Exploring Optimization Methodologies for Systematic Identification of Optimal Defense Measures for Mitigating CB Attacks

Roshan Rammohan, Molly McCuskey
Mahmoud Reda Taha, Tim Ross and Frank Gilfeather
University of New Mexico

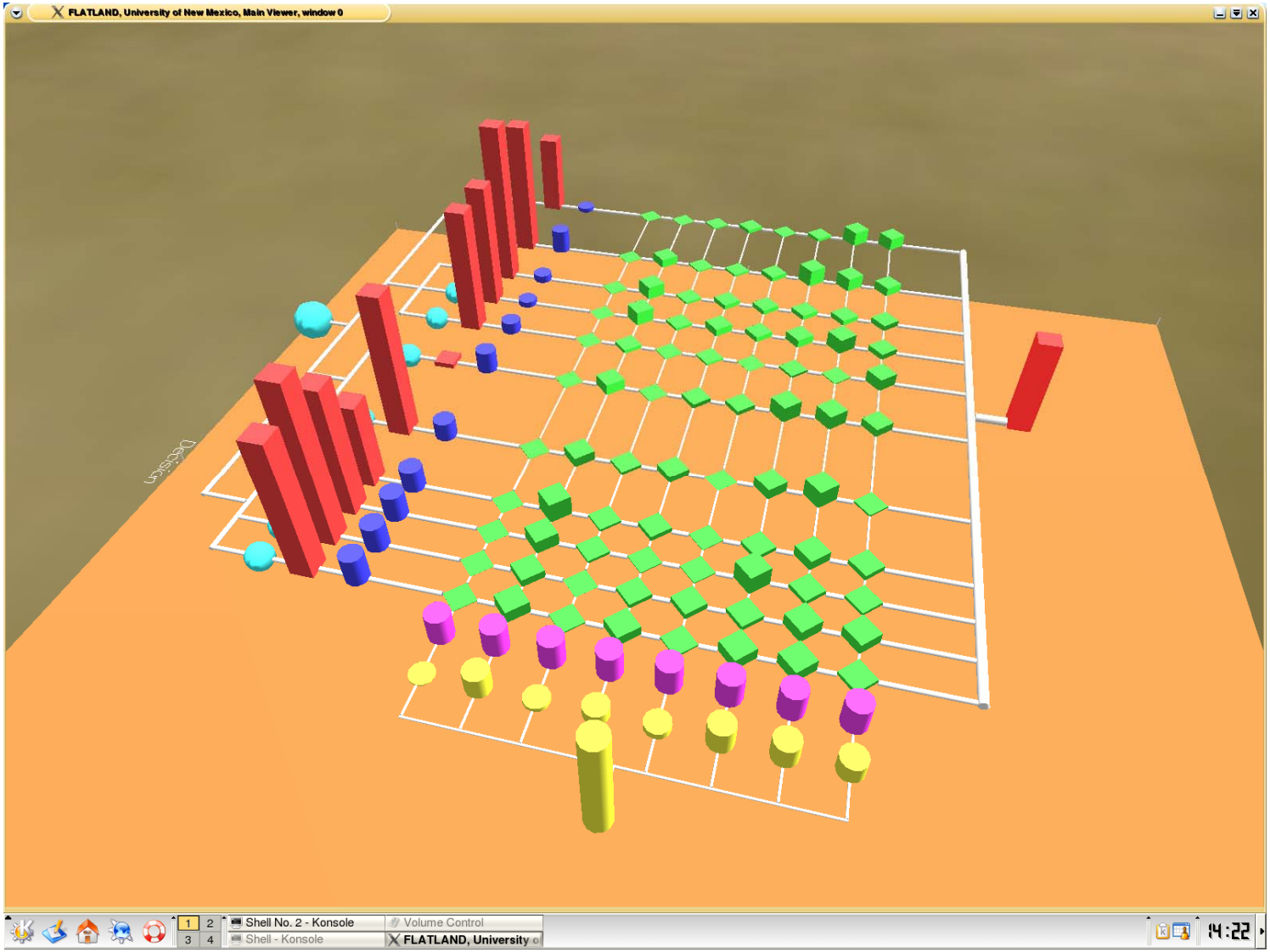
Ram Prasad

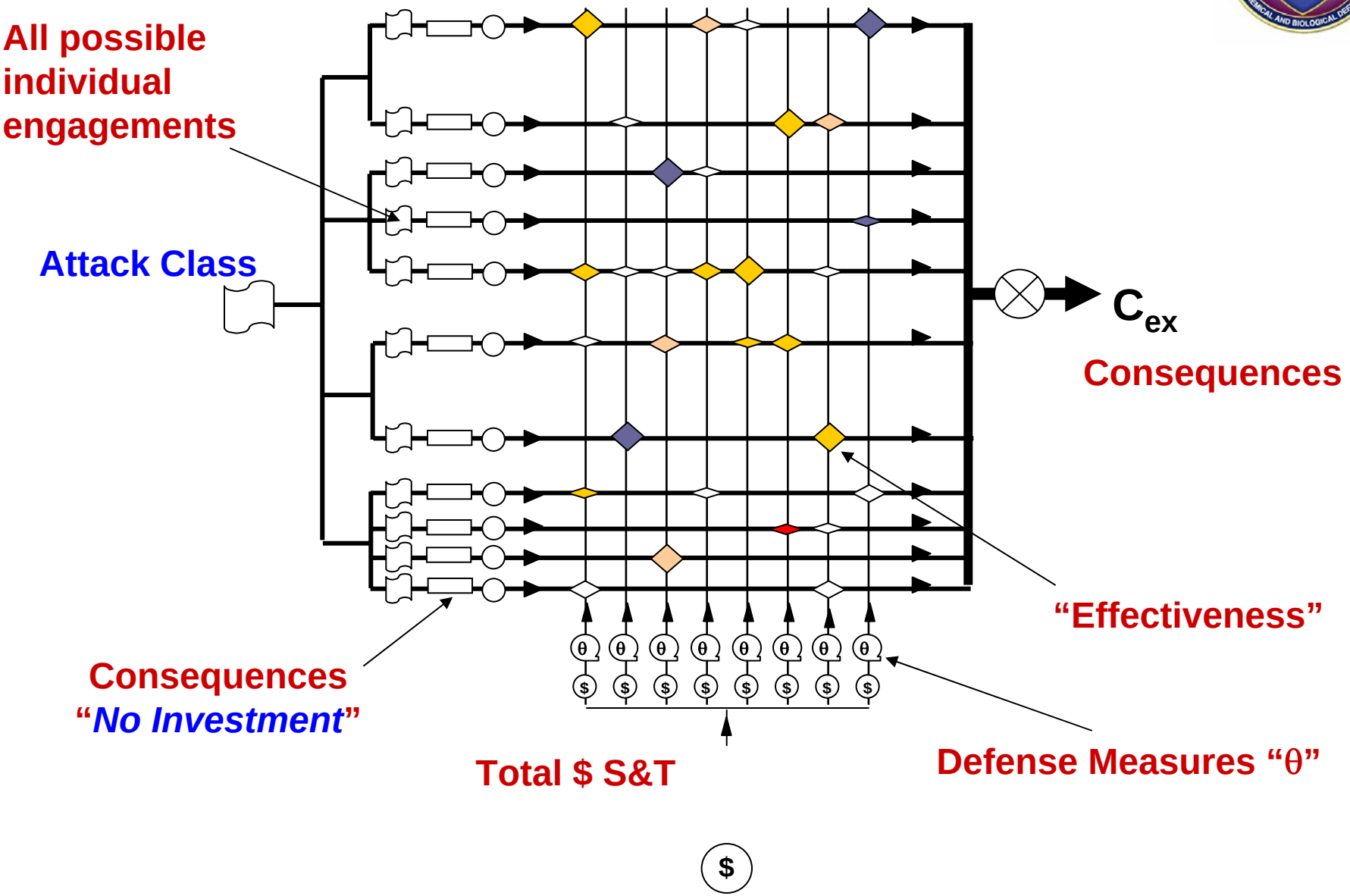
New Mexico State University

Outline

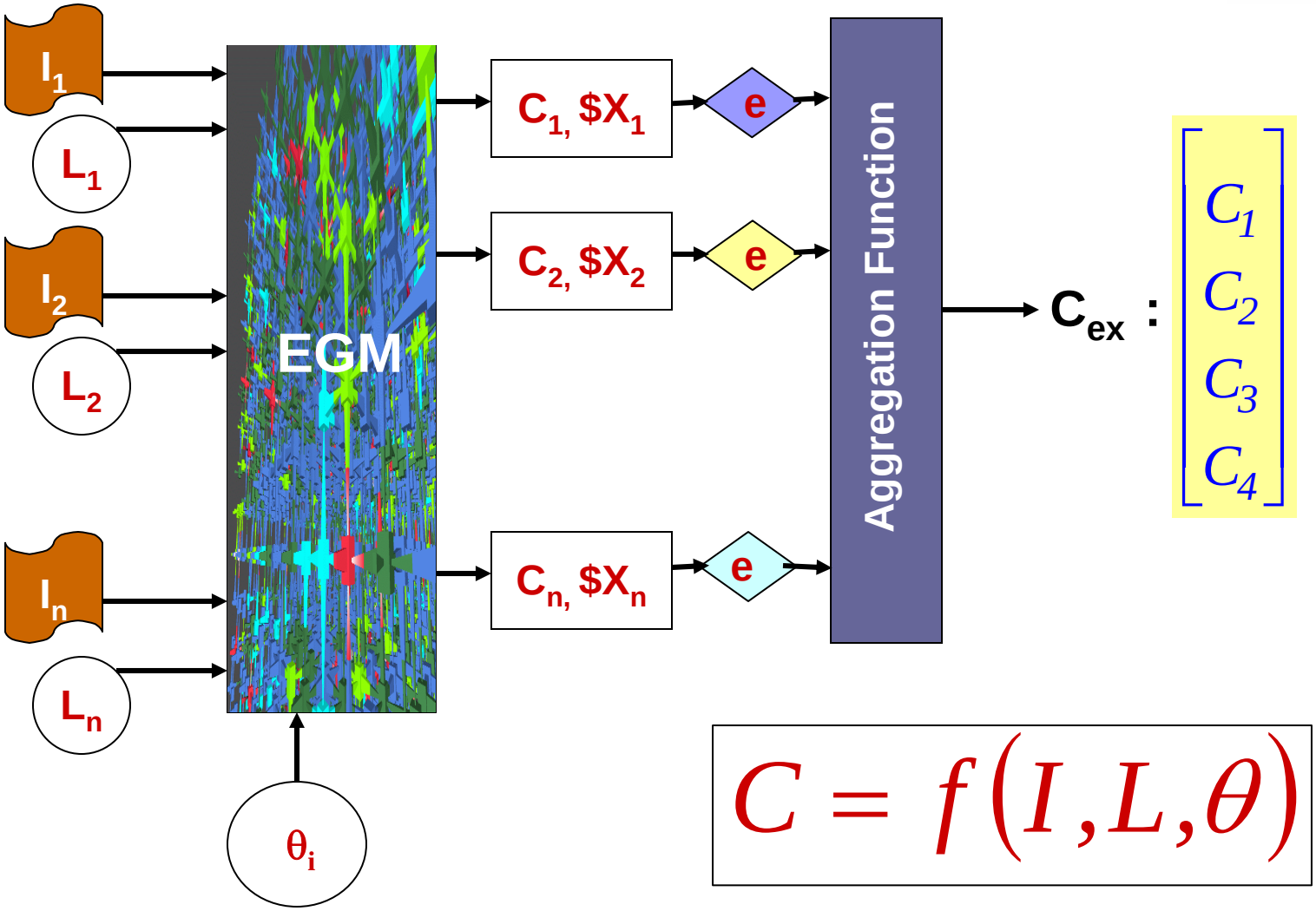
- The general architecture
- How the analytic tool relates to the architecture
- Optimization mode: the problem
- Optimization Techniques With Example Application
- Conclusions

The General architecture




All possible individual engagements
Attack Class
C_{ex}
Consequences
"Effectiveness"
Consequences
"No Investment"
Total $ S&T
Defense Measures "θ"
θ
$

The Analytic Tool "Exploration Mode"



$$C = f(I, L, \theta)$$

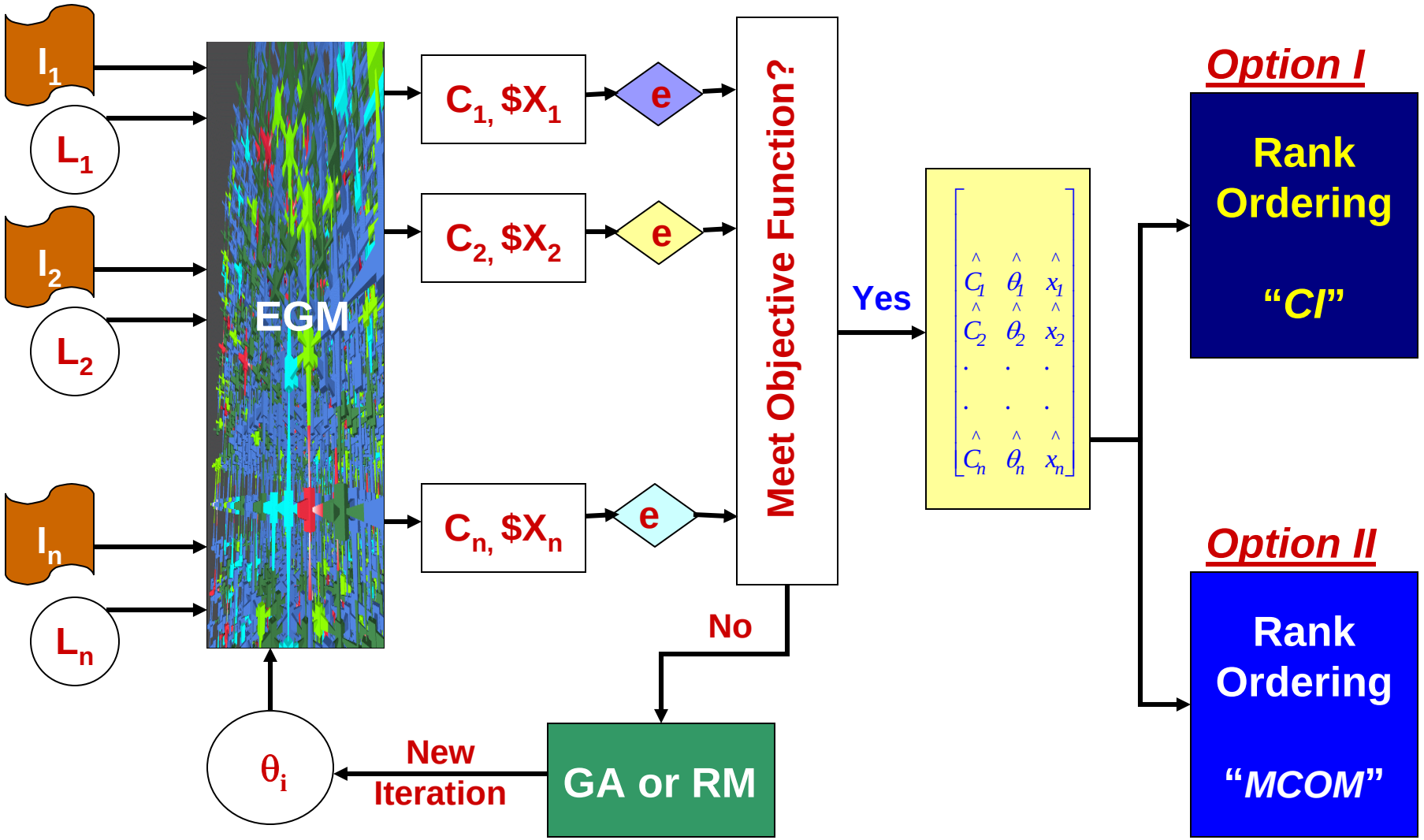
EGM: Engagement Generation Module

The Analytic Tool: "Optimization Mode"

❑ Problem Statement

What is the ***optimal way*** to distribute ***$X*** to ***N (mitigating variables) defense measures*** in order to reduce damage ***(consequences) of a CB attack***?

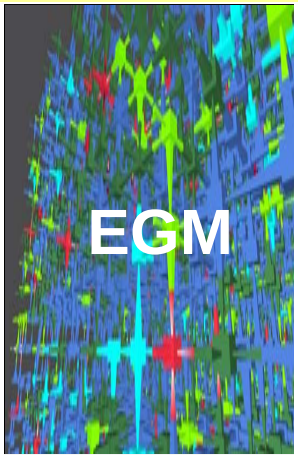
The Analytic Tool: "Optimization Mode"



Analytic Toolbox

- Three main components

Component I:



Component II:

Optimization Module

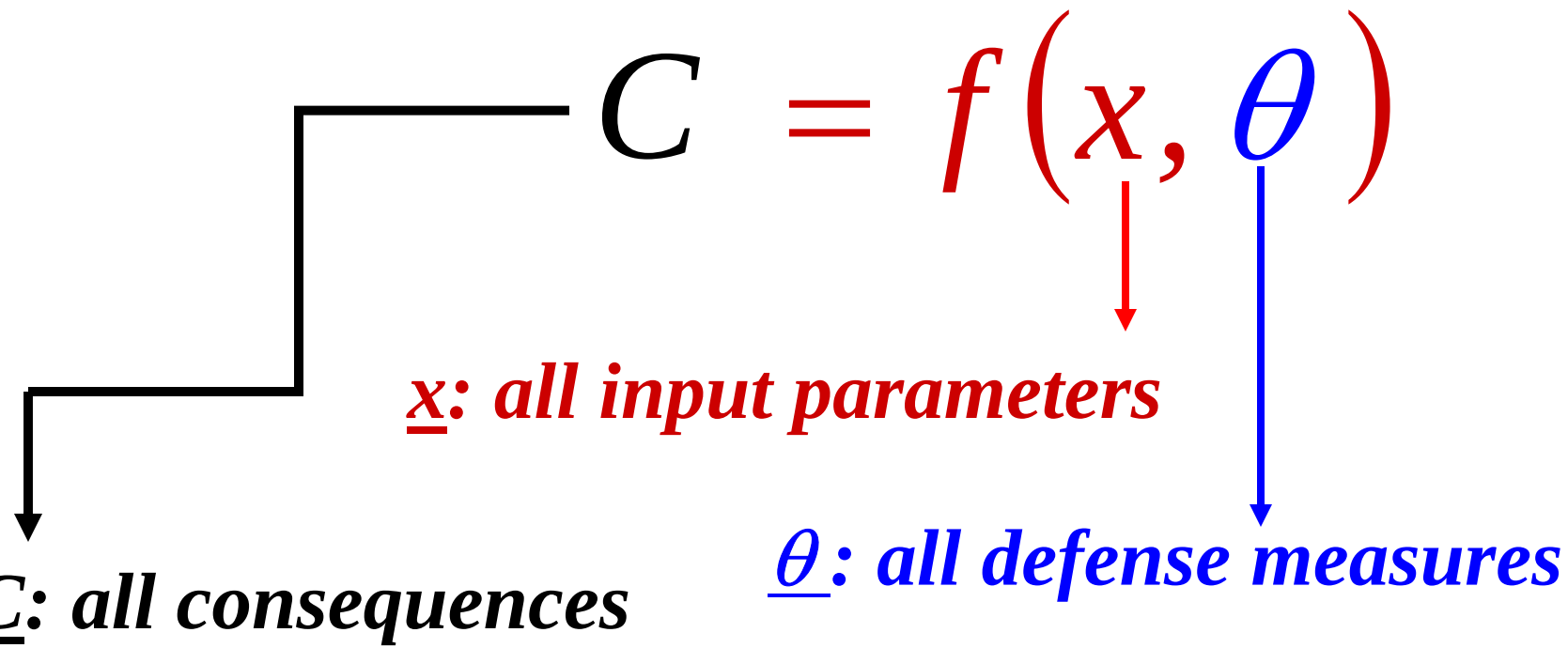
Component III:

Rank Ordering Module

Focus of this talk

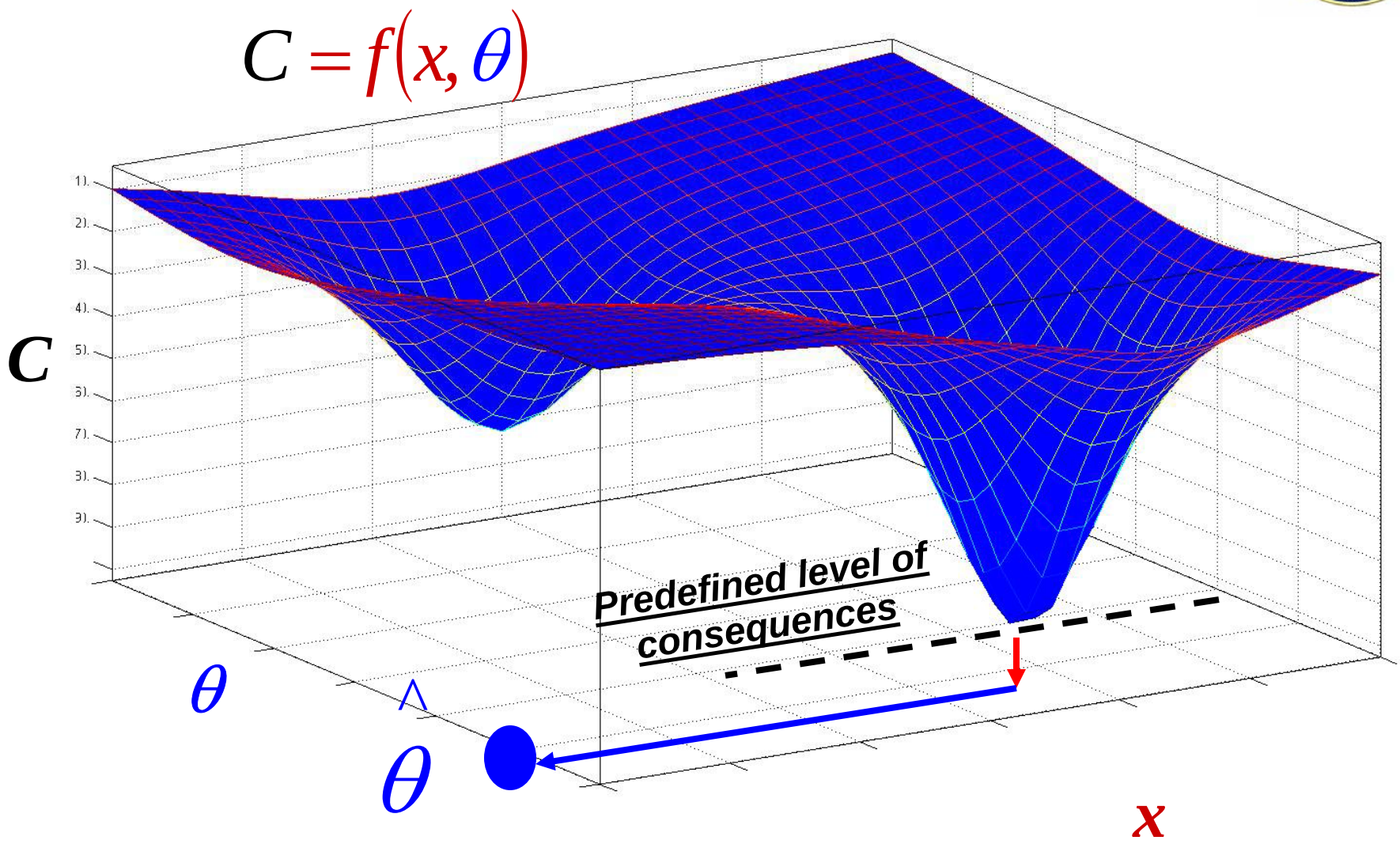
Component II: Optimization Module

Mathematically, we can describe ***the relation*** as



The ***optimization module*** targets finding the optimal ***defense measures*** ($\hat{\theta}$) and their associated ***cost*** ($\$\hat{X}$) that achieves a predefined set of consequences ($\boldsymbol{C_{ex}}$) considering all possible attacking engagementss.

If we have a bimodal surface



The challenge is that the ***function*** that can describe the ***relationship*** between ***CB attack parameters*** (attack target, attacker, etc), the defense measures and the ***attack consequences*** is ***unknown***

When ***the function is unknown***, a well known technique ***is to minimize the error*** (squared error) between the ***desired output*** and the ***model's output***.

predefined consequences

EGM output

$$E(\theta) = \sum_{k=1}^{n} \left(C_{desired} - f(x, \theta) \right)^2$$

Objective function

Two optimization approaches can be used here

Stochastic approximation

-Robbins Munro Optimization (RM)

Search Methods (Derivative free optimization)

- Genetic Algorithms (GA)

- Simulated Annealing (SA)

- The first technique is ***Robbins Munro (RM)*** as a technique to perform ***stochastic optimization***.

-This method is designed to find the roots of ***an unknown function f (θ)*** when the value of ***f(θ)*** can be provided for any specified θ

- ***By replacing f(θ) by its derivative f(θ)'***, the optimal defense measures $\hat{\theta}$ to achieve ***pre-specified consequences (C_0)***can be found.

Capabilities of RM

-Due to the use of a numerical gradient in determining the rate of convergence, this method has ***high ability to adapt to local rates*** of change of the function along its many parameters.

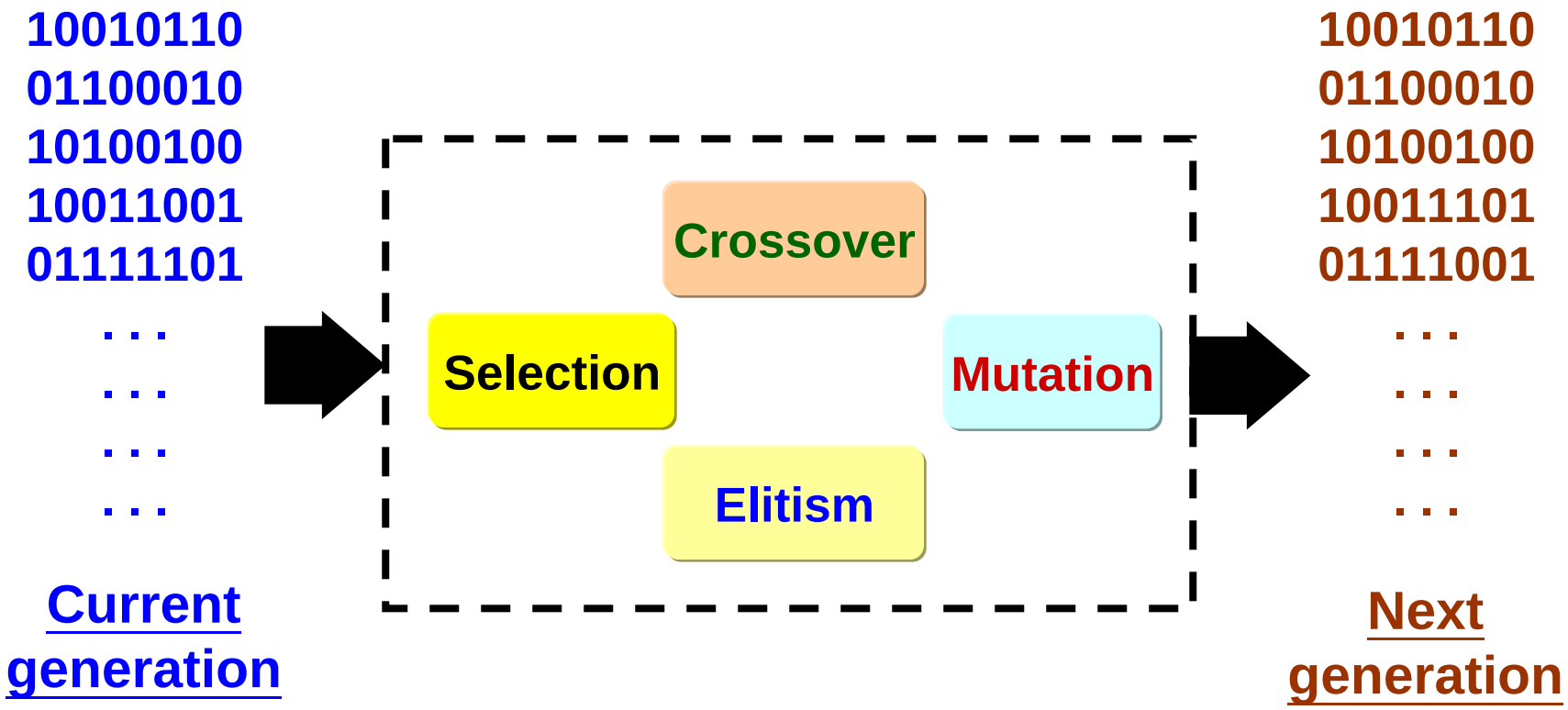
Limitations of RM

- There is an implicit assumption ***about the function being unimodal***.

Genetic Algorithms (GA) mimics laws of ***Natural Evolution*** which emphasizes "***survival of the fittest***".

In GA a "***population***" that contains different possible solutions to the problem is created.

Genetic Algorithms (GA)



The process is repeated until ***evolution happens***

"***a solution is found!***"

Capabilities of GA

- In contrast to traditional techniques, ***GA is the most likely technique to find global peaks*** than traditional techniques.

Limitations of GA

-Unlike traditional optimization methods, ***GA is not the best module for handling continuous variables***

- ***Relative fitness*** depends on probabilistic criteria of the variables that ***might be unknown***.

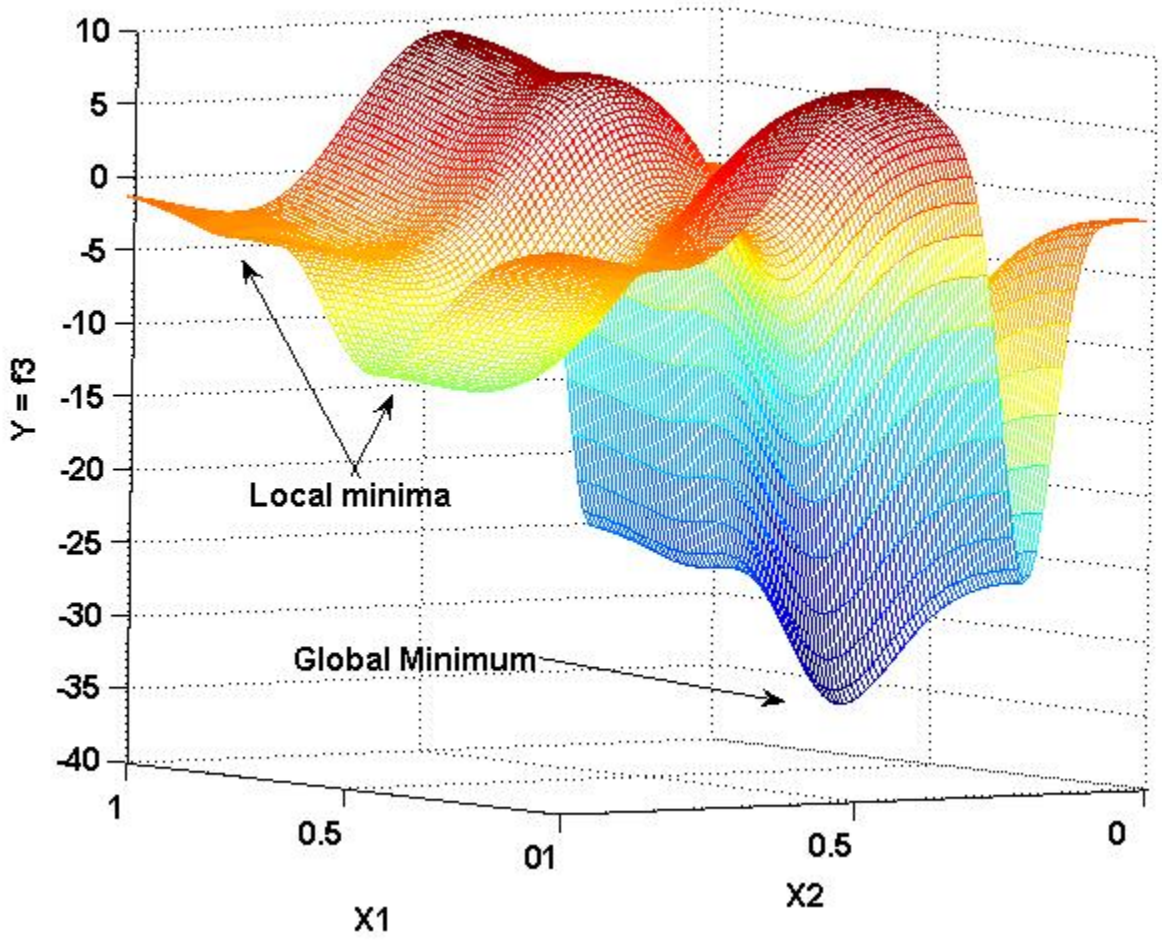
Comparison between GA and RM

-We have conducted a series of ***research experiments*** to compare efficiency of the RM and GA for ***functions*** with ***different levels of complexity.***

- We examined the methods on two, three, four dimensional multivariates.

- We present here example results for optimizing ***a two dimensional multivariate Gaussian functions.***

Comparison between GA and RM



Two dimensional multivariate Gaussian functions

Comparison between GA and RM

Method	Iteration #	x_1	x_2	y	
RM	1st Iteration **1000 iterations**	0.816	0.422	**-12.89**	**LM**
	2nd Iteration **1000 iterations**	0.815	0.753	**-4.71**	**LM**
	3rd Iteration **1000 iterations**	0.198	0.422	**-35.27**	**GM**
GA	1st Iteration **50 generations**	0.198	0.423	**-35.27**	**GM**
	2nd Iteration **50 generations**	0.191	0.440	**-34.84**	**GM**

Comparison between GA and RM

-It became obvious that **RM *is very sensitive to the starting point*** of the search. This is why RM algorithm ***fell in almost all local minima***

- On the contrary, **GA** is ***not sensitive to initial start*** and its temporal performance is better than RM.

- ***However***, it is well known that ***there is no optimal choice for optimization methods***, they are ***problem-dependent*** and thus ***further research is needed***.

Example Application of GA

GA for Optimal Defense Measures Identification

- Here we used the **EGM using ANFIS** ***as the relation model*** and ***examined*** using ***GA*** to ***identify the optimal defense measures*** ($\hat{\theta}$) for a given attack engagements.

- We operated the DS tool in
  - ***Exploration mode to validate EGM***
  - ***Optimization model to examine GA***

Exploration Mode

Engagement Description

CB attack on a U.S. Air force in the Persian Gulf

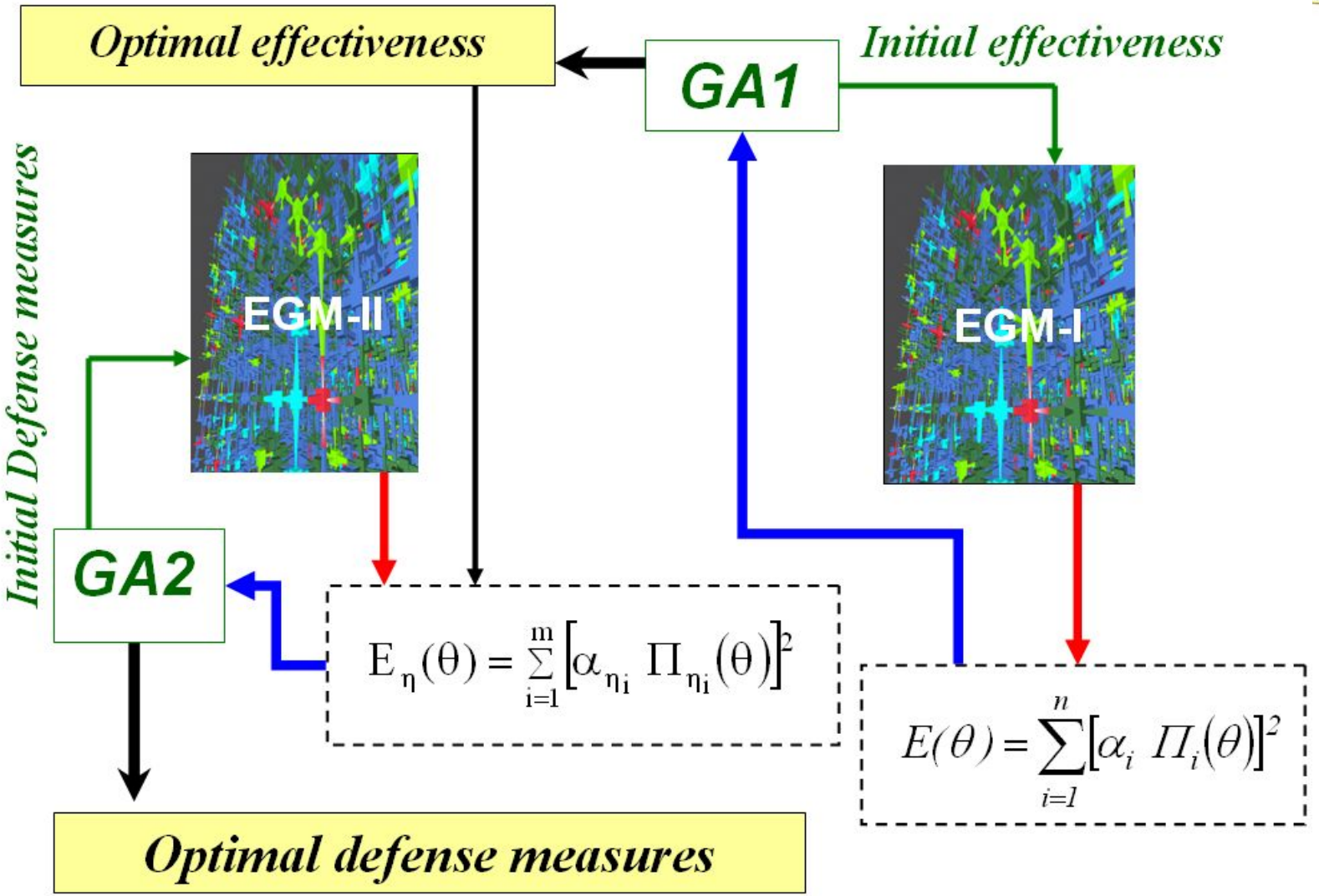
- ***Preparator***: Hostile foreign state
- ***Motivation***: Interrupt Strategic functions
- ***Military facilities***: Flight operation and support
- ***Chemical/Biological agent***: Vx
- ***Dispersal mechanism***: Missile warhead: Cluster
- ***Point of Release***: 2km SE of personnel area
- ***Other characteristics…..***

Exploration Mode

Consequences		Var 1	Var 2	Var 3
Casualties	Expected	150-350	150-250	150-250
	Model	**377**	**263**	**346**
Cost (US $ M)	Expected	70	65	60
	Model	**72**	**57**	**65**
Days of Int.	Expected	7	5	5
	Model	**7**	**5**	**5**

- EGM sensitivity to defense measures was examined.

Two stage GA


Optimal effectiveness
GA1
Initial effectiveness
Initial Defense measures
EGM-II
EGM-I
GA2
$E_\eta(\theta) = \sum_{i=1}^{m} [\alpha_{\eta_i} \Pi_{\eta_i}(\theta)]^2$
$E(\theta) = \sum_{i=1}^{n} [\alpha_i \Pi_i(\theta)]^2$
Optimal defense measures

Optimization Mode

- Predefined consequences include

Predefined level of Consequences	
Casualties	**430**
Remediation Cost $M	**70**
Days of Int.	**7**
Cost of Add. S&T $M	**170**

Optimization Results

The output of the ***optimization module*** was 250 ***possible combinations of defense measures*** that will

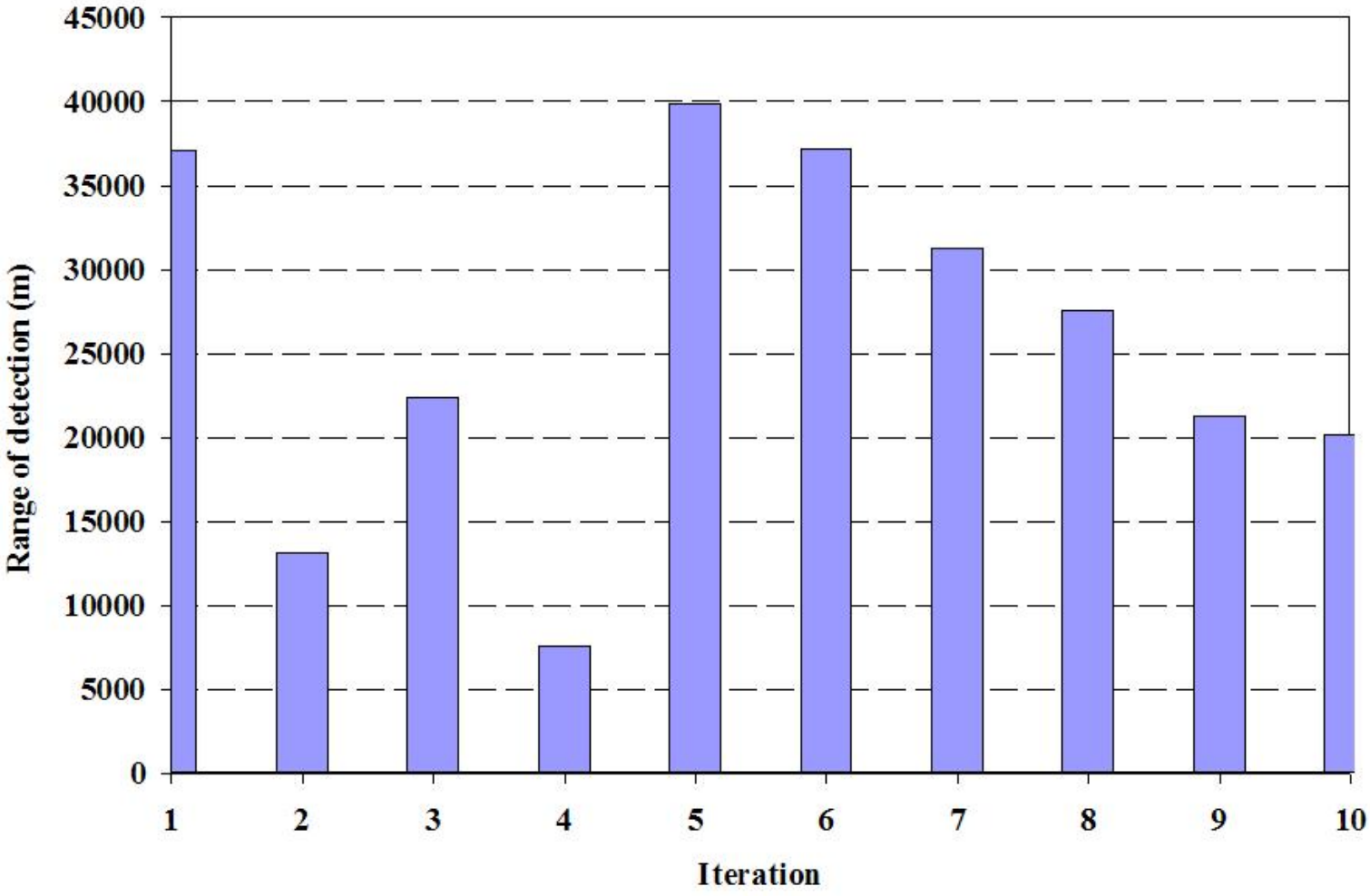
- Achieve a level of minimum ***consequences***

- Limit the ***S&T*** dollars to the total available fund

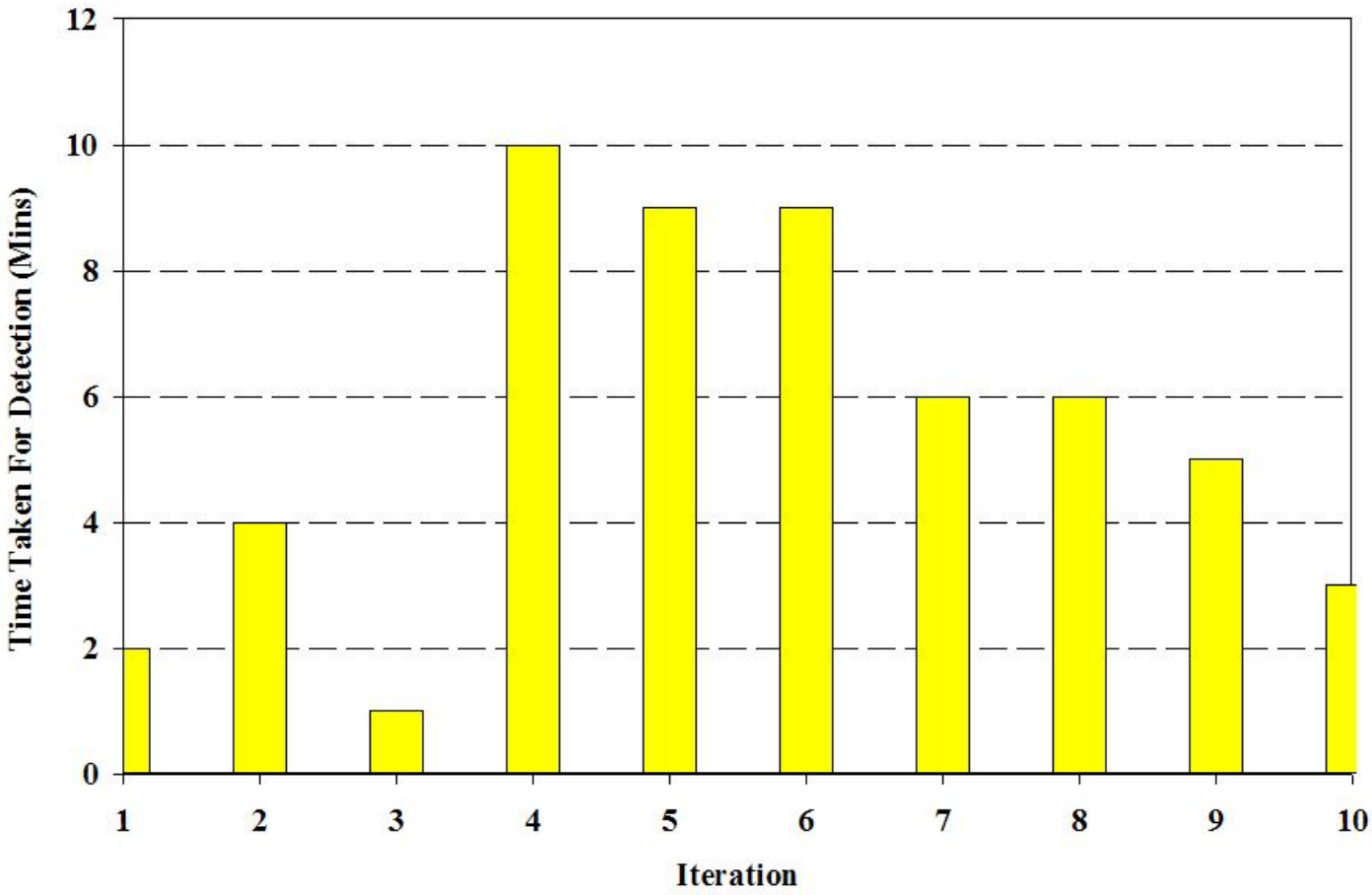
The question becomes

Which solution to choose?

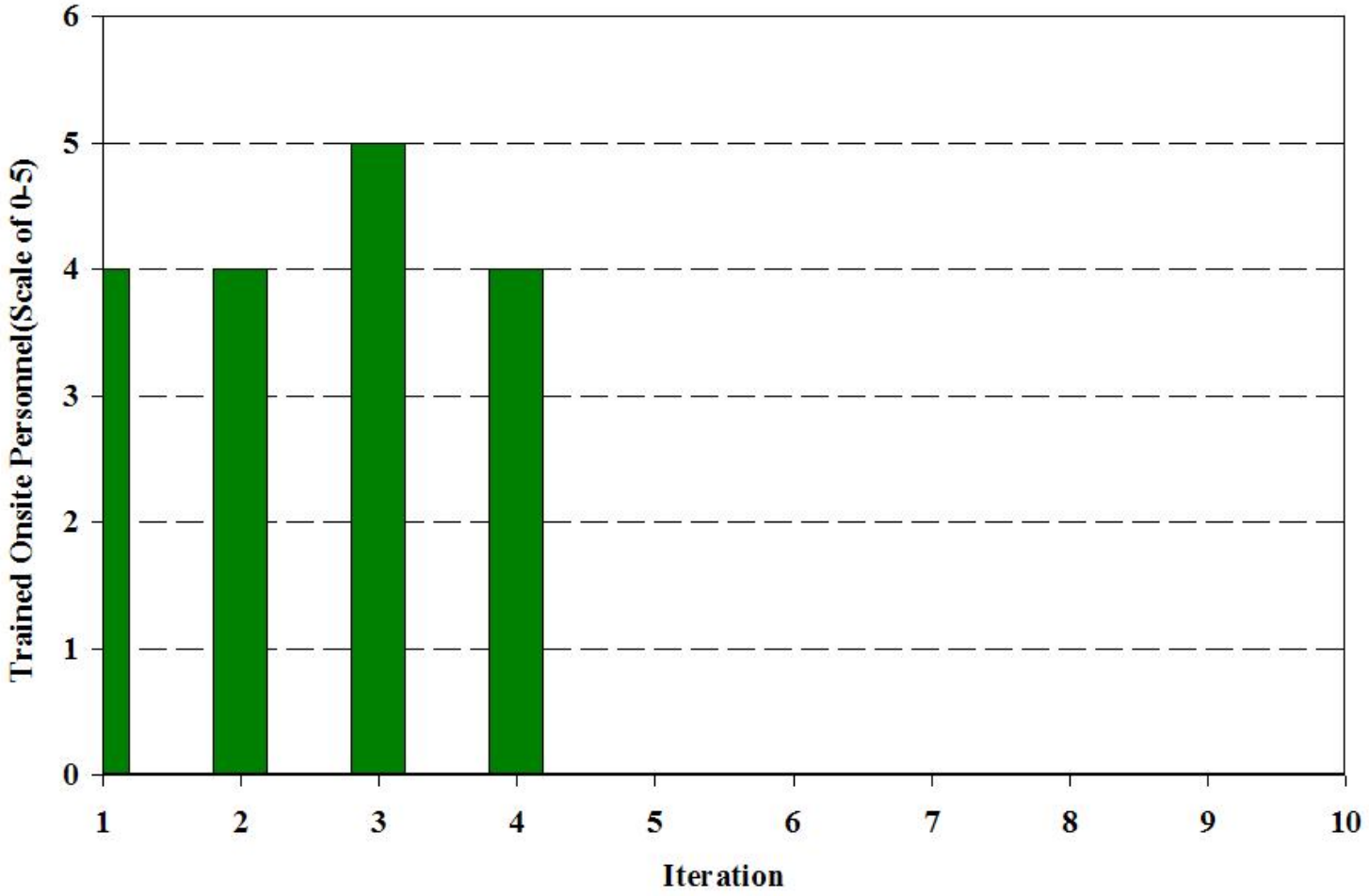
Possible solutions



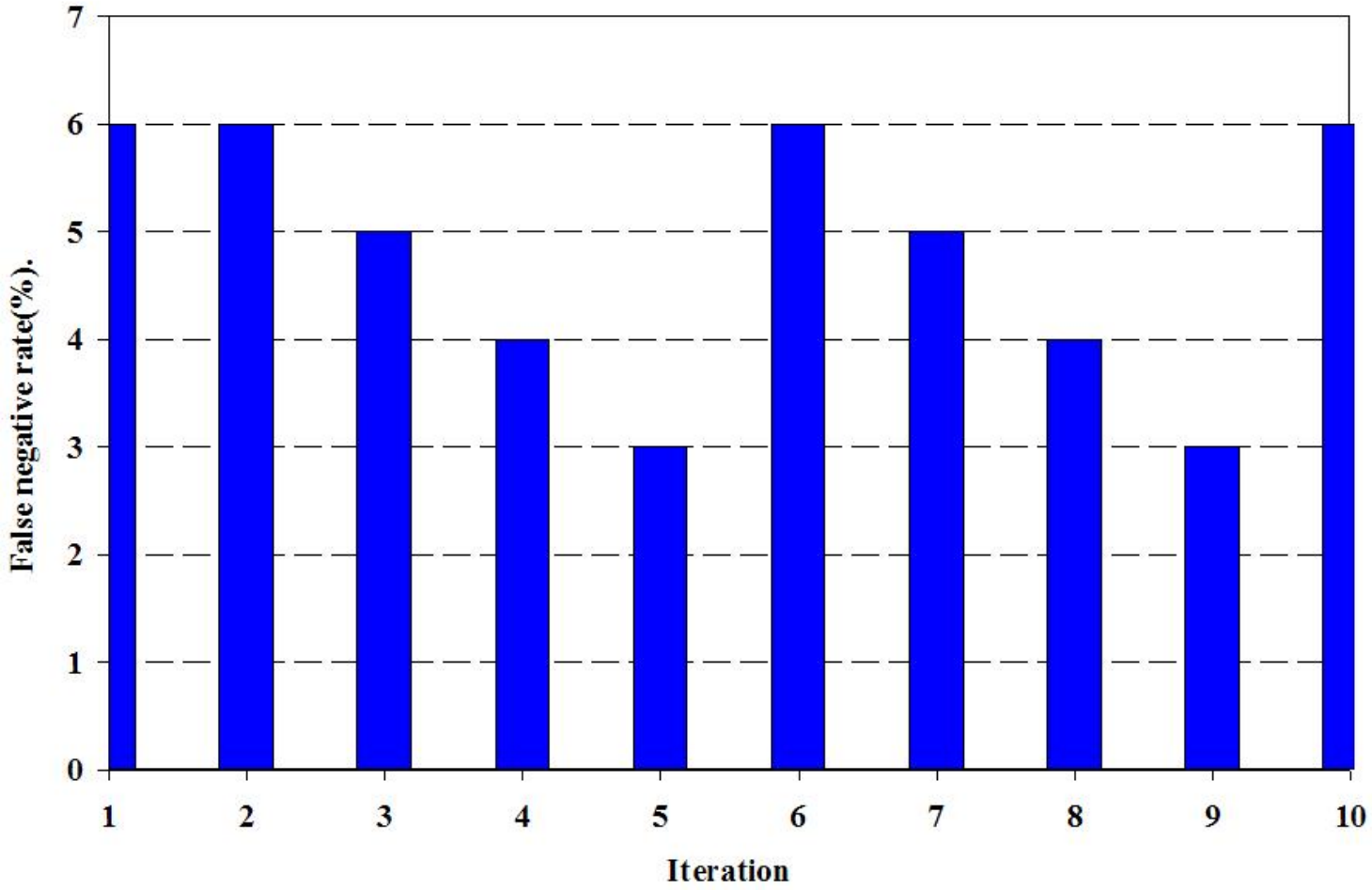
Possible solutions



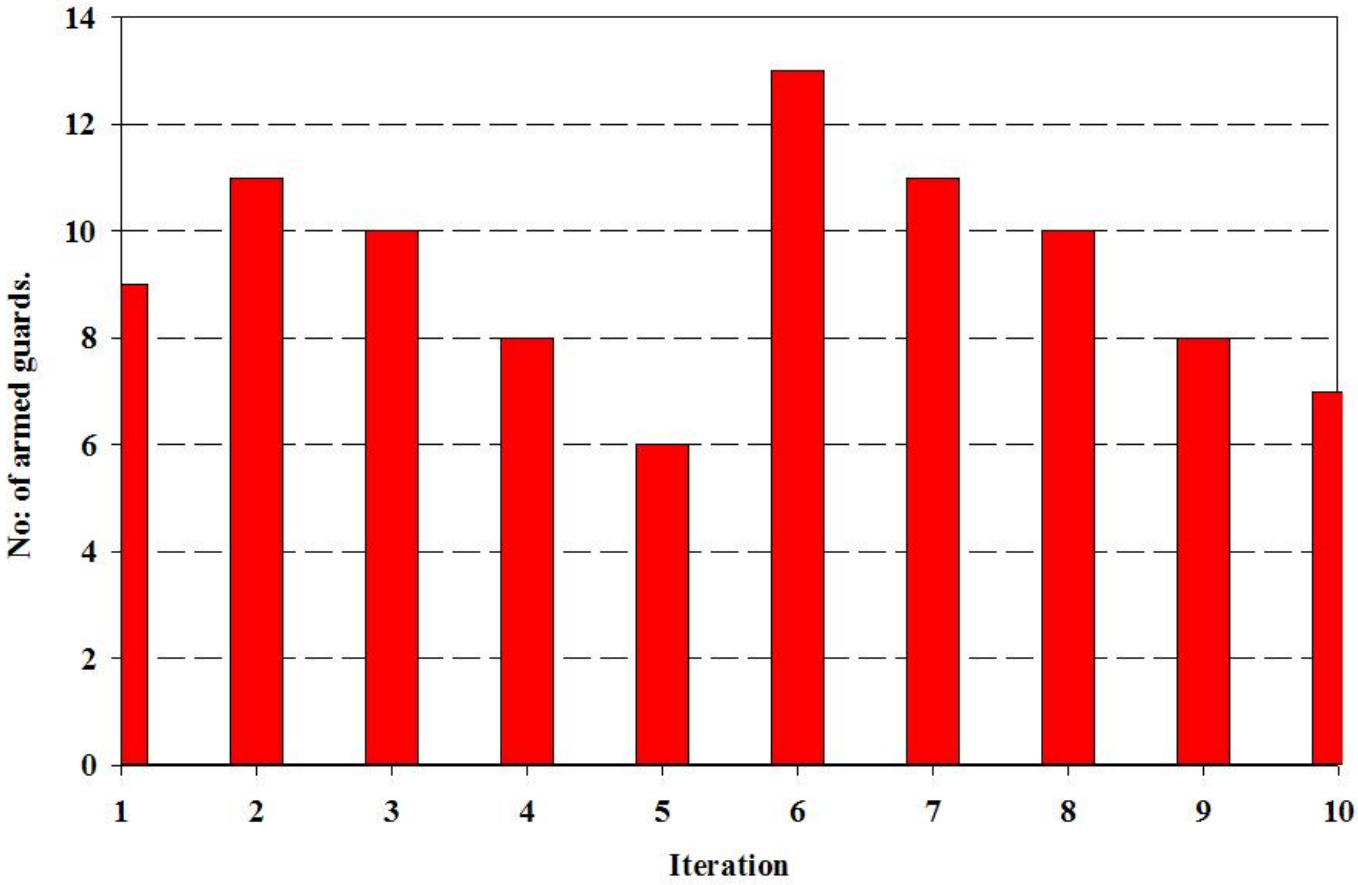
Possible solutions



Possible solutions



Possible solutions



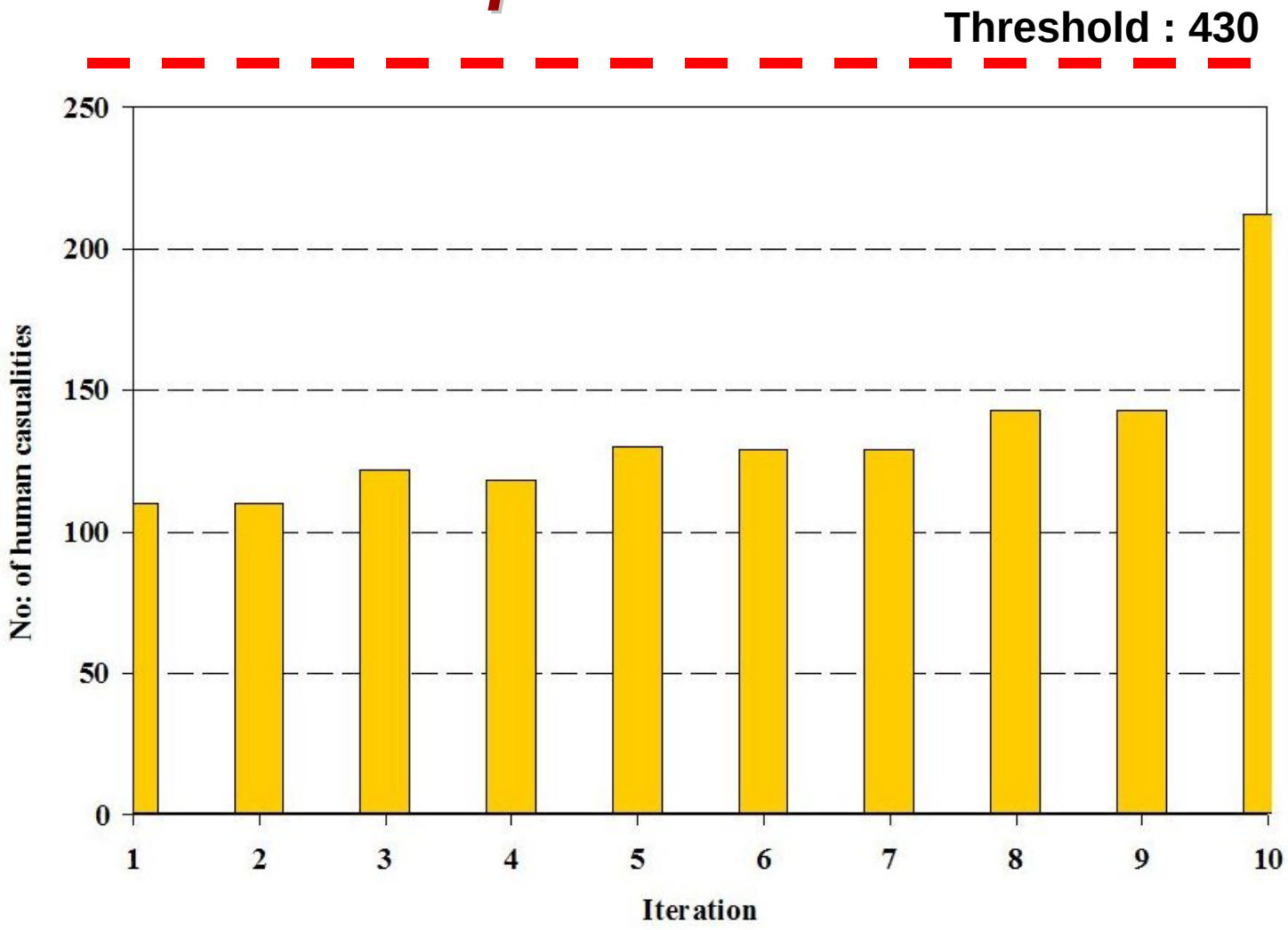
Rank ordering

In our problem, ***ranking criteria are interactive***. In such a situation, ***it is proved in decision theory that nonlinear aggregation operators are more efficient***.

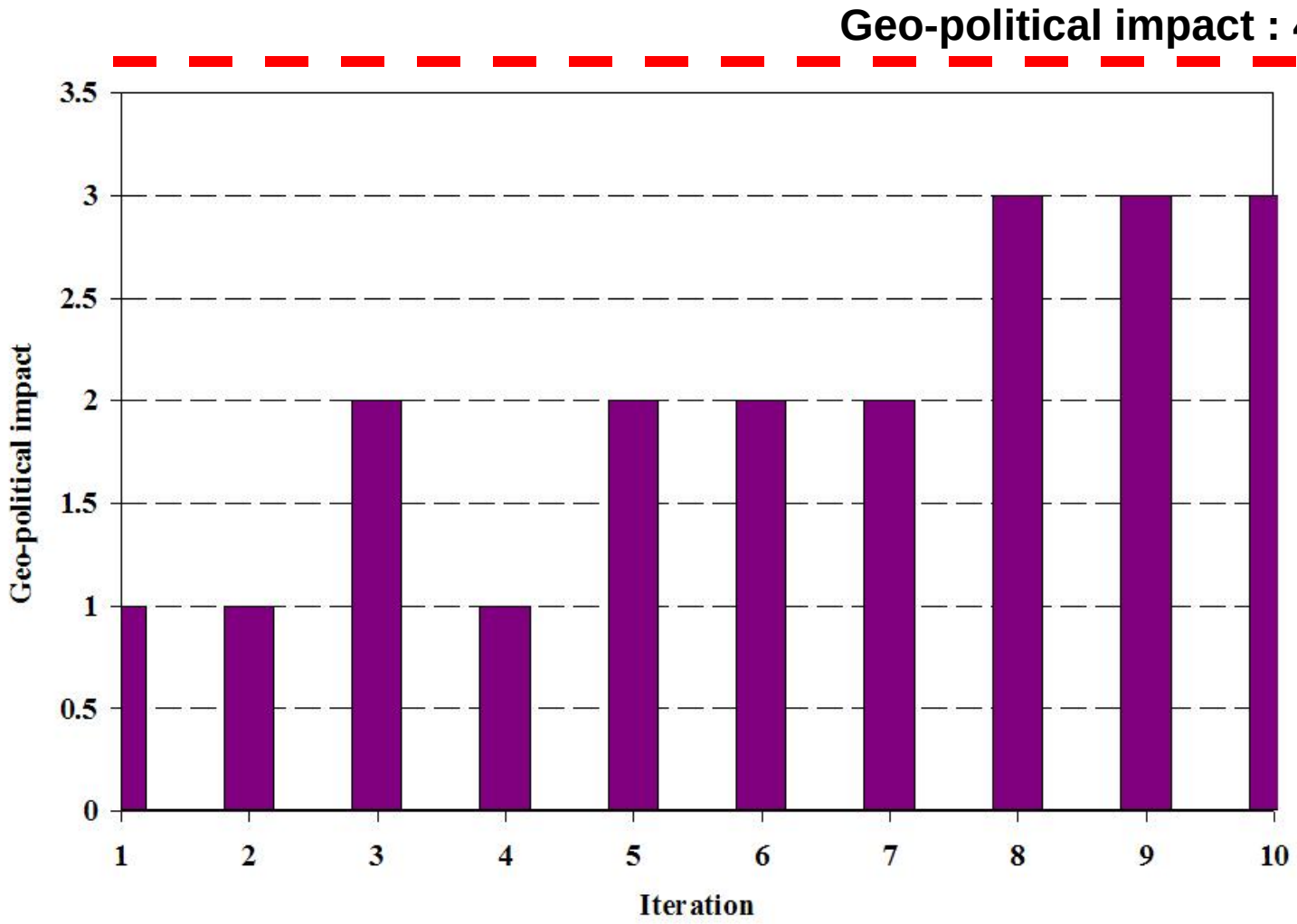
A few possible techniques

- ***Choquet Integral (CI)***
- ***Multi criteria decision making (MCDM)***

Consequences If optimal defense measures are implemented



Consequences If optimal defense measures are implemented



Conclusions

-We demonstrated the possible use of derivative-free optimization as an efficient system for optimization for finding the optimal S&T investments to minimize the consequences of CB attacks

-A two step optimization using GA proved more efficient than a one-stage optimization methods in performing the analysis

- The optimization tool showed good accuracy in finding the optimal defense measures to minimize consequences due to CB attacks

- Research is currently on-going to integrate this method with rank ordering module.

Acknowledgment

This research is funded by Defense Threat Reduction Agency (DTRA).

The authors gratefully acknowledge this funding.

Questions