Section 8– Relazioni Internazionali
Chairs: Carla Monteleone, Vittorio Emanuele Parsi

Panel 8.15 Cyber Security and Sovereignty: doctrines, approaches and perspectives

Cybersecurity has become a crucial topic in international affairs, at the intersection of technology and policy at the national and global levels. Different models and definitions of cybersecurity have emerged from the academic debate, and different approaches and strategies have been formulated
by governments, international organisations, security agencies and civil society actors, so that cybersecurity is still a field with blurry boundaries, competing conceptualisations, and marked by simultaneity of interests and threats.
Traditionally, cybersecurity is considered within the realm of the Security Studies (Cavelty 2013; Cavelty - Balzac 2016), and it is an integral part of governments' national defense, foreign and security policies and doctrines (Amoretti – Fracchiolla, 2017; Adamson, 2016). Also, cybersecurity calls into question the issue of sovereignty, unfolding it into new and multifaceted fields of application, and bringing into the scene new strategic actors such as epistemic communities, Internet corporations, IT vendors, standard organisations, social movements and so on, beside traditional actors such as national governments, international organisations, the military, police forces, intelligence, etc. Further, recent contributions have highlighted the constitutive role of culture, and particularly the security cultural context, in structuring the cybersecurity field and different paths of action (Kaldor 2016, 2018).

Against this complex scenario, the panel seeks to discuss conceptual, strategical and operational developments of cybersecurity. Papers are invited to investigate – theoretically, methodologically and empirically – some crucial questions, including the following ones:

• Who has the sovereignty to deal with the threats and to give a normative framework in the cybersecurity field?
• Who is in charge to enact coercive or preventive actions?
• In what context is a claim of state sovereignty likely to occur?
• To whom is a sovereignty claim addressed?
• What normative structures are used to determine the legitimacy of a sovereignty claim?
• Which are contents and features of this emerging international public policy that represent the state in action?
• How is cybersecurity framed and addressed in different political, cultural and institutional contexts?
• Which are the relationships between state and non-state actors?
• Which processes of institutionalisation are affecting cybersecurity?
• What are the relationships between cybersecurity and other technology-related new policy fields?
• What is the role of public discourse in building cybersecurity narratives and in legitimising actors and strategies?

Chairs: Domenico Fracchiolla,Mauro Santaniello