Paradox of Terror Prevention

Parimal Bag (National University of Singapore)
Nona Pepito (ESSEC Business School)

SAS ERM - ESSEC CREAR Conference
26-27 July 2018

Surge in terror threats and attacks

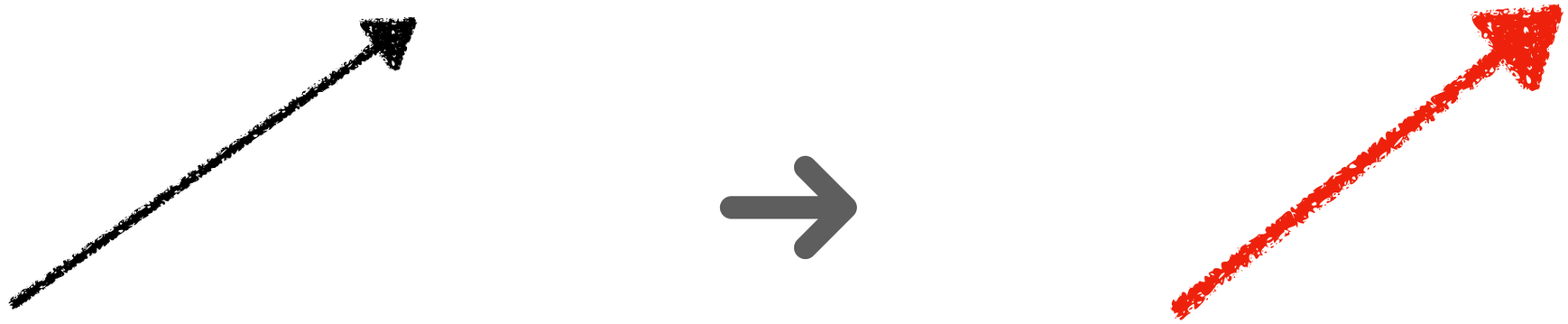
Counterterror spending

US federal expenditure on homeland security

Has grown by $360 bn annually on average since 2001

EU

€5.7m (2002)
€93.5m (2009)



Counterterror spending

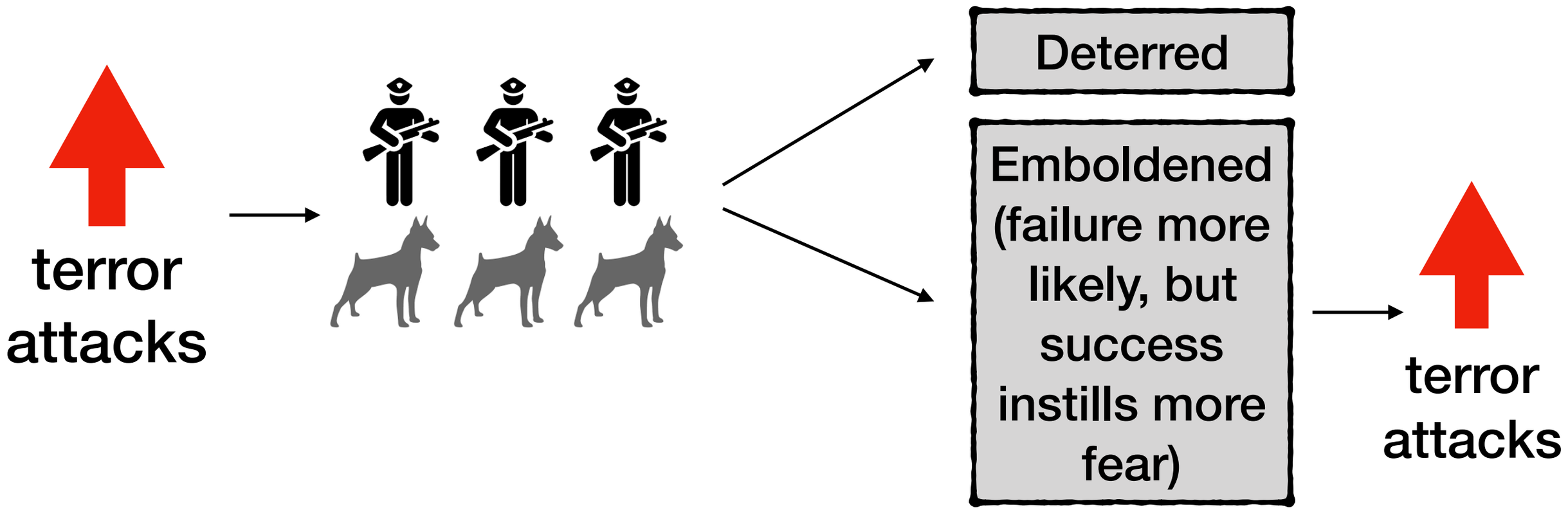
Terror incidence and severity

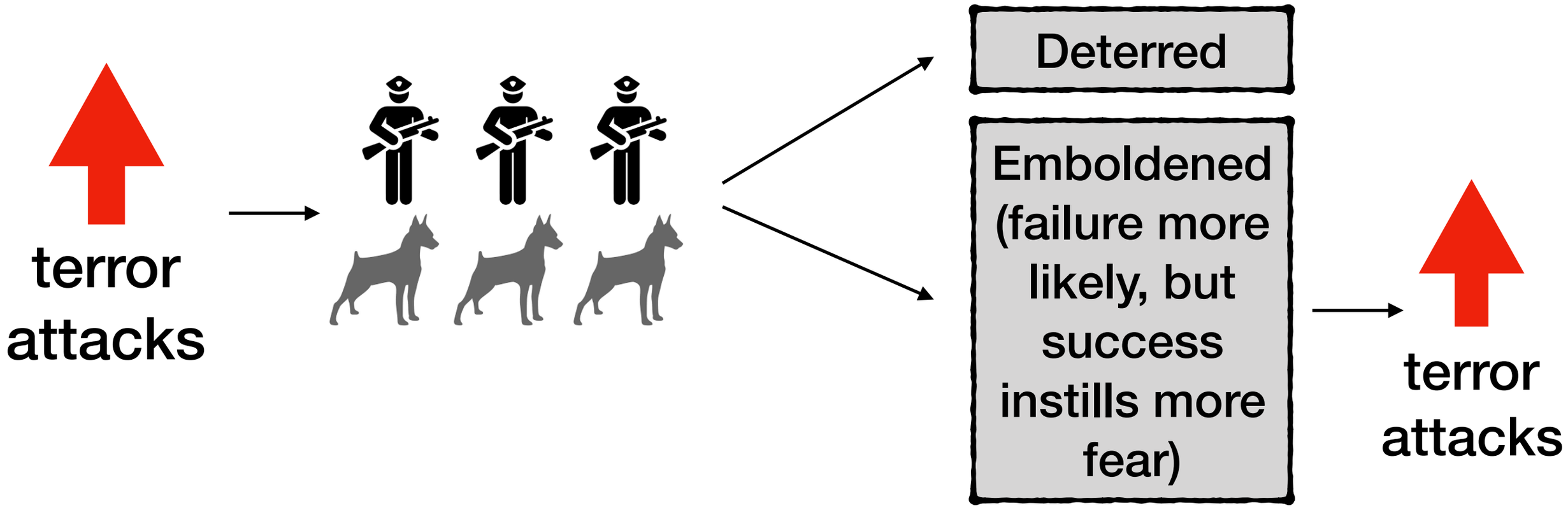
Relevance of paradox for cybersecurity

- Cybersecurity has become a vital element of deterrence
- Cyber attacks may be political

WHY?

- One explanation: spending framework is flawed
- **Another explanation (our focus):**



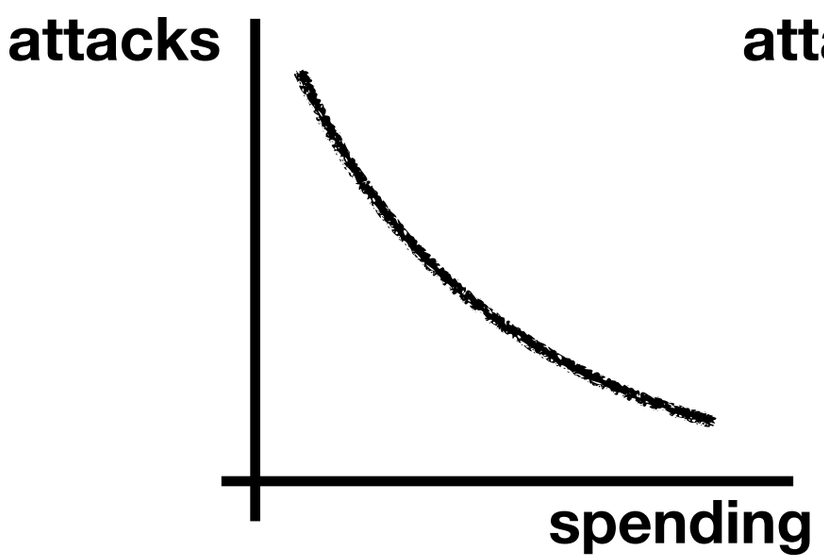


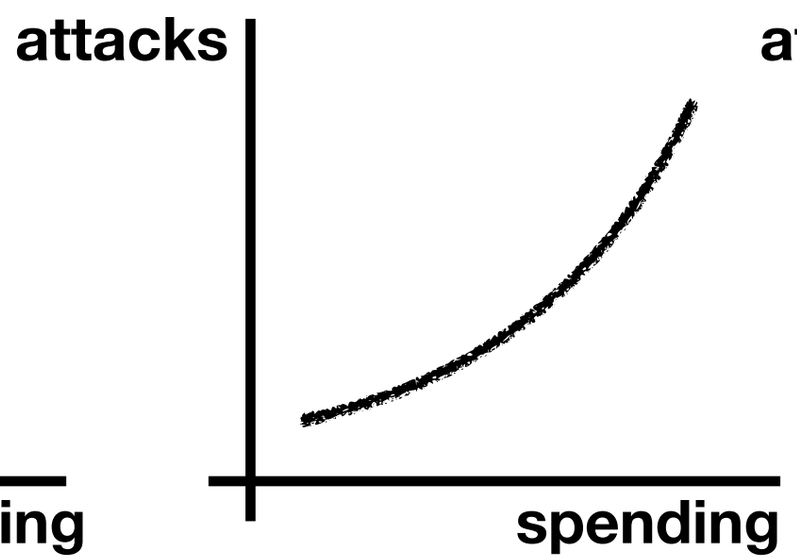
- Our paper is game-theoretic: anticipation and response to risks has to take into account that terrorists are strategic, calculating actors

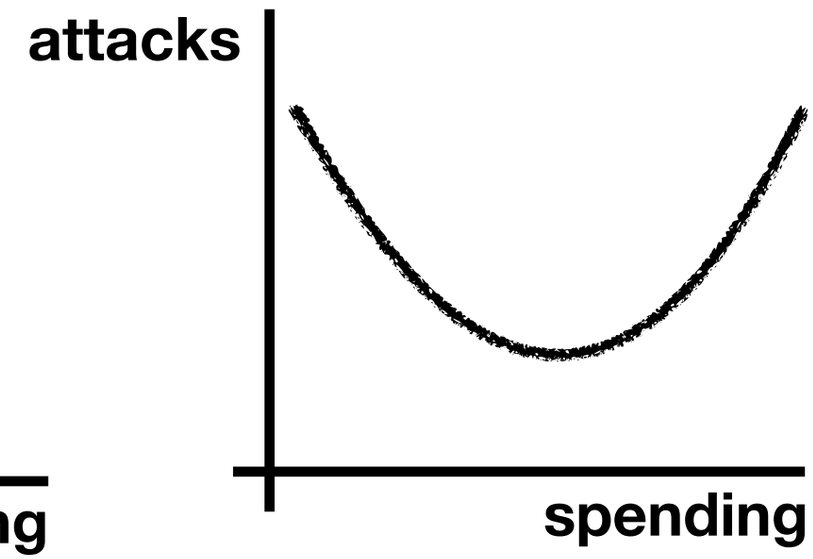
- Has implications on the assessment of cyber risks

Questions

- How do we explain the paradox?
- Nature of the relationship: monotonic or non-monotonic?

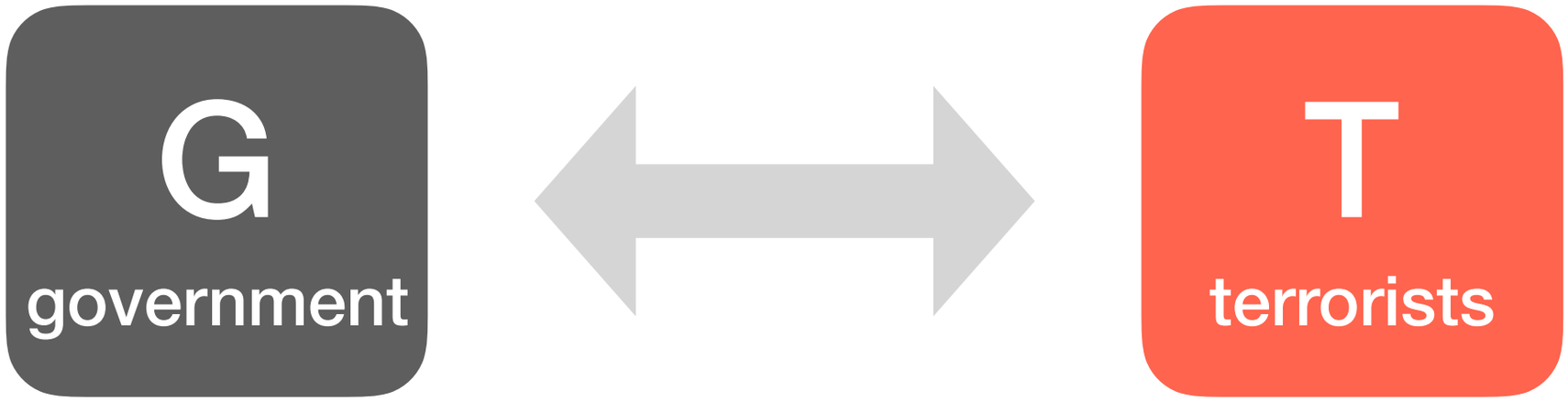






- If increased spending can lead to more aggression, then how can counterterror strategy be improved?

The environment



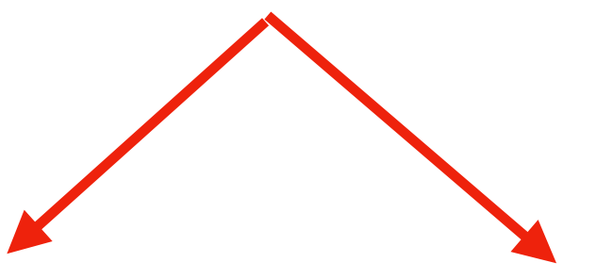
Aim: deter T

Tool: counterterror spending (g)

$$\uparrow g \rightarrow \downarrow \mu$$

Aim: inflict damage, sow fear, destabilise

Tool: attack



$$[\textbf{Prob} = \mu]$$

Uncertainty

high-ability
low-ability

G

Uncertain about the type of the terrorist

affects the effectiveness of spending *g*

T

high-ability
med-ability
low-ability

Uncertain about the type of the government

attack

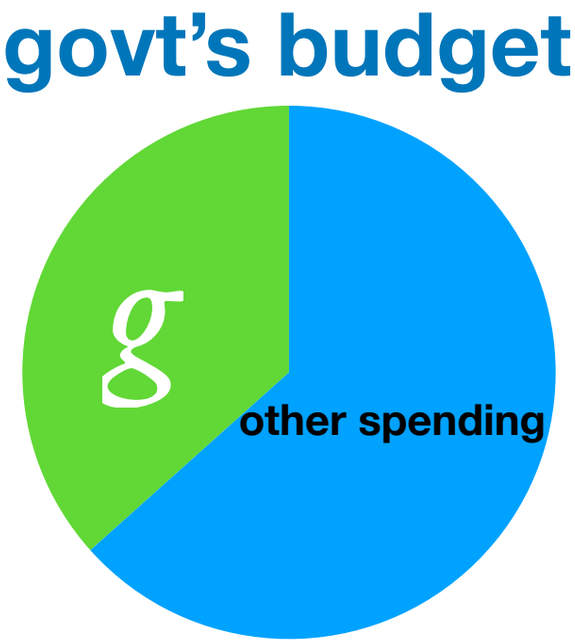
succeed

fail

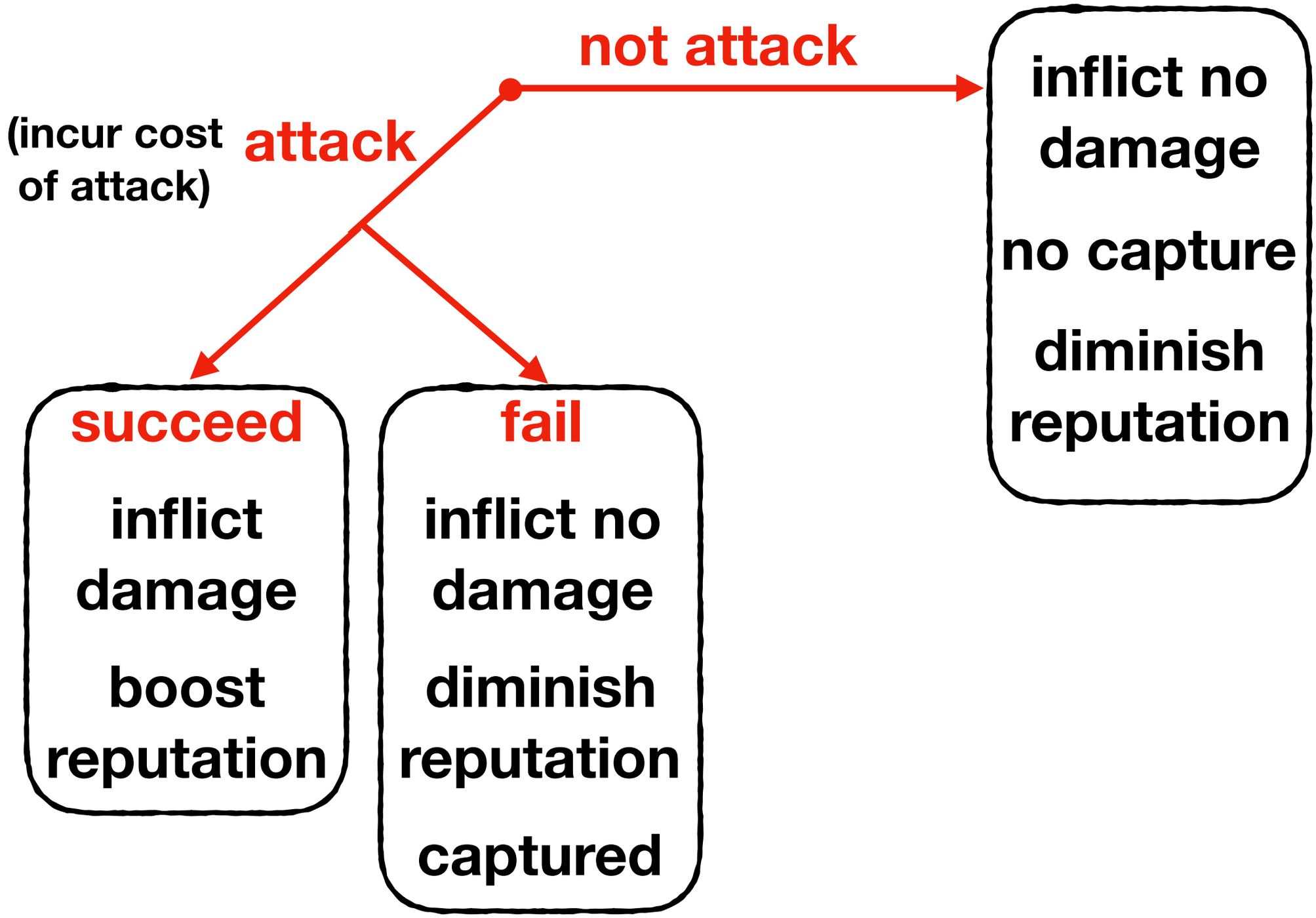
[Prob = μ]

Govt receives a signal of the terrorist's type

$$\sigma \rightarrow g$$

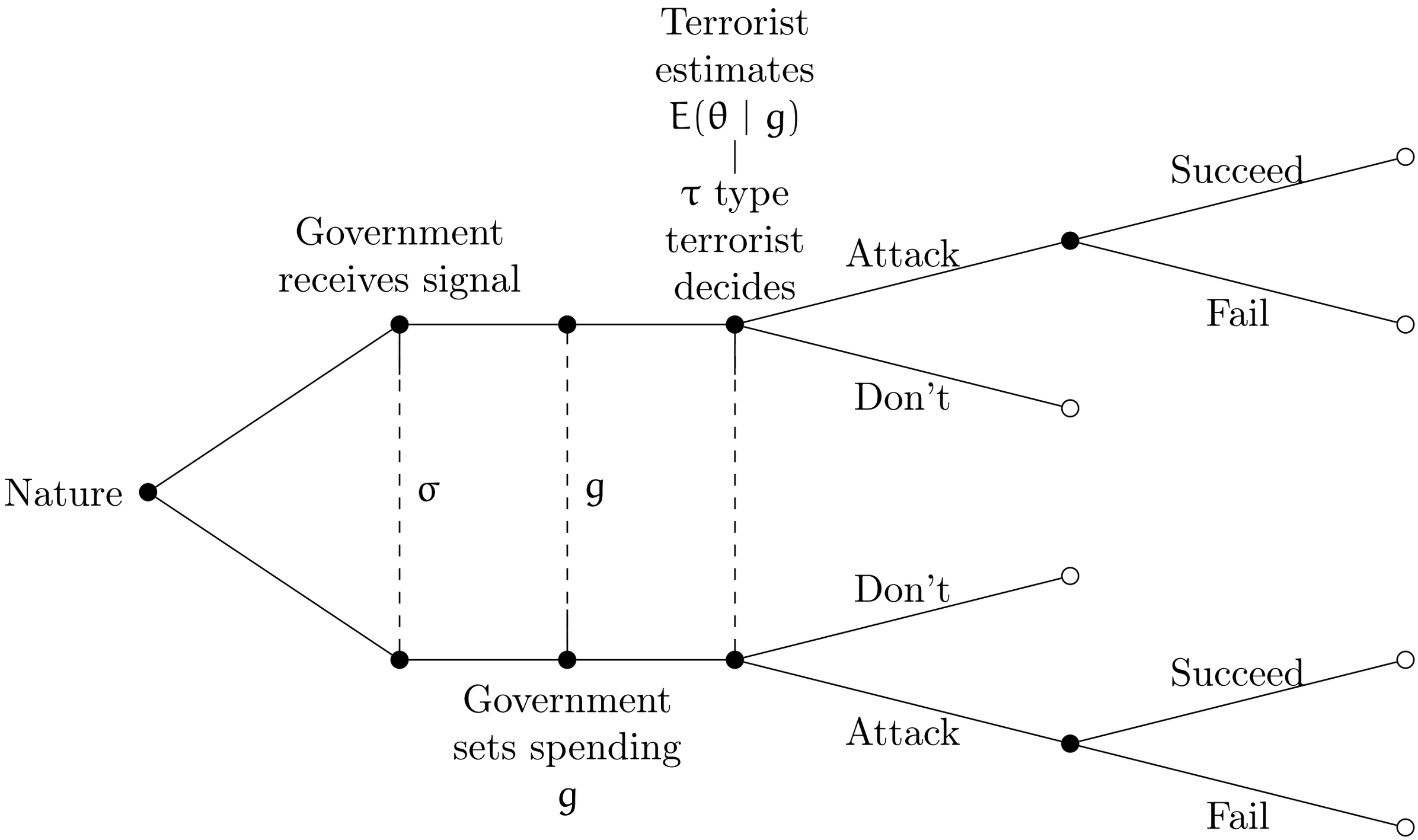


Terrorist's payoffs

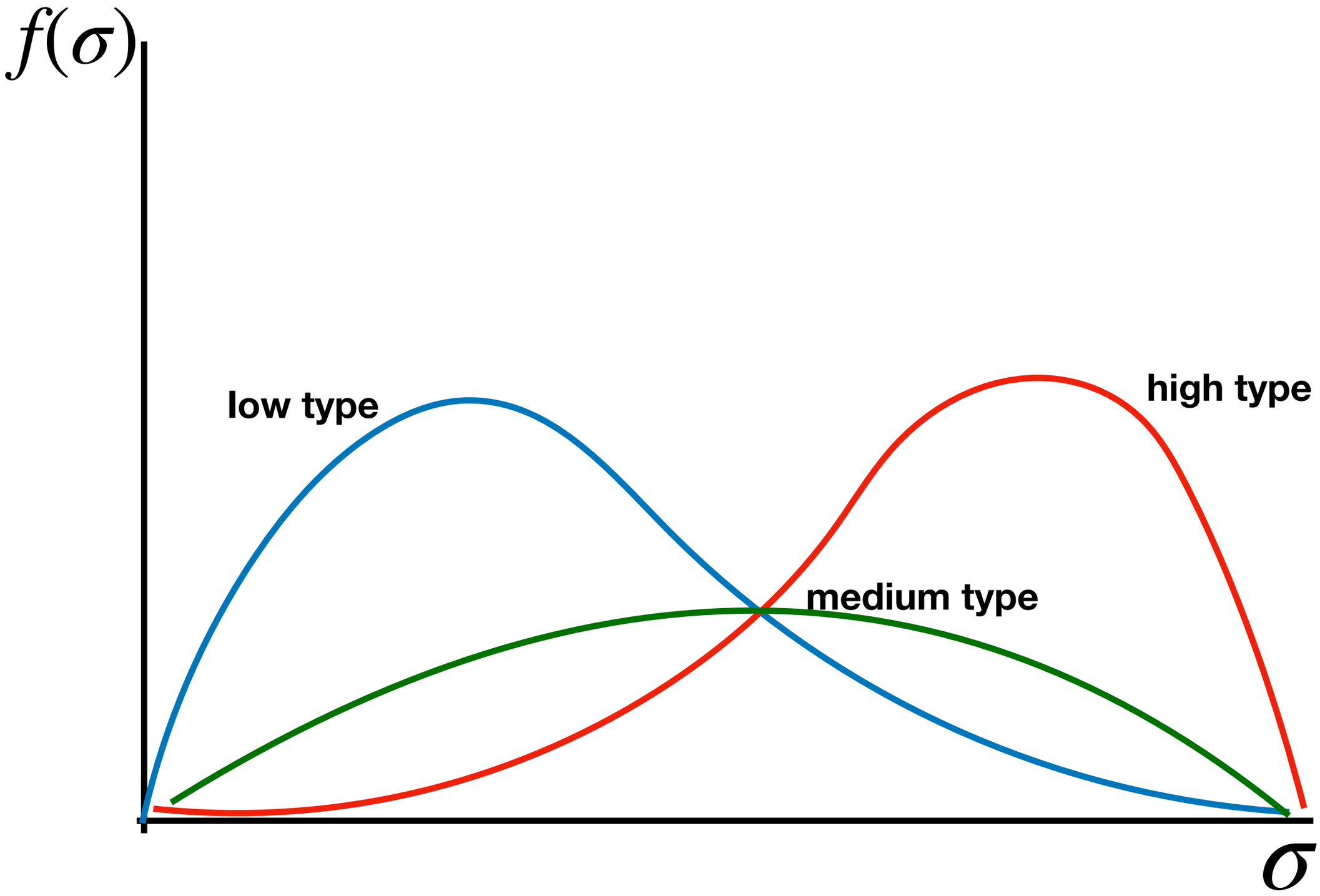


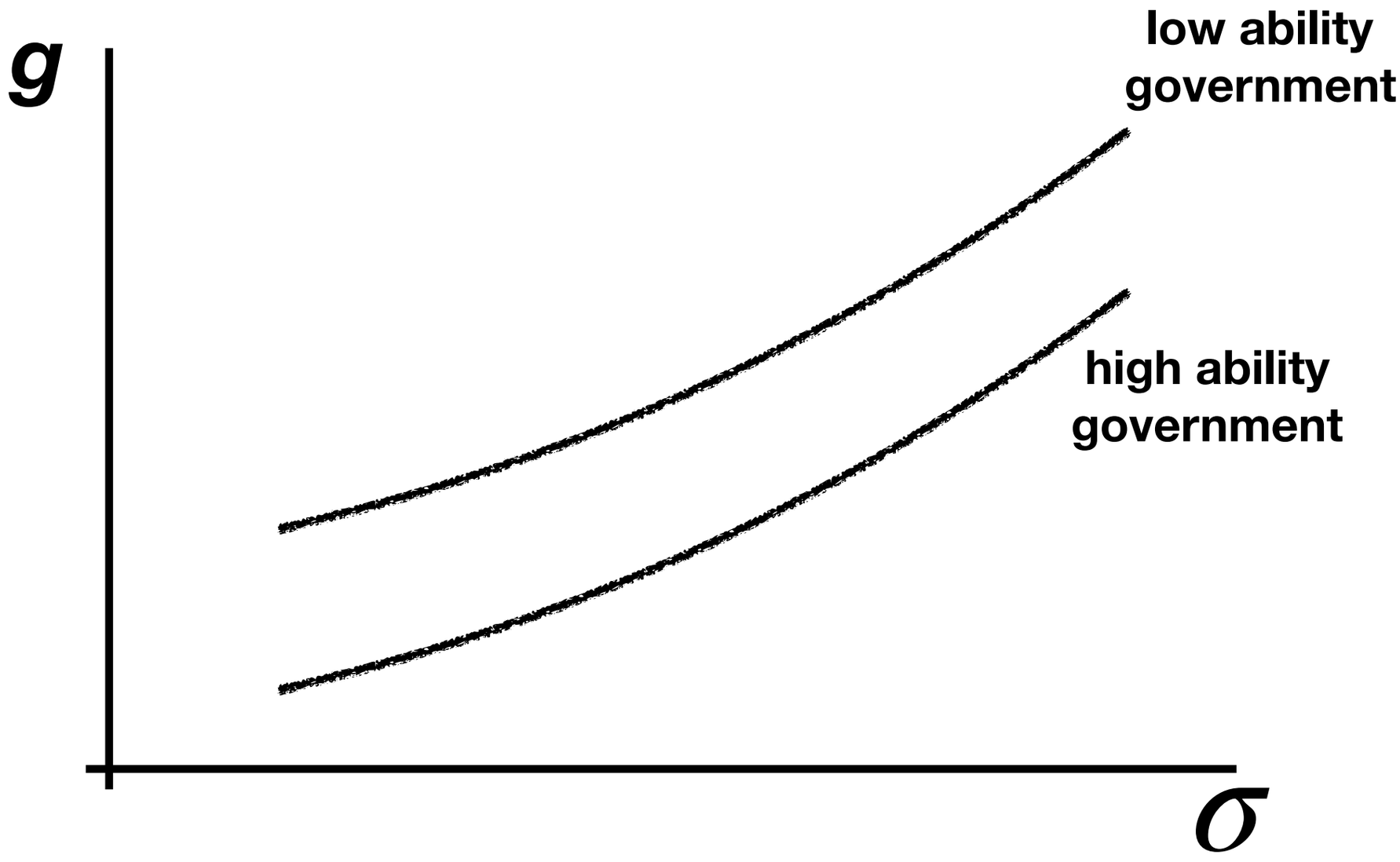
Timeline

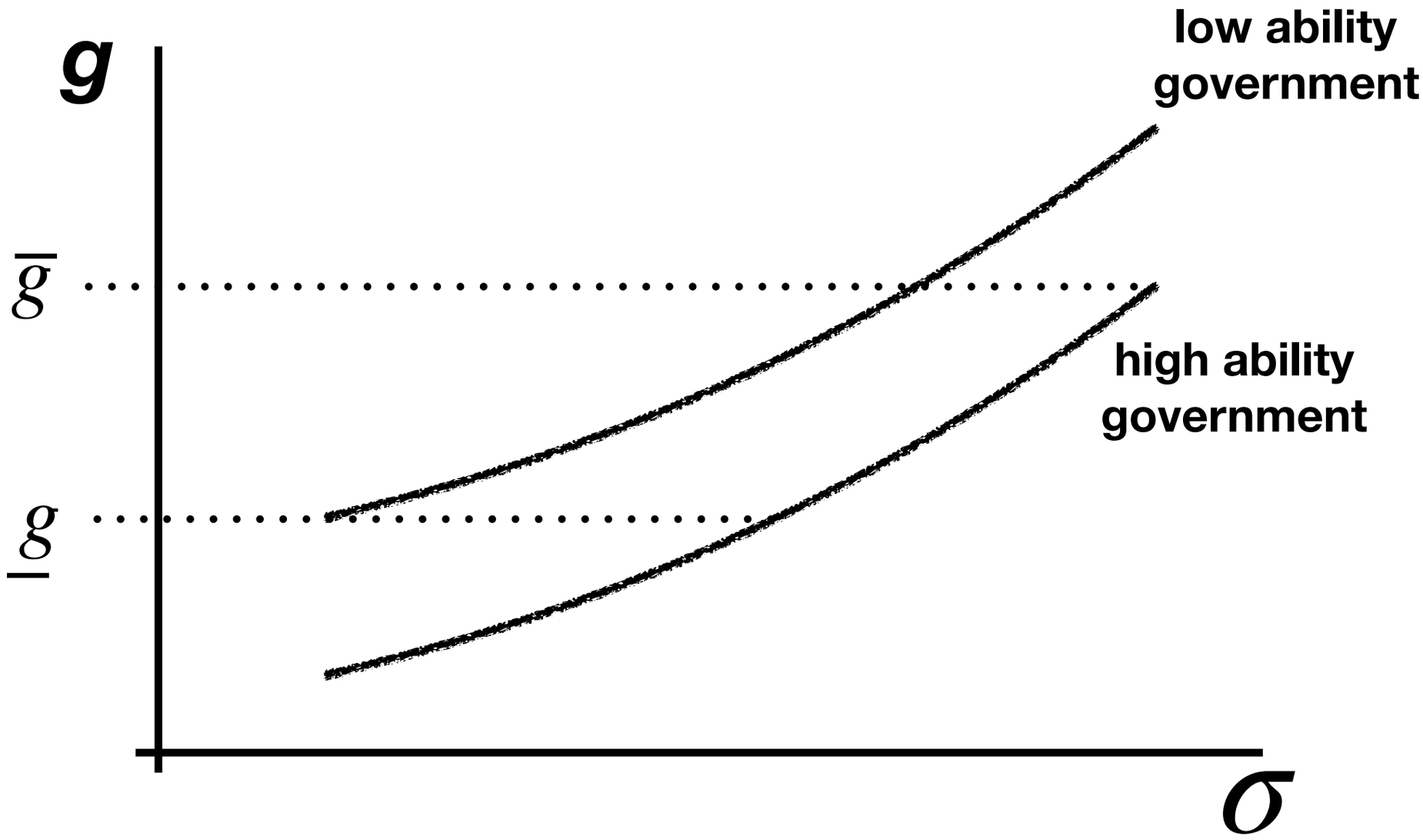
- **G** receives signal of terrorist's type
- **G** sets counterterror spending ***g***
- **T** observes ***g*** and infers **G**'s type
- **T** decides whether to attack or not
- Public sees ***g***, **T**'s decision, and in the case of an attack, whether successful or not
- Public forms beliefs about **T**'s type


Terrorist
estimates
E(θ | g)
|
τ type
terrorist
decides
Government
receives signal
Attack
Succeed
Fail
Don't
Nature
σ
g
Don't
Government
sets spending
g
Attack
Succeed
Fail

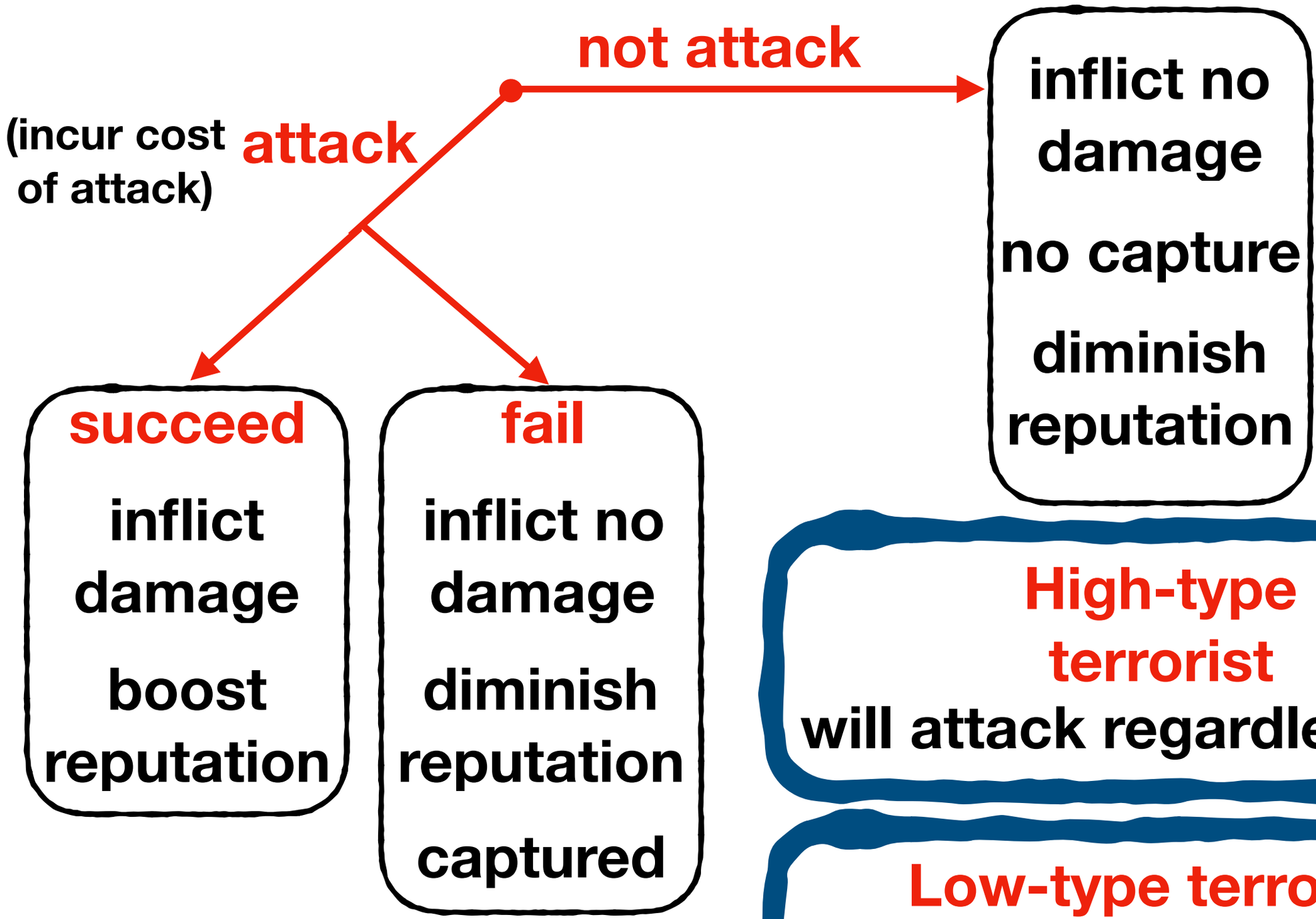
How does g vary with σ ?




g
low ability
government
high ability
government
σ

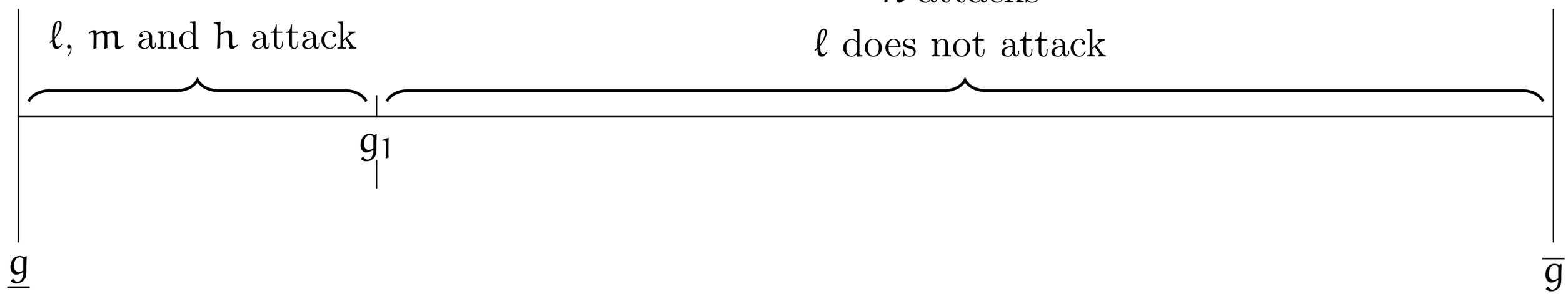

g
low ability
government
high ability
government
σ

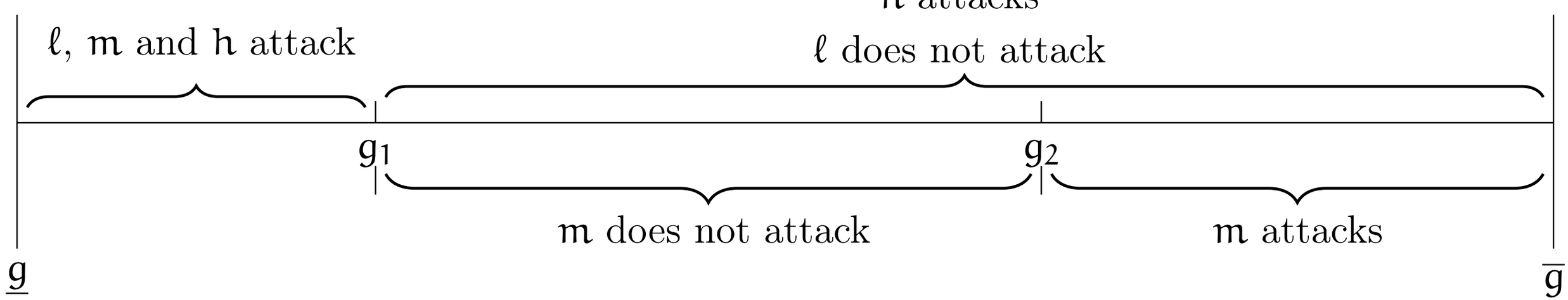
Terrorist's decision

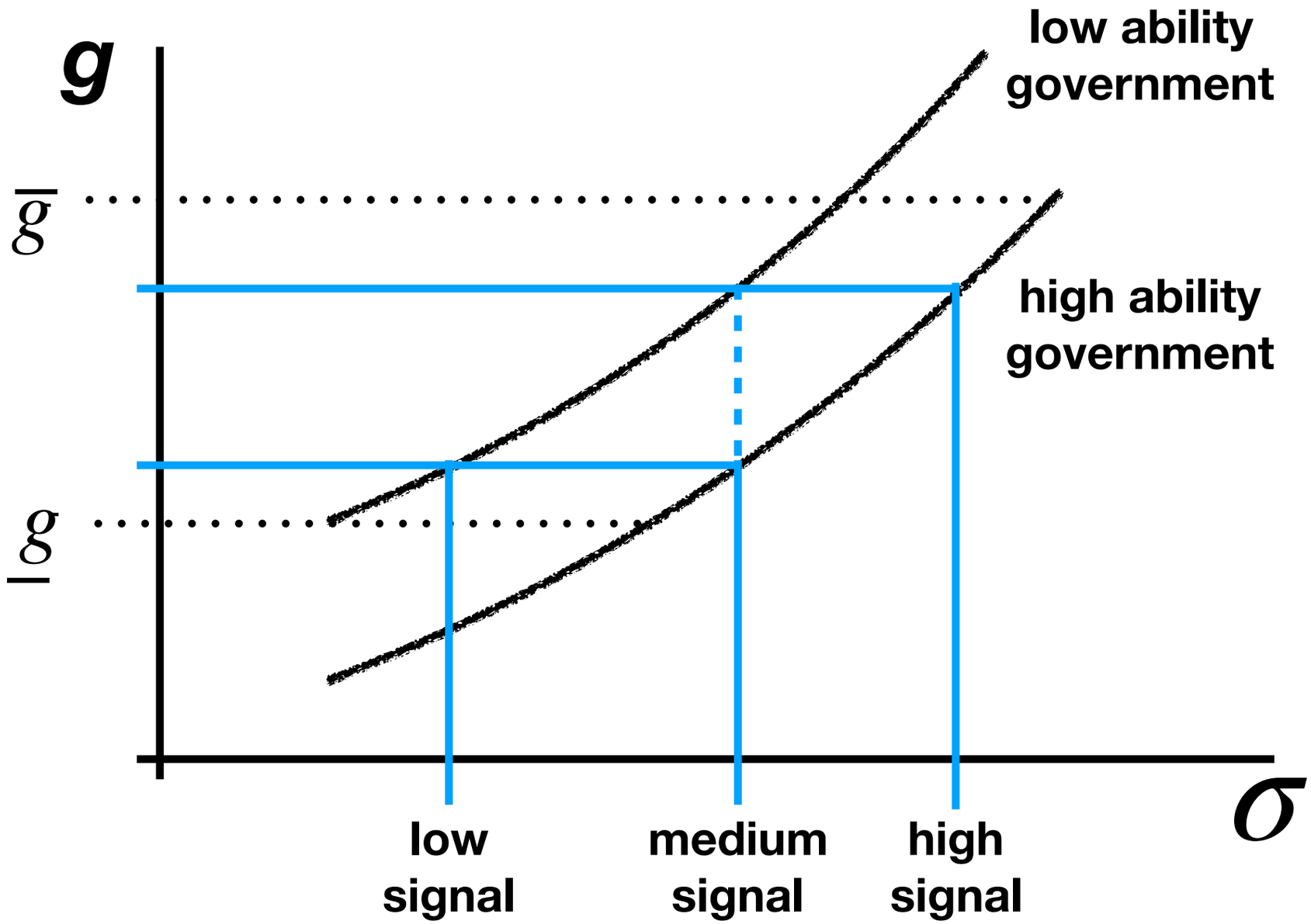


High-type terrorist
will attack regardless of *g*

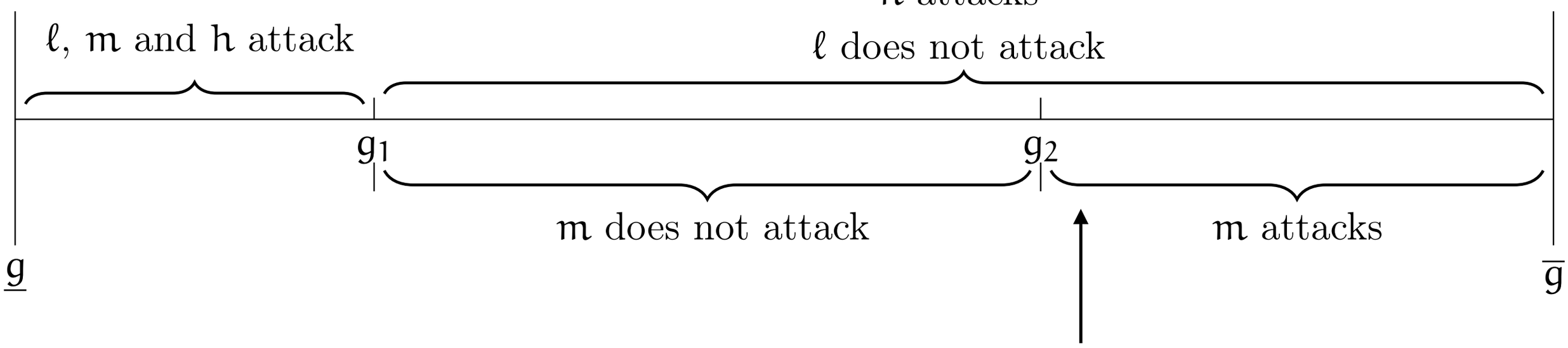
Low-type terrorist
will attack only at low levels of *g*


$\mathfrak{h}$ attacks
ℓ, $\mathfrak{m}$ and $\mathfrak{h}$ attack
ℓ does not attack
g_1
$\underline{g}$
$\overline{g}$


ℓ, m and h attack
h attacks
ℓ does not attack
g
g1
g2
m does not attack
m attacks
g
g


g
low ability government
high ability government
$\bar{g}$
$\underline{g}$
σ
low signal
medium signal
high signal

Main result:
relationship between deterrence efforts and effective deterrence is non-monotonic



belief-flipping by the medium-type terrorist

Main points

- When terror attacks are on the rise, the government wants to deter and foil further attempts

- At the same time, terrorists want to destabilize and create panic

- Focusing on visible terror prevention initiatives, these counterterror efforts can lead to more terroristic aggression in a climate of uncertainty

    - More spending → less likely to succeed → deterrence

    - But if succeed → signals to the public that it is formidable and deadly, instilling more fear

Main points

- The relationship between government vigilance and deterrence is non-monotonic
- Driven by uncertainty by:
  - government regarding the type of the terrorist
  - terrorist regarding the type of the government
- Implications:
  - improve the precision of the signal
  - Other credible ways of conveying government ability
- Further research: role of *unobservable* counterterror initiatives


END