

Bart Jacobs, Radboud University, Nijmegen, The Netherlands

Cyber Security and Warfare

This talk will illustrate how the traditional relational status between countries in terms of the distinction "in war" or "not in war" has become fuzzy due to digital developments. The small scale confrontations between opposing intelligence services during the Cold War (see e.g. the book "Spies" by Calder Walton) have developed into more large scale confrontations (like the Stuxnet case, see "Countdown to zero day" by Kim Zetter) with larger impact and where a lack of clear attribution gives not only more space to manoeuvre but also more risks of escalation. At the same time, against the expectations of many, the war in the Ukraine has remained largely kinetic. This will offer ample opportunities for further discussion.

Cyber Intelligence

Traditionally, spying involves "humint", intelligence from human sources. In the 20th century the emphasis has shifted to signals intelligence ("sigint"), which works faster and is often more reliable. The resulting communication security issues have a defensive and offensive side, sometimes with opposing interests --- see the recurring discussions about end-to-end encryption for message-apps. The latest dimension in this development is hacking for intelligence purposes, which may be even more efficient than sigint, since it can give access to information before encryption takes place. The general aim of intelligence services to control strategic (information) positions has taken new forms in the digital age. After these general developments, this talk will focus on the disinformation (see the book "Active Measures: The Secret History of Disinformation and Political Warfare" by Thomas Rid) and the importance of authenticity of information, now that we are entering the era of automatically generated content (see "The AuthenticityCrisis", <https://doi.org/10.1016/j.clsr.2024.105962>).