How do complex systems protect themselves from malicious behavior?

Benjamin Edwards
University of New Mexico
bedwards@cs.unm.edu

Stephanie Forrest
University of New Mexico
Santa Fe Institute
forrest@cs.unm.edu

May 6, 2015

Abstract

In many complex systems, self-optimizing agents exploit other agents and their environment to achieve a competitive advantage. When such behavior subverts the operating rules of the system, whether explicitly stated or implicit, it is viewed as malicious. Thus, viruses and cancer exploit the reproductive mechanisms of host cells to replicate and spread; Invasive species displace natives by occupying under-filled niches; Bullies use intimidation to exert power in social groups; Investors are duped by numerous schemes to manipulate financial markets; and cybercriminals exploit software and supply-chain vulnerabilities to steal information and money, block access to critical resources, or harm victims directly.

It should not be surprising then that a wide variety of defenses has been devised to counter these myriad threats. In this paper we argue that although the variety of malicious behaviors is vast, most defensive responses fall into a few generic categories: Observe, Hide, Filter, Repair and Counterattack. Cancer screenings and intrusion-detection systems are examples of observation. Bully avoidance, camouflage and the Tor network are examples of hiding. Blacklisting malicious IP addresses and quarantines of infected populations are examples of filters. Releasing software patches and gene editing are examples of repair. Botnet takedowns, fines and corporal punishment are examples of counterattacks.

Not all complex system use each of these defenses, but most that we have studied exemplify at least one of these strategies. The paper describes the basic categories of response with illustrations from multiple complex systems, including the immune system, medicine, and cybersecurity.

A common language and framework for understanding malicious behavior and responses across many complex systems will support the development and communication of generic models for these processes. We speculate that such models will reveal important patterns and provide guidance about when particular kinds of defenses will be most effective.