# How Risky are Advanced Cyberattackers who Face Uncertainty?

Amitai Gilad

## Abstract

This study develops defense strategies against sophisticated and well-funded cyber-attacks that can cause extensive damage to major organizations. We develop and analyze a game between a cyber-attacker and a defender operating a network that manages a large organization (a bank, say) in which the defender moves first and deploys detection measures to protect her network from cyber-attacks. Then, the attacker, who has learned the network structure and defense profile, attempts to deliver the maximal flow of malicious elements to a target node, possibly by investing in R&D to remain undetected. While previous studies analyzed the deterministic game setting using *graph cuts* and found the optimal set of arcs to defend in the graph (a d-cut), in this study we seek to understand whether and how the defender's optimal strategy is affected by uncertainties that are posed to the attacker. Specifically, we analyze the game under two types of uncertainties: (1) the attacker's uncertainty regarding the defender's vigilance level (Vigilance-U); and (2) the attacker's uncertainty regarding the outcome of his R&D program (R&D-U). We find that the attacker's willingness to invest in R&D is increasing and then decreasing in the magnitude of Vigilance-U, whereas the selection of the d-cut remains consistent. In addition, we find that the level of R&D-U affects the allocated budget to R&D and the probability of actual detection, and consequently the selection of the d-cut by the defender. Finally, we discuss real-life data to develop hypotheses, which in turn support policy-makers in devising strategies that utilize these mere uncertainties.