Suggestion for paper for ISMS Copenhagen 6-8 NOV 2023. Book chapter under preparation for RDDC book project.

Mikkel Storm Jensen, Major, MSc, Phd-candidate.
msje@fak.dk

Title: The Cyber War in Ukraine – Initial Insights:

Russia's relentless attacks on Ukraine through cyberspace that has accompanied the full-scale invasion since February 2022 have so far provided three valuable insights into cyber's role in modern inter-state conflict:

Firstly Russia's ability to inflict paralysing or destructive attacks on Ukriane through cyberspace has been less than feared and perhaps expected prior to the invasion. While Russia's ability has proven inadequate to the task, her demonstrated willingness to inflict potentially destructive attacks has been high. Further more Russia has through proxies conducted a large number of nuisance attacks against Western states, including Denmark, to undermine their support for Ukraine. Hence it is important to revisit how well the Western democracies are implementing societal cyber resilience strategies.

Secondly the war has given students of offensive cyberspace operations' strategic role in interstate warfare between modern, digitalised industrial states the first empirical observations to validate hitherto theorised assumptions regarding the means' military efficacy. The initial observations indicate that our conceptual understanding of such operations may shift from "cyber-Pearl Harbor" to "death by a thousand cuts".

Thirdly a hitherto unseen number of non-state actors have emerged to participate in the cyber conflict: Russian criminals and "active patriots" attack targets in Ukraine and Western states that support their defence, whereas Anonymous and other Western-based hackers attack targets in Russia, sometimes under the umbrella of the Ukraine IT-Army. While one can only have sympathy for this, the West's passive approach to such cyber vigilantes may undermine Western efforts to uphold norms for responsible state conduct in the cyber domain.