Roundtable 3: Cyber and the Role of Private Actors
Co-Authored by: Victor Oriere, Erick Lajara, and Jackson Colling

The third Roundtable on "Cyber and the Role of Private Actors" brought together experts to discuss the complex intersection of cybersecurity, private-sector involvement, and international conflict. The symposium was moderated by David Simon of Skadden, and featured Kate Charlet of Google, Matt Fussa of CISCO, Lt. Col Laura West, an Army Judge Advocate, and Jan Kleffner from the Swedish Defense University. The discussion touched on key topics such as safeguarding data during conflicts, public-private partnerships and legal considerations, and the legal implications of private actors in cyber warfare.

Safeguarding Data in Conflict Zones
The roundtable began by addressing the challenges of safeguarding data during conflicts, particularly in the context of the Russian bombardment of Ukraine. Kate Charlet highlighted Google's efforts to protect sensitive data from kinetic attacks, including collaborating with foreign and state partners to store data offsite (Cloud Storage). She further elaborated on Google's efforts to protect users from disinformation by banning Russian state media and adverstising on Youtube while promoting authoritative information. Matt Fussa explained how CISCO has played a role in Ukraine since 2014, assisting Ukraine in researching cyber threats and performing mitigation. CISCO has played a more hands-on role since Russia escalated the conflict, helping to design and build secure networks for Ukraine. Matt Fussa emphasized that, while governments prefer on-site data storage, offsite storage can be more secure with the right rules and safeguards in place. He praised the agility displayed by Ukraine in streamlining bureaucracy during the conflict, highlighting the lessons that can be learned from their example in the face of cyber threats.

Public-Private Partnerships and Legal Considerations
Lt. Col Laura West, drawing on her military background, stressed the importance of public-private partnerships in dealing with cyber threats. She pointed out that sharing information with partners, both international and local, is crucial. However, she also acknowledged the legal complexities surrounding information sharing, including U.S. constitutional law, liability, and restrictions on sharing certain types of information, such as trade secrets. The GDPR was noted as a potential impediment to effective cyberspace information sharing.

Legal Implications of Private Actors in Cyber Warfare
A major topic of conversation was the increasing role that civilians are playing in warfare. Jan Kleffner discussed potential liability for private actors involved in cyber warfare, explaining how civilians in Ukraine have become increasingly involved in cyber operations on behalf of the government. Kleffner highlighted groups like the IT army of Ukraine and talked about civilians assisting the Ukrainian military by sharing Russian positions and information via targeting apps. The panel discussed a sensor-saturated battlefield and the extent to which civilians could be classified as directly participating in hositilities given the prevelance of such targeting apps. This led to a discussion about tech companies' ethical obligations to warn users of the risk that they could be targeted for sharing such information on those apps. The panel then touched on whether private actors connected to war crimes would be prosecuted. Kleffner noted how it is possible for individuals to be held liable for cyber war crimes, but noted domestic courts are the most likely venue given the limited routes to prosecute cyber criminals in international courts. Lt. Col Laura West added that the U.S. relies on domestic laws to go after cyber criminals, but noted that attributing cyberattacks to specific actors remains challenging.