Respondent

**Presentation.**

1. Good Morning your excellencies.
2. May it please the Court **(reverencia)**
3. My name is ABH and I am the agent for the respondent, the state of RAISLAND
4. I will divide my presentation in 2 issues:

I. RAISLAND bears no international responsibility for the cyber-attacks

II. and **Furthermore** RAISLAND did comply with its due diligence obligation

**I. RIESLAND BEARS NO INTERNATIONAL RESPONSIBILITY FOR THE CYBER-ATTACKS**

As mentioned above, the first issue I will address will be that RAISLAND bears no Int. Responsibility for the cyber-attacks, I will divide this issue in two:

### 1) The cyber-attacks are not attributable to Riesland

### 2) In any event, the cyber-attacks did not breach Riesland’s international obligations.

A State bears international responsibility whenever an **action or omission**

1. Is attributable to it,
2. And constitutes a breach of an international obligation.

|  |  |
| --- | --- |
| **The cyber-attacks are not attributable to Riesland** | **In any event, the cyber-attacks did not breach Riesland’s international obligations.** |
| 1. ***Submitted evidence does not reach the applicable standard of proof***   A cyber-attack may only be attributed to a State whenever **a clear and convincing link** between the former attack and a State *de facto* or *de jure* agent is **proved conclusively**.  For instance, in 2007, governmental offices of Estonia suffered several cyber-attacks that employed methods unavailable to the general public and were traced to Russian governmental computer infrastructures  Nonetheless, NATO members **refrained** **to take action against Russia due to the lack of proof associating the cyber-attacks and any person acting on behalf of that State**.  Similarly, the attacks on *The* *Ames Post* and Chester & Walsingham **were allegedly carried out with the same malware used by the Bureau and traced to Riesland’s governmental infrastructure.**  However, **there is no evidence providing a nexus between the attacks and a Rieslandic *de jure* or *de facto* agent.**  The cyber-attacks are not attributable to Riesland.   1. ***Furthermore, Riesland had no control over the cyber-attacks***   **Conducts of non-State actors are attributable to a State whenever such perpetrator is under its effective control.**  In Nicaragua Case pg 95/99 the *contras* were financed, trained, equipped and received help in planning its operations from the US.  Despite the group’s preponderant reliance on the US, the Court considered that the group lacked complete dependence on the State for its operations and thus its activities were not attributable to the State  Similarly, although allegedly the attacks’ perpetrators employed malware exclusively used by Riesland, there is no evidence proving complete dependence on Riesland’s support by the individual or group that perpetrated the attack.  **The attacks are not attributable to Riesland**. | 1. ***The cyber-attacks do not reach the threshold of use of force***   A cyber-attack constitutes an unlawful use of force **whenever it inflicts a material damage to the scale and effects of a military armed attack**.  ***i.e.* widespread material destruction.**  For instance, in 2009, a cyber-attack on various Iranian nuclear facilities destroyed multiple centrifuges used to enrich uranium and Iran’s nuclear program was delayed for years.  The attacks **were not considered as an unlawful use of force** since the damages **did not reach a widespread material** destruction an armed attack would cause.  Similarly, although the present attacks resulted in the loss of virtual information valuated in €45-50 million they did not cause any physical or kinetic damage whatsoever within Amestonia’s territory, but rather mere informatics loss.  The cyber-attacks were not an unlawful use of force.   1. ***Furhtemore, Riesland enjoyed extraterritorial jurisdiction for law enforcement***   **States may conduct extraterritorial law enforcement measures in cyber-space against threats to their national security**  for instance, whenever anti-terrorism strategies are leaked.  In the *Yahoo! v LICRA* case*,* from America, *Yahoo!* published **certain Nazi materials** on **cyber-space considered as offensive and against public order under French legislation**, causing **a French Court to emit a judgment ordering the cessation of the publications, which *Yahoo!* claimed to be unenforceable in American territory**  However, when submitted to the Court of Appeals in the Ninth Circuit of the US, the latter dismissed Yahoo’s claim and recognized **that the French Court had jurisdiction to enforce its law given that its public order was affected**  Presently, Riesland’s national security was compromised by *The Ames Post’s* since it included, *inter alia*, determinant information concerning Riesland’s counter-terrorism campaign.  Since Amestonia was unwilling to halt the publications, Riesland had to exercise its jurisdiction to protect its national security  **Therefore, in any case, the cyber-attacks constitute a legitimate law enforcement measure** |

**II.FURTHERMORE, RIESLAND DID NOT VIOLATE ITS OBLIGATION OF DUE DILIGENCE**

**Due diligence obliges States to employ all reasonably available means within their capacityto avoid any known activity in their territory that could inflict damage to other States**.

In the *Genocide* case, **an army financed by Serbia** and purely composed by ethnic Serb militaries **attacked a non-Serb Bosnian population**. **The Court ruled that, since Serbia had undeniable influence over the army, it violated its due diligence duty by failing to take any initiative within its power and influence to prevent the attack.**

Conversely, although the cyber-attacks **were launched from Riesland’s governmental** infrastructure, **they were instantaneous and had no continuity**, **rendering the State unaware and unable to prevent the situation.**

Therefore, **Riesland did not violate its obligation of due diligence**.

**Questions: Respondent:**

1. **Standard of Proof:**
2. **Effective Control:**
3. **Genocide Case:**