Abstract

This study examines the role and utility of low-severity cyber operations in one state's policy toward another within the context of a long-term hostile feud. This study has fulfilled this task through an explanatory qualitative analysis with cyber operations as an embedded unit of study. The subject of research is the policy of the Islamic Republic of Iran toward the United States in the time spanning from the historic agreement of the Joint Comprehensive Plan of Action (JCPOA), also known as the Nuclear Deal, in July 2015 through 2020. The *role* of the cyber operations in Iran's policy is examined by juxtaposing the pattern of escalations and de-escalations occurring in the context, and in the political and military domains conducted by the Islamic Republic with their deployment of cyber operations. Through this pattern matching, this study identified a visible relative restraint in the cyber domain during the first years following the conclusion of the JCPOA, as the Islamic Republic had obtained its top strategic goal, defined as eliminating all sanctions burdening its economy. Iran's cyber operations towards the United States re-emerged when Washington exited the Nuclear Deal in 2018 and began re-instating sanctions, and the operations were intensified when Tehran began steadily escalating in the political domain the following year. The *utility* of the operations was determined by examining the pattern detailed and the direct and indirect implications of the operations seemingly benefiting the Islamic Republic.

The identified pattern suggests that the operations fulfill the function of signaling broad policy stances and are generally not used as a precision tool. The cyber operations appear to be deployed as a supplementary measure of signaling tied to the moves in the political domain. Meanwhile, the military moves are dual in aim and appear to follow a parallel rationale. Although the *direct* effects of the Iranian cyber operations were almost absent, the indirect and communicative effects were positive for Tehran. The psychological aspect of cyber operations prove a central part of their effectiveness for the Islamic Republic, making resistance visible, yet with vanishingly little escalation risk. The findings of this study strengthen the scholarship on policy in cyberspace that holds that cyber operations of low-severity *can* have a positive effect on a state's stance in an adversarial relationship. This research indicates that the entrance of cyber operations in a dynamic feud does not have to increase the escalation risk in the relationship because the wielder of the operations can obtain a needed effect through low-severity operations. Thus, the presence of cyber operations can

be seen as stabilizing because they provide an option for signaling discontent with low escalatory risk. The study further provides evidence on how low severity cyber operations can function as conscious signaling tools despite their covert nature, supporting their status as ‘open secrets’ alluded to in segments of relevant literature.

Keywords

Cyber Operations, Cyber Policy, Escalation, Coercion, Non-Coercive Cyber Operations, The Islamic Republic of Iran, The United States of America, The JCPOA, Iran Nuclear Deal, Trump Administration, Maximum Pressure Campaign, Cyber Competition, Cover Cyber Operations, Political Escalation, Military Escalation, Cyber Escalation.