Cyberspace

The majority of the panel's time focused on the existing LOAC. Nonetheless, in the course of discussing whether and how the LOAC applies to cyber operations, **various proposals for new LOAC cyber norms were made**. Five are worth noting here:

- A requirement that States **protect (and not attack) information technology infrastructure** itself (with some discussing expanding this prohibition to other critical infrastructure).

- A proposal to **develop a concept of "cyberpeace"** (in the sense of geo-strategic stability where actors refrain from disruptive activities) that could be a part of future discourse alongside the existing rubrics of cyberwar and cybercrime.

- A requirement that military cyber operations adopt specific functional requirements; for example, **requiring any attack to be reversible where the technology exists to allow reversibility**.

- The development of an **agreed means to electronically mark computer systems and networks deserving special protections**, such as hospitals or the International Committee for the Red Cross.

- The **development of rules of engagement where cyberattacks must be attributable in some way**; that is some equivalent of uniforms in cyberspace.

In sum, the LOAC panel and the other participants recognized the importance of the LOAC discussion as a key component of the larger dialogue on governance and norms in cyberspace.