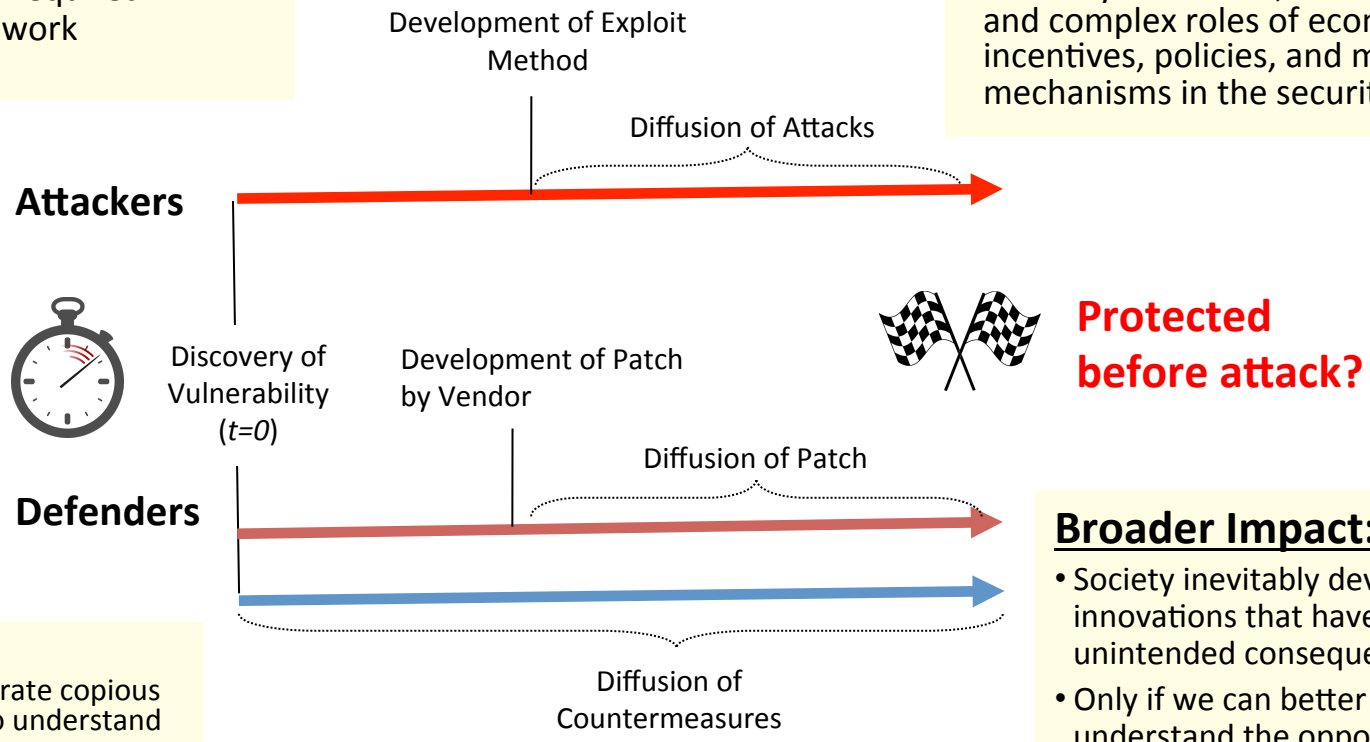
Using Analytics on Security Data to Understand Negative Innovations

Challenge:

- Unlike defenders, attacker behavior is difficult to understand
- Typical techniques (e.g., surveys, lab experiments, "required" reporting) won't work

Scientific Impact:

- Economic and sociology theories of technology adoption model diffusion of a negative innovation through an attacker population
- Quantify the subtle, non-intuitive and complex roles of economic incentives, policies, and market mechanisms in the security setting



Solution:

- Modern systems generate copious trace data; use data to understand attacker behavior.
- Don't expect technical panaceas; instead, model attackers as economic agents in an innovation race of technology adoption

Broader Impact:

- Society inevitably develops innovations that have unintended consequences.
- Only if we can better a) understand the opposing diffusions and b) educate / communicate can we benefit from innovation and reduce concomitant negative consequences.

Award 1350061: Sam Ransbotham, Boston College