Reasoning about Security Interventions

Computer security is practiced largely as a reactive discipline -- putting in place mechanisms or procedures to thwart the efforts of adversaries. These range from purely technical defenses, to civil seizures and criminal prosecutions. In each case, the hope is that each particular action will prevent or mitigate the harm being perpetrated and even disincent future attacks of the same variety. However, while there are tremendous resources focused on developing and deploying such security interventions, we lack a firm foundation from reasoning about their efficacy -- what actions are truly disruptive to our adversaries and which simply represent a minor nuisance? In this talk I will discuss a research agenda we've been pursuing over the last five years to place security intervention on an empirical footing. By combining a holistic understanding of online attackers, their motivations and business structures, with large scale empirical intervention experiments, we've been able to shed significant light on these questions. How do various kinds of techniques -- filtering, blacklisting, deranking, server seizures, domain name seizures, merchant account closures, and botnet takedowns -- impact real security outcomes? While we have not settled the general issue of security "return on investment" I will provide strong evidence that real-life efficacy varies considerably between approaches and that a more strategic, data-driven approach to security is likely to maximize impact.