Duncan B. Hollis
Member of the Inter- American Juridical Commitee
Presentation at the Extraordinary Session on International Humanitarian Law

Begin with **Thanks to Dept. of International Law** for inviting me and hosting such an important conversation.

As a professor, my students are always asking me for tips or tricks to help them remember what I'm teaching. I often try to give them a mind map by offering a seemingly random combination of things and then explaining how they relate to the topic at hand. And if they just remember each thing, they'll usually remember what it's about.

So, for my talk today, I've got 4 things I want you to remember:

- **John Paul Sartre, a Baby Carriage, Horses, and Simon & Garfunkel**

A strange answer I know. But it usually **gets everyone's attention** since most people want to see how on earth I connect Jean Paul Sartre, a baby carriage, horses and Simon & Garfunkel to International Humanitarian Law and new technologies.

But, I assure you, I'm up to the task. Each of these 4 things **says something quite fundamental** about the state of International Humanitarian Law as it relates to information & communication technologies or the broader concept of cyberspace.

I. **Existential Arguments**:

For starters, there is Jean Paul Sartre – the father of existentialism. I choose him to symbolize what I'd call the **existential challenge** to International Humanitarian Law in cyberspace. This is the question whether specific international legal regimes even exist or apply at all in cyber space?

- For a time, some States had an **existential argument about international law in its entirety** in cyberspace; they were reluctant to concede it applied to cyberspace at all; claiming that its novelty kept it freed from existing rules.

Fortunately, one of the positive outcomes of the **UN GGE process -** United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - was the 2013 consensus **report** indicating that

> "*international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment*."

The **2015 Report** built on that consensus and the United Nations General Assembly endorsed it in Resolution 266 on earlier this month.

But the question of whether International Humanitarian Law applies to cyberspace is, unfortunately, still a live one.

The 2017 GGE failed, reportedly, because several nation States refused to concede that International Humanitarian Law existed or otherwise applied to cyber activities.

Other States just as vehemently insist that, of course, International Humanitarian Law can apply to a cyber operation.

- Several international organizations, including the European Union and North Atlantic Treaty Organization have said that it does,

- Thus, one question for the OAS **is whether at a political level it would be useful for it to inquire if Member States share this view and to publicize it?**

Because only if International Humanitarian Law exists and is applicable can it operate to regulate its subjects, in this case States.

II. Interpretative Challenges:

Which brings me to my **Baby Carriage.** I mention the baby carriage because it is symbolic of a different challenge we face in applying International Humanitarian Law to cyber operations – an interpretative one, drawing on the famous debate between the **legal philosophers HLA Hart and Lon Fuller**.

- Hart had posited a legal rule "***No vehicles are allowed in the public park.***" Hart assumed such a rule was drafted to keep out things with wheels like cars. But, Hart asked what about bicycles? roller skates? What about toy automobiles. Are they vehicles for purposes of the rule?

- Fuller, in reply, went further, and asked if the rule prohibited vehicles, what did that mean for an **ambulance**, or even a stroller, **a baby carriage**?

Thus, the baby carriage symbolizes how, even when we agree a legal regime exists – no vehicles in public parks, or a cyber operation can constitute an attack—we **still may can have lots of problems figuring out what that rule means** as it is tested in different ways.

- For example, among those accepting IHL's application to cyberspace, there is a long-standing interpretative inquiry into when a cyber operation would qualify as an "attack" subjecting the operation to various International Humanitarian Law rules like distinction, proportionality and precautions.

- Does a cyber operation rise to the level of an "attack" **only when it produces the sorts of violent consequences** generated by kinetic or biological weapons – i.e., death, destruction or property damage.

- Or could a cyber operation **that disrupts the integrity of the target –** say scrambling the decimal places in a stock exchange without killing anyone or damaging anything physically do so.

In many cases, these interpretative debates often end up being a debate over default rules – when we have novel behavior, not clearly prohibited nor clearly permitted by International Humanitarian Law, where do we put it -- implicitly prohibited or implicitly permitted?

III. Procedural Challenges:

Answering that question brings me to horses. The relevance of horses to cyberspace was established some 20 years ago in 1996. U.S. jurist Frank **Easterbrook** gave a famous speech **critiquing the need for a new law of cyberspace.**

- Easterbrook noted how law schools do not teach a class on "the Law of the Horse." He said, of course, laws exist regulating horses – **contracts** in which horses are bought and sold; **licensing schemes** for racing them, cases on **veterinarian** malpractice; the **torts** horses commit if they hurt people.

- But Easterbrook said we don't need to have a field of law for horses specifically because and I quote "*The best way to learn the law applicable to specialized endeavors is to study general rules.*"

- Easterbrook said the same was true for cyber – we should **focus more on figuring out how the general rules apply to cyber** and spend less time trying to build cyber-specific rules.

A couple of years later Harvard Law Professor **Larry Lessig rebutted Easterbrook by claiming that cyberspace IS unique such that it requires new, tailor-made rules.**

- Sure, he said, existing laws apply to cyber, there are social norms for programmers and companies; market forces work in cyber as well. But Lessig noted it **also has code** – the ICT architecture.

- Lessig famously coined the phrase, "**Code is Law**" to express the idea that code regulates cyber in the way the laws of physics regulate the natural world. Unlike physics, however, we can change the code and the question becomes when should governments require this and when should they leave well enough alone?

Thus, for me, the **horse stands in for the procedural challenges** facing international law going forward. Assuming a desire to resolve the existential and interpretative ambiguities I've identified, **there's a question of how to do so.**

    - Some are **against devising any law of the horse for cyberspace**. They do not think we need new international humanitarian law rules or laws, but believe we can understand how to regulate this space by **focusing more on how the existing, general prinicples of International Humanitarian Law apply.**

  - This is the **Tallinn Manual** approach – taking existing laws and trying to clarify or adjust only slightly what they mean for global cybersecurity.

  - **For states**, moreover, international law also authorizes them to **develop law by accretion** – customary international law is a law that derives from state practice.

    - Thus, there is some suggestion that if we **just let states continue to interact here** long enough especially **as attribution possibilities are on the rise,** States will work out the kinks in international humanitarian law as a matter of custom.

      - I note, for example, the ICRC has suggested that we'll have to await further state practice to decide whether and when cyber operations alone may rise to the level of an armed conflict triggering the application of international humanitarian law.

On the other side of the procedural divide lie those who want a **law of the horse,** who want there to be a specific set of international humanitarian law rules for cyberspace, tailored to the potential and perils of this space.

- We already have this with respect to cybercrime, in that rather than rely on existing criminal law, States went out and agreed on a new set of crimes under the **Budapest Convention** (of course, that treaty was specifically crafted not to cover State behavior).

- And we've got some **nascent efforts** pushing for new international legal rules and standards with things like the Paris Call.

There are, moreover, debates within these debates about whether a new tailor-made law requires a truly global effort of whether progress can be made bilaterally or regionally. Thus, we've seen in recent years efforts to **adopt tailor-made rules** for cyber security, whether

- **bilateral ones** like the Russia-China cybersecurity agreement,
- regional ones like the **African Union** Cybersecurity Convention,
- or **global calls** like Microsoft's proposal for a Digital Geneva Convention? (DISCLOSURE)

The question for International Humanitarian Law lawyers is ***whether or not the Tallinn Manuals have done the job or whether we need some affirmative process*** to tailor specific new international humanitarian law rules for cyber operations?

Which brings me to my finally one of the **greatest musical duos of all time – Simon and Garfunkel.** I mention them because of their most famous song – the **Sounds of Silence,** as silence constitutes a fourth and final challenge for International Humanitarian Law in cyberspace today.

The Tallinn Manuals are **undoubtedly important reference works** and **governments were consulted** in their drafting.

But recent research by Yuval **Shany**, the Chair of the UN Human Rights Committee and Dan **Efrony** formerly of the Israeli Defense Forces suggests that **States have left these Manuals "on the shelf"** in their actual practice.

Simply put, States have **<u>been largely silent about how they understand international law generally and international humanitarian law specifically applies to cyber operations.</u>**

There is scant evidence that States are invoking international law in response to specific cyber incidents and only a few States have offered public statements on the application of international law generally with relatively little details on what this means for international humanitarian law and questions like

- which cyber operations are triggering or occurring in armed conflicts?
- what's the definition of an attack?
- If a cyber operation only targets data, is that operation subject to the principle of distinction where States may only target military objects not civilian ones?

In some ways, the current sounds of silence are the most critical of the four challenges I've mentioned.

If we don't know how States understand the law, it undermines our understanding of **whether there's law here at all,** let alone what it says.

Given that in international humanitarian law we're talking about life & death behavior, moreover, are real risks two States may adopt divergent views on whether international humanitarian law applies or what it says that could inadvertently escalate a conflict (i.e., one State views another State's behavior as an attack that violates the requirements of distinction/proportionality while the other didn't think it was an attack subject to international humanitarian law at all).

In sum, as we look forward to the future of international humanitarian law in cyberspace, I hope you, like me, will now see **Jean Paul Sartre, a baby carriage, horses, and Simon & Garfunkel as challenges arrayed in front of you**.

- We see **challenges that are existential** – does international humanitarian law even exist for cyber-operations or not?

- **Challenges that are interpretative** – given an existing international humanitarian law rule such as distinction, what does it mean when it comes to cyber operations looking say to exfiltrate data?

- **Challenges that are procedural** – should we continue to focus on things like the Tallinn Manuals and custom to encapsulate the existing law of the horse or do we need to have a dialogue about drafting and agreeing to some new international humanitarian law rules?

- **And, finally, how do we get States to break the sound of silence** – how do we get greater clarity or transparency on what States understand international humanitarian law to be and mean in cyberspace?

On the part of the CJI – we've decided to focus on **the fourth challenge** – to try and break the silence a bit –.

We agreed at our last regular session to add a project to our agenda to **improve transparency with respect to international law and cyber-operations**.

We will be sending out a **Questionnaire** to Member States shortly on not just international humanitarian law but an array of international law issues implicated by State cyber-operations.

Our goal is **not to offer a Committee position** on the appropriate answers, but simply to **get Member States to think about the answers** if they've not yet done so **and publicize their views** so that both in the region and beyond.

It's our hope that by compiling a set of OAS Member State views on international law and cyberspace we can **map areas of convergence and divergence**.

In doing so, we hope to improve international law's efficacy with respect to this rapidly growing and critical ecosystem we call cyberspace.

I'll stop here, but am happy to take questions. Thank you.