



What is the Game in Cyber Security?

Ravi Sandhu
Executive Director and Endowed Professor
February 2011

ravi.sandhu@utsa.edu, www.profsandhu.com, www.ics.utsa.edu

- Multiple games at multiple levels
- More than 2 players or teams
 - ❖ defenders, attackers, technology innovators, ...
- Many ways to change the game

- Biggest challenges
 - ❖ we don't get to set the rules
 - ❖ we don't get to pick the adversary
 - ❖ asymmetric: defense is harder than offense

- Most important recommendation
 - ❖ cyber security needs to be a proactive rather than reactive discipline

From Wikipedia, the free encyclopedia:

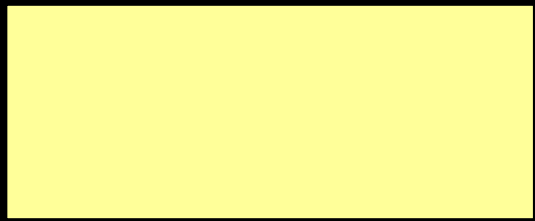



Microeconomics (from Greek prefix micro- meaning "small" + "economics") is a branch of economics that studies how the individual parts of the economy, the household and the firms, make decisions to allocate limited resources, typically in markets where goods or services are being bought and sold. Microeconomics examines how these decisions and behaviors affect the supply and demand for goods and services, which determines prices, and how prices, in turn, determine the supply and demand of goods and services.

This is a contrast to **macroeconomics**, which involves the "sum total of economic activity, dealing with the issues of growth, inflation, and unemployment. Microeconomics also deals with the effects of national economic policies (such as changing taxation levels) on the before mentioned aspects of the economy.

- Most cyber security thinking is microsec
- Most big cyber security threats are macrosec

- **Microsec**
 - ❖ Retail attacks vs Targeted attacks
 - ❖ 99% of the attacks are thwarted by basic hygiene and some luck
 - ❖ 1% of the attacks are difficult and expensive, even impossible, to defend or detect

- Rational microsec behavior can result in highly vulnerable macrosec

	Old technologies	New technologies
Old attacks		
New attacks		

➤ Cyber Security is all about tradeoffs

