**Balancing Contradicting Human Rights Obligations in Armed Conflicts and Counter Terrorism workshop**
**December 2 – 4, 2024, Prague, Czechia**

**Round Table Discussion III - Law and Technology**

Chair: Tomás Minárik, Department of International Cooperation and the European Union, National Cyber and Information Security Agency of the Czech Republic

## Critical Infrastructure and Security

The discussion explored the implications of state control over extraterritorial cyber infrastructure, particularly in relation to human rights obligations. Questions arose regarding the extent to which state control over data—such as through cloud services—triggers specific human rights responsibilities, whether in terms of protection, prevention, or respect for fundamental rights.

A key issue was the duty of states to act upon discovering illicit or harmful content while exercising cyber control. If a state gains access to a cloud server or a private computer and finds evidence of criminal activity (e.g., child exploitation material), does it have a duty to intervene? Additionally, the discussion considered the state's obligations to the data owner, such as when private images are discovered. The potential human rights implications, particularly in relation to privacy (Article 8 ECHR), were debated in light of European jurisprudence, including the Romanian case where authorities failed to protect an individual's privacy from non-consensual distribution of explicit images.

## Data Localisation and Extraterritorial Human Rights Obligations

The conversation then shifted to data localisation policies and their impact on human rights. The EU's ongoing efforts to regulate cloud services and limit access to foreign providers were noted, with participants debating whether such measures truly enhance security or merely introduce new risks.

Extraterritorial human rights obligations were examined through the lens of cyber control. If a state exerts effective control over foreign infrastructure, at what point does it assume responsibility for rights violations occurring within that domain? A parallel was drawn to transboundary environmental harm, referencing the American Convention’s approach, which imposes duties on states to prevent cross-border damage. While this reasoning is well-developed in environmental law, European courts have been more hesitant to apply similar principles in the cyber domain.

## State Responsibilities in Cybersecurity and Human Rights Violations

A key scenario involved a cyber attack on critical infrastructure, such as hospitals or water supplies, and the corresponding state obligations. The discussion referenced ECtHR

jurisprudence on positive obligations, particularly in cases of state negligence in preventing foreseeable harm.

The example of a cyber attack on Prague's water system, following years of governmental inaction despite known vulnerabilities, was analyzed in relation to the right to life (Article 2 ECHR). Some participants argued that, under ECtHR precedent, such failures could constitute a violation of state obligations, but only in cases of extreme negligence. The broader question of socioeconomic rights was also raised—while there is an emerging duty to protect essential services, defining its precise scope remains a challenge.

This issue was juxtaposed with counterterrorism measures. If a state refrains from mass surveillance that could have prevented an attack, has it failed in its duty to protect the right to life? McCann and Others v. UK was discussed as a foundational case, highlighting the balancing act between public safety and the right to life, even in cases involving suspected terrorists.

## Freedom of Business and National Security

Another debate concerned restrictions on cloud service providers based on national security grounds. Some companies claim that such restrictions violate their freedom to conduct business—a right recognized in the EU Charter. However, this argument was deemed relatively weak compared to competing state interests. The discussion noted that recent legal developments have seen economic freedoms deprioritized in favor of national security, with a parallel drawn to European cases concerning religious expression in the workplace.

## AI and Cyber Regulation

The role of AI in cybersecurity governance was explored, with concerns raised about regulatory approaches that attempt to impose a uniform legal framework on highly diverse technologies. Participants emphasized the need for issue-specific regulation rather than broad, one-size-fits-all treaties.

One approach suggested was to integrate AI-related concerns into existing legal frameworks rather than crafting entirely new legal instruments. Instead of treating AI as a distinct domain, its impact on specific legal areas (e.g., data protection, autonomous decision-making, or accountability) should be addressed within the corresponding legal regimes.

## Attribution and Accountability in Cyber Operations

The discussion examined current mechanisms for attributing cyber operations to state actors and whether existing legal standards are sufficient. It was noted that most cyber operations involve either state organs or private entities acting under state direction, meaning existing attribution standards remain applicable.

Legal and evidentiary challenges were also highlighted. The issue of proof in cyber attribution—whether states require conclusive evidence or lower thresholds for action—was debated in light of recent state practice. Examples included U.S. legal action against Russian intelligence officers

and UK judicial decisions on cyber espionage cases, such as the hacking of the Emir of Dubai's wife and legal team.

Questions also arose regarding private sector involvement in attribution. Insurance companies and financial institutions are increasingly incorporating nation-state cyber attack clauses into contracts. This raises concerns about whether such determinations align with international legal standards or are based on internal industry criteria. The broader issue of adapting evidentiary rules for cyber-related cases was also discussed—if traditional legal thresholds are unattainable due to the nature of cyber operations, should legal standards be adjusted?

## Privacy and Encryption

Finally, the role of encryption in safeguarding privacy was discussed, particularly in relation to state surveillance and law enforcement access. Participants considered the tension between privacy rights and security concerns, noting that legal frameworks must strike a balance between protecting encrypted communications and enabling legitimate investigations.

Overall, the discussion reflected the complexity of cybersecurity governance, highlighting the intersection of state sovereignty, human rights obligations, and emerging technological challenges.