This study examines hactivism and cyberterrorism, how OSCE participating states have responded to these phenomena and have these responses respected user's human rights, especially the right to freedom of expression.OSCE states have responded to hacktivism and cyberterrorism with domestic legislation and institutions, international conventions, technical measures and specialized institutions.Cyberterrorism consists of politically motivated illegal attacks against information, computer systems, programs and data resulting in violence against noncombatant targets.This right includes the freedom to hold opinions without interference and seek, receive and impart information and ideas trough any media and regardless of frontiers.Software piratism, copyright issues and cyber war attacks conducted by states are outside the scope of this study.A short case study on Poland is included.