Removing the veil on Offensive Cyberspace Operations - Implications for Sweden

Gazmend Huskaj
Swedish Defence University, University of Skövde

Abstract: The aim of this research is to remove the veil on offensive cyberspace operations. Shrouded in secrecy, limited information about offensive cyberspace operations has existed. Furthermore, certain States have limited knowledge about cyberspace operations in general, and offensive operations in particular. This is especially true if States fulfil the criteria of long military neutrality, long history of peace and lack of experience of what actions to take if the motherland is threatened. Therefore, offensive cyberspace operations for deterrence for defense requires further investigation. Removing the veil on offensive cyberspace operations is achieved by surveying the current state of research in offensive cyberspace operations; how an ambidextrous model and framework for offensive cyberspace operations should look like; what ethical and policy implications are related for vulnerability disclosure?; what ethical dilemmas are related to conducting offensive cyberspace operations?; what considerations should be taken by cyber commands when designing attack infrastructure for offensive operations?; to explore the possibilities of collecting meaningful data for research on Command and Control, Cyber Situational Awareness and Intelligence during a cyber defense exercise; and how the threat from offensive cyberspace operations is perceived by the civilian sector. The research design is grounded in the philosophical paradigm of interpretivism because it is well suited for research that identifies, explores and explains phenomena in a social context, and how information systems are used. The philosophical paradigm directs the choice of research strategy, data generation methods, and data analysis. This research uses the case study research strategy, with interviews, observations and documents as data generation methods, and applies qualitative data analysis. The preliminary results show that to conduct offensive cyberspace operations for deterrence for defense requires not only doctrine, training and exercises, it first requires a deterrence strategy that directs how offensive cyberspace operations are to be used against which adversarial targets. Next, the policy level requires an understanding of what offensive cyberspace operations are, how they are conducted, what kind of attack infrastructure is required, what ethical dilemmas with zero-day vulnerabilities exist and the conduct of offensive operations, and who gives the green light to GO, and who takes the political risk. Finally, intelligence support from multiple intelligence disciplines as well as Cyber Intelligence, Surveillance and Reconnaissance (ISR) is crucial for the success rate of offensive cyberspace operations.