ALSCRM

An Automated method for Large Scale Comprehensive Risk Management of cyber-security

Background

- **Our Goal:** to build tools and metrics to assist cyber decision-making.
- An attempt to overview the problem in a systematic way.

"He who defends everything defends nothing"

Fredrick the great, 1779

"A chain is only as strong as its weakest link"

-Thomas Reed, 1786

The "classic" approach to cyber-security is insufficient

- The classic approach: "Closing all the gaps"
  - The field emerged bottom up from the world of "tech' breaches";
  - The language used is usually very low-level and technical, and sometimes very high-level (actors etc.);
  - The focus is on the "new and exciting", without general context;
  - Defenders end up constantly chasing the most recent events.

- The dangers of this approach:
  - Missing the relative importance of different issues;
  - Difficulty assessing comprehensive vulnerability unbiasedly ;
  - Sub-optimal resource allocation;
  - Difficulty translating between strategy and practical steps;
  - A gap between connecting regulation to actual benefit.

ى

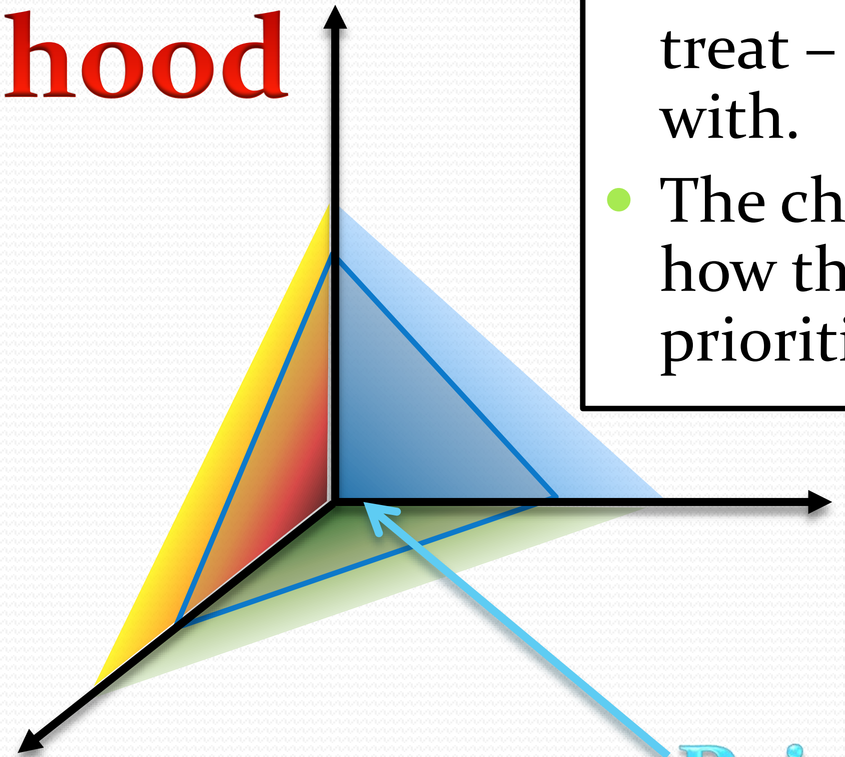
The approach here: ALSCRM

An Automated method for Large Scale Comprehensive Risk Management

- The use of a mid-level language of Attack Stories
- This approach benefits by giving the abilities to:
  - Translate high-level strategy into detailed practical steps;
  - Look at all the data in an organized fashion;
  - Focus resources to main weak points;

Prioritizing the threats

- The threats that are likelier, more severe and cheaper to treat – are the first to deal with.
- The challenge is determining how the threats should be prioritized.



Likelihood

Severity

Treatment Cost

Prioritized threat

Attack Stories (AS)

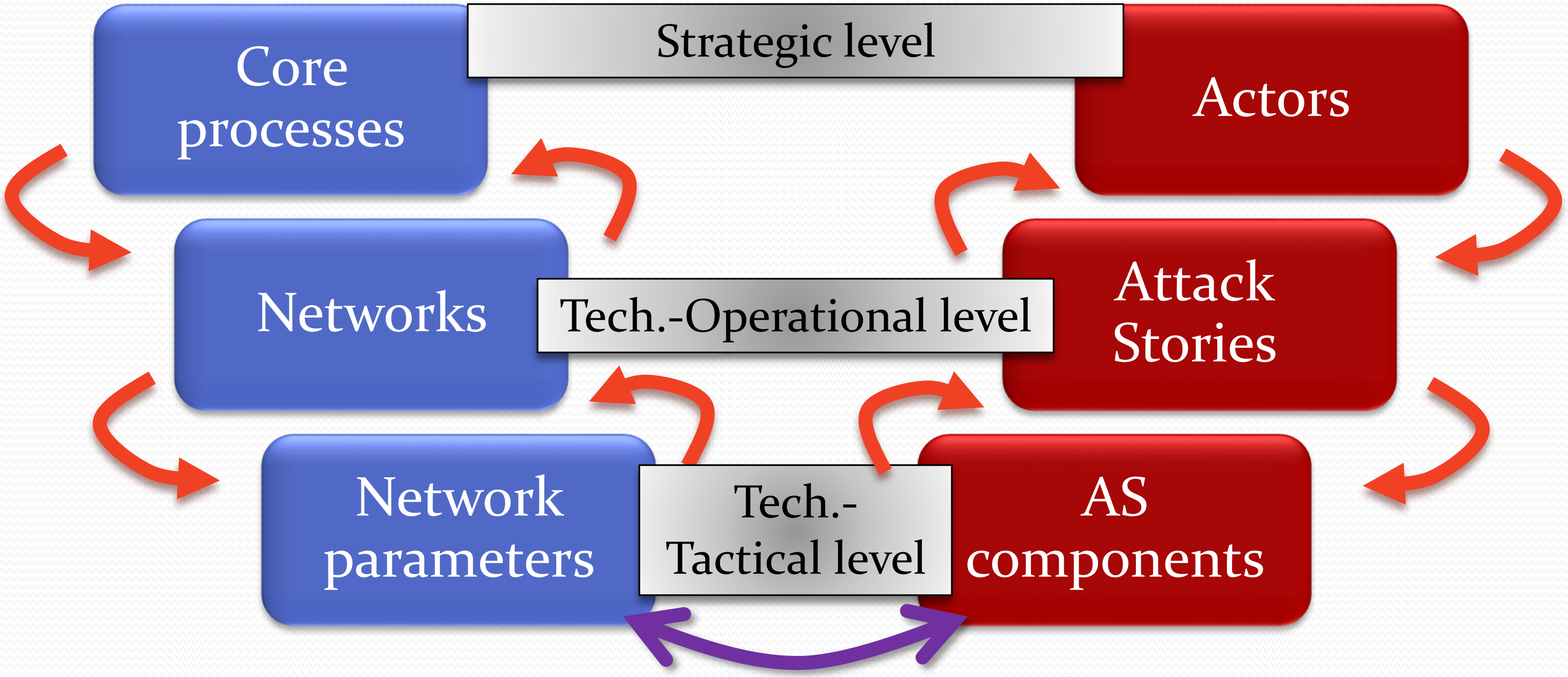
- A useful definition of the cyber threats needs to address the **strategic level** (actors and capabilities) an the **technical level** (actions in a network)
- Therefore we defined the "attack story" – a full description of an attack, in a high level, yet technical, language.

Example: "***Access*** ***to the network via SpearPhising insertion,*** ***Spread*** ***via Automated non-targeted MW with zerodays, for the*** ***Effect*** ***of "Loud" Network disruptions***".

- Each attack story involves malware, and the stages of an attack:
  - ***Access ➔ Spread ➔ Effect***

The multiple layers of interest

Example: "***Access*** *to the network via SpearPhising insertion,* ***Spread*** *via Automated non-targeted MW with zerodays, for the* ***Effect*** *of "Loud" Network disruptions".*



Core processes

Strategic level

Actors

Networks

Tech.-Operational level

Attack Stories

Network parameters

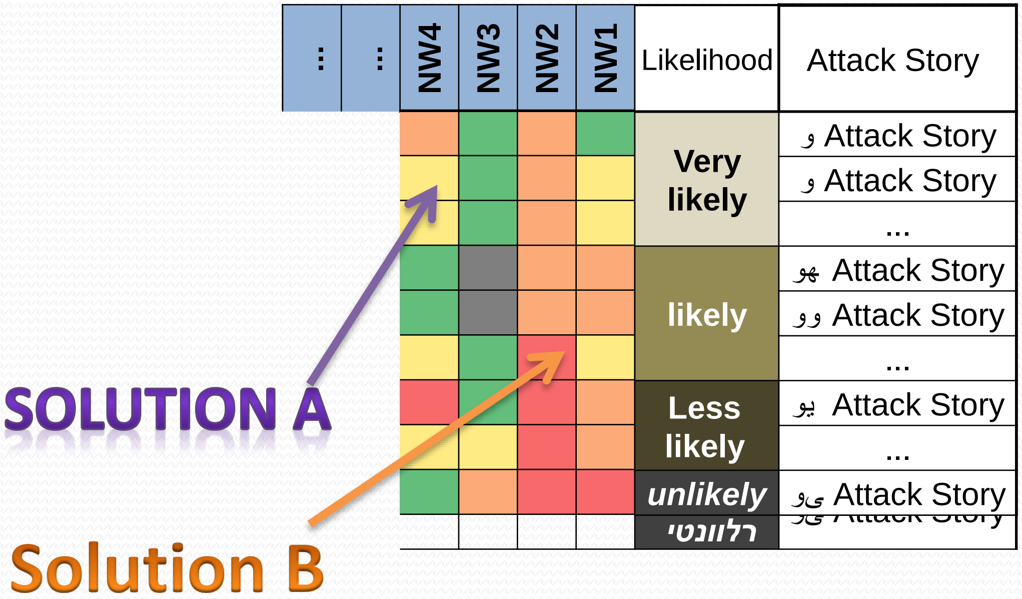
Tech.-Tactical level

AS components

Full specs

Specific malware

Process Overview

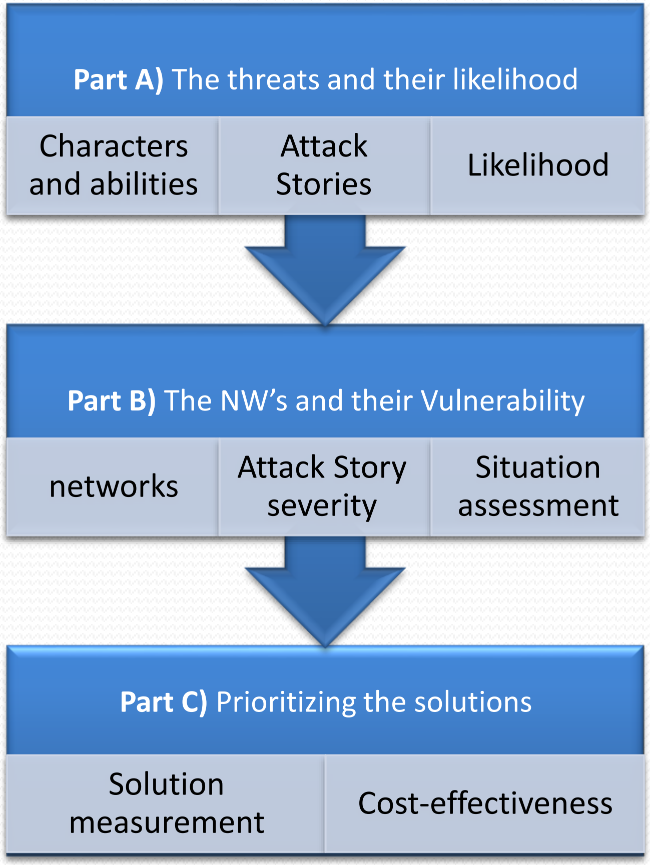


…	…	NW4	NW3	NW2	NW1	Likelihood	Attack Story
		🟧	🟩	🟧	🟩	**Very likely**	و Attack Story
		🟨	🟩	🟧	🟨		و Attack Story
		🟨	🟩	🟧	🟨		…
		🟩	⬛	🟧	🟧	**likely**	هو Attack Story
		🟩	⬛	🟧	🟧		وو Attack Story
		🟨	🟩	🟥	🟨		…
		🟥	🟩	🟥	🟧	**Less likely**	يو Attack Story
		🟨	🟨	🟥	🟧		…
		🟩	🟧	🟥	🟥	***unlikely***	ىو Attack Story
						רלוונטי	ىو Attack Story

SOLUTION A

Solution B

Light damage	🟩
Medium damage	🟨
Severe damage	🟧
Very Severe damage	🟥



Part A) The threats and their likelihood

Characters and abilities | Attack Stories | Likelihood

Part B) The NW's and their Vulnerability

networks | Attack Story severity | Situation assessment

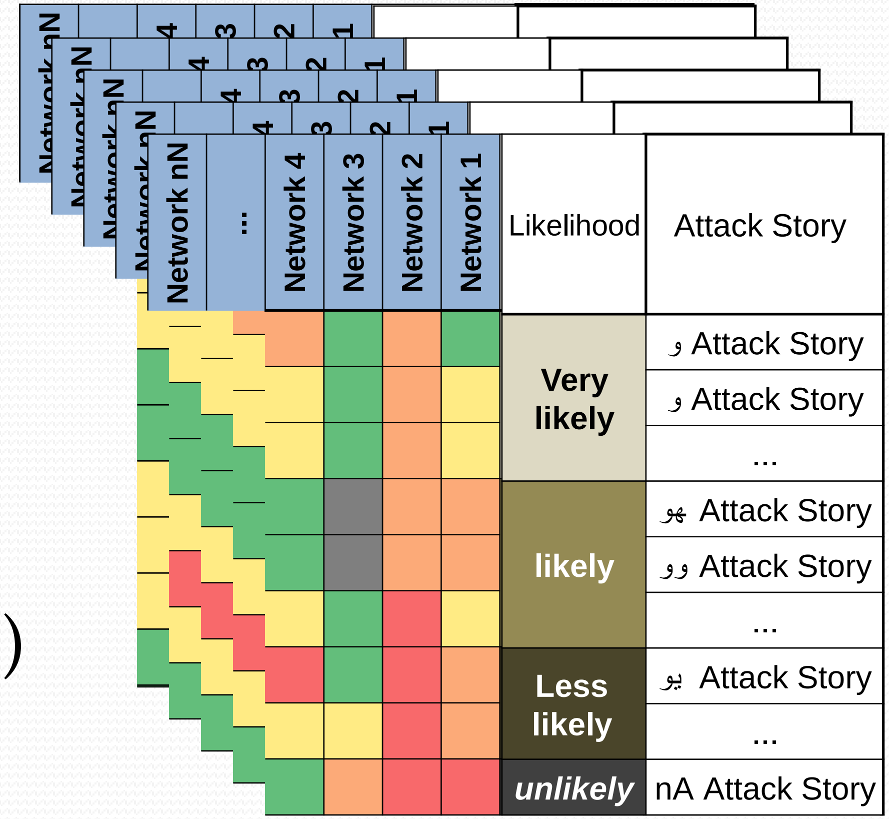
Part C) Prioritizing the solutions

Solution measurement | Cost-effectiveness

combinatrics

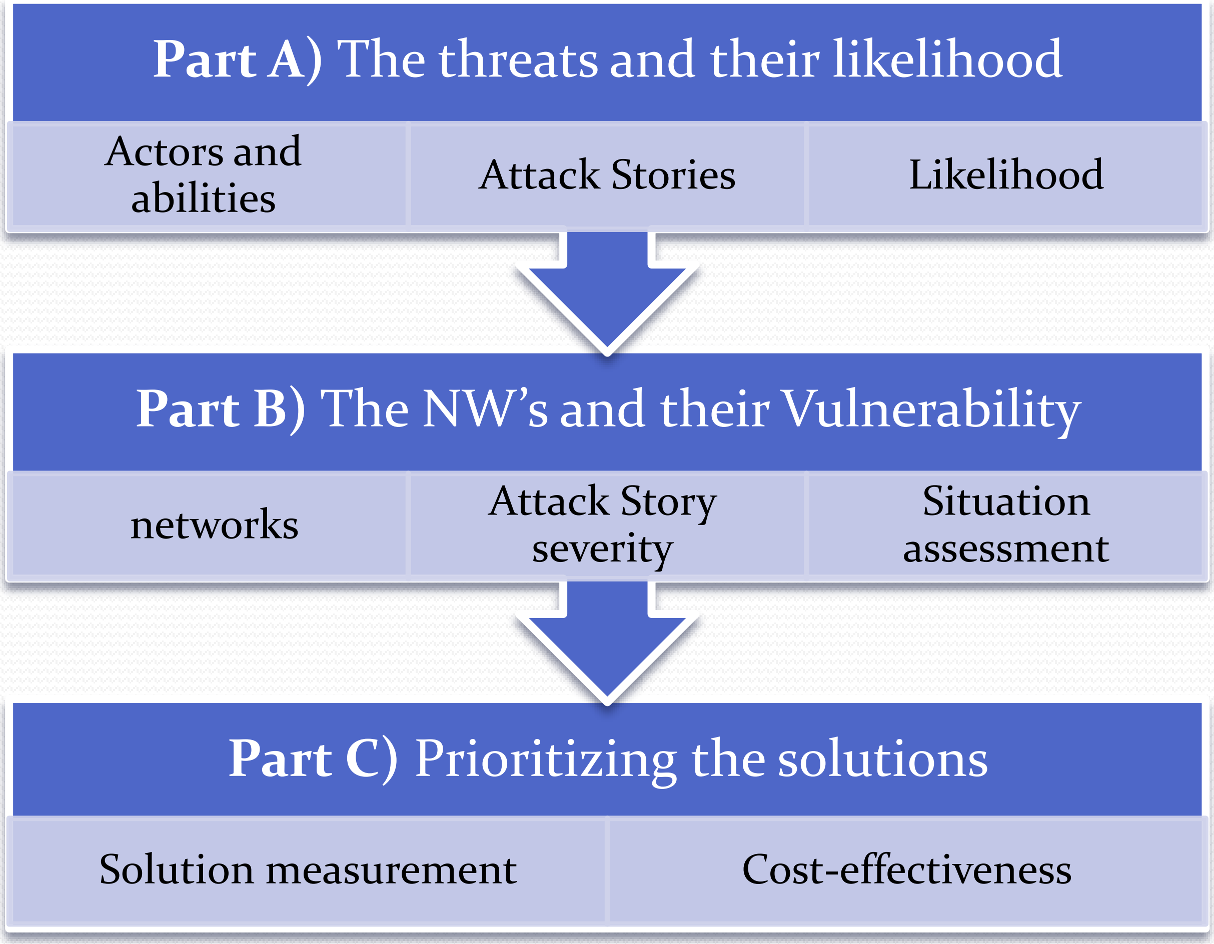
- nA - attack stories
- nN - networks
- nS - solutions

- Combinations: nA*nN*(nS!)



Network nN	...	Network 4	Network 3	Network 2	Network 1	Likelihood	Attack Story
		🟧	🟩	🟧	🟩	**Very likely**	و Attack Story
		🟨	🟩	🟧	🟨		و Attack Story
		🟨	🟩	🟧	🟨		...
		🟩	▨	🟧	🟧	**likely**	هو Attack Story
		🟩	▨	🟧	🟧		وو Attack Story
		🟨	🟩	🟥	🟨		...
		🟥	🟩	🟥	🟧	**Less likely**	يو Attack Story
		🟨	🟨	🟥	🟧		...
		🟩	🟧	🟥	🟥	***unlikely***	nA Attack Story

Table of contents



Part A) The threats and their likelihood

Actors and abilities

Attack Stories

Likelihood

Part B) The NW’s and their Vulnerability

networks

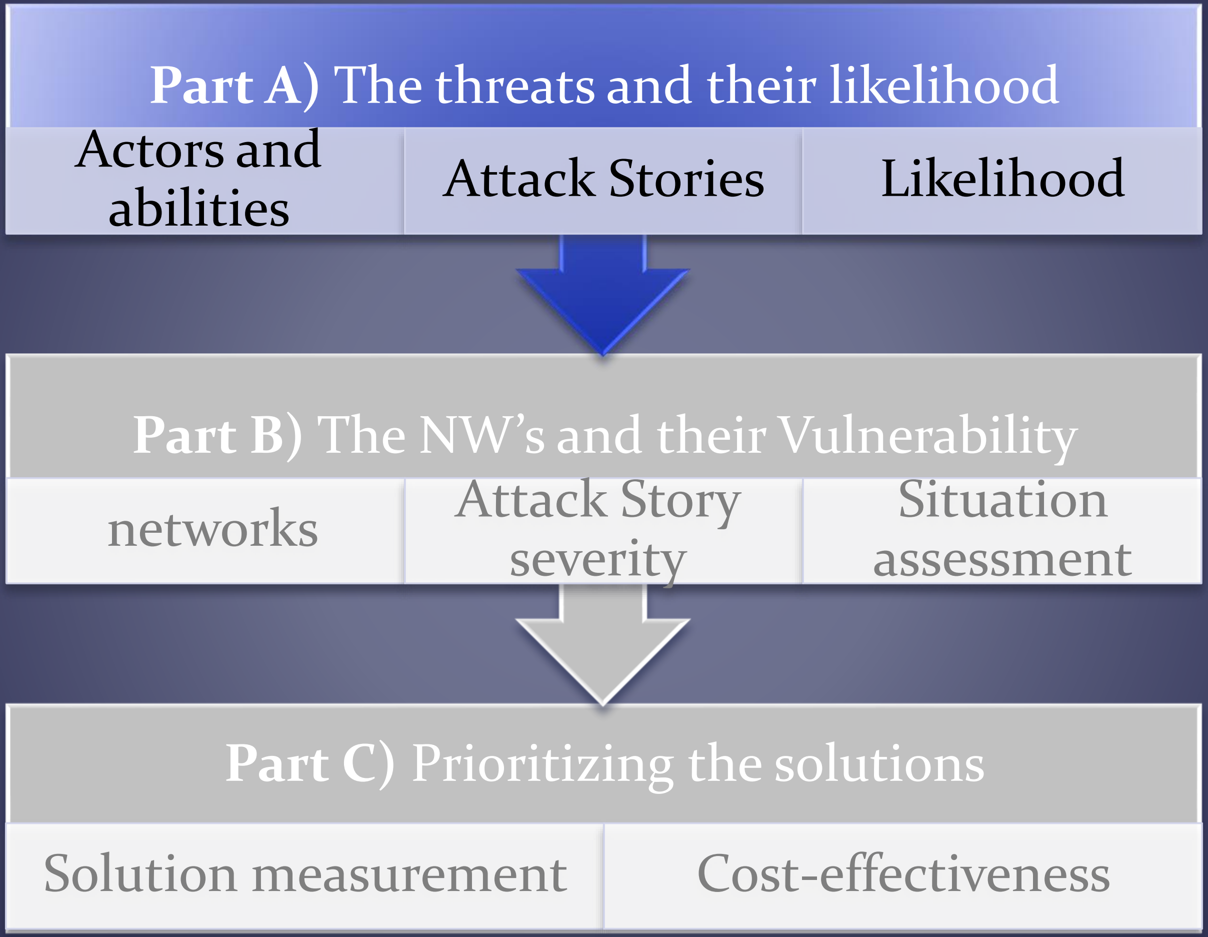
Attack Story severity

Situation assessment

Part C) Prioritizing the solutions

Solution measurement

Cost-effectiveness



Part A) The threats and their likelihood

Actors and abilities

Attack Stories

Likelihood

Part B) The NW's and their Vulnerability

networks

Attack Story severity

Situation assessment

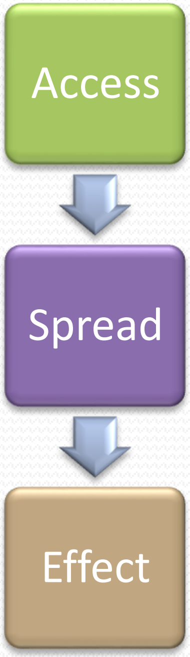
Part C) Prioritizing the solutions

Solution measurement

Cost-effectiveness

Attack Story components

Phase
Access
Access #1
Access #2
Access #3
Access #4
Access #5
Spread
Spread #1
Spread #2
Spread #3
Spread #4
Effect
Effect #1
Effect #2
Effect #3
Effect #4


Access

Spread

Effect

Attack Story components

*RANDOM DATA

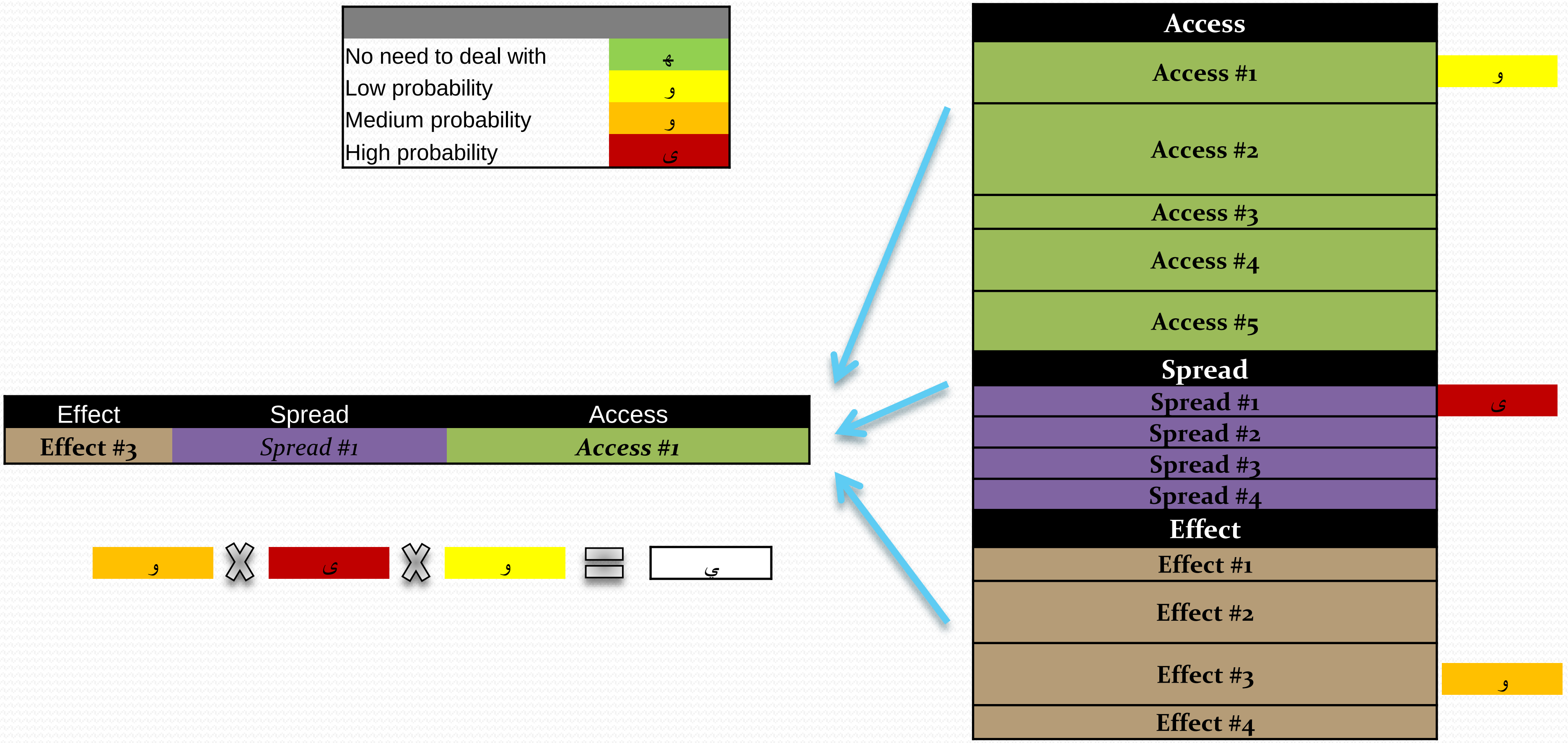
Phase	Actor 4	Actor 3	Actor 2	Actor 1
Access				
Access #1	ى	ى	و	ى
Access #2	ى	ﻬ	ى	و
Access #3	ﻬ	ﻬ	ﻬ	ﻬ
Access #4	و	ﻬ	و	و
Access #5	و	و	و	و
Spread				
Spread #1	و	ﻬ	ى	ى
Spread #2	و	و	و	و
Spread #3	ﻬ	و	ﻬ	ى
Spread #4	و	ى	و	و
Effect				
Effect #1	ﻬ	ى	و	ى
Effect #2	و	ﻬ	و	ﻬ
Effect #3	و	ﻬ	و	ﻬ
Effect #4	ى	ﻬ	و	ى

Access
Spread
Effect

Index	
No need to deal with	ﻬ
Low probability	و
Medium probability	و
High probability	ى

Attack Story likelihood

No need to deal with	ﻪ
Low probability	و
Medium probability	و
High probability	ى



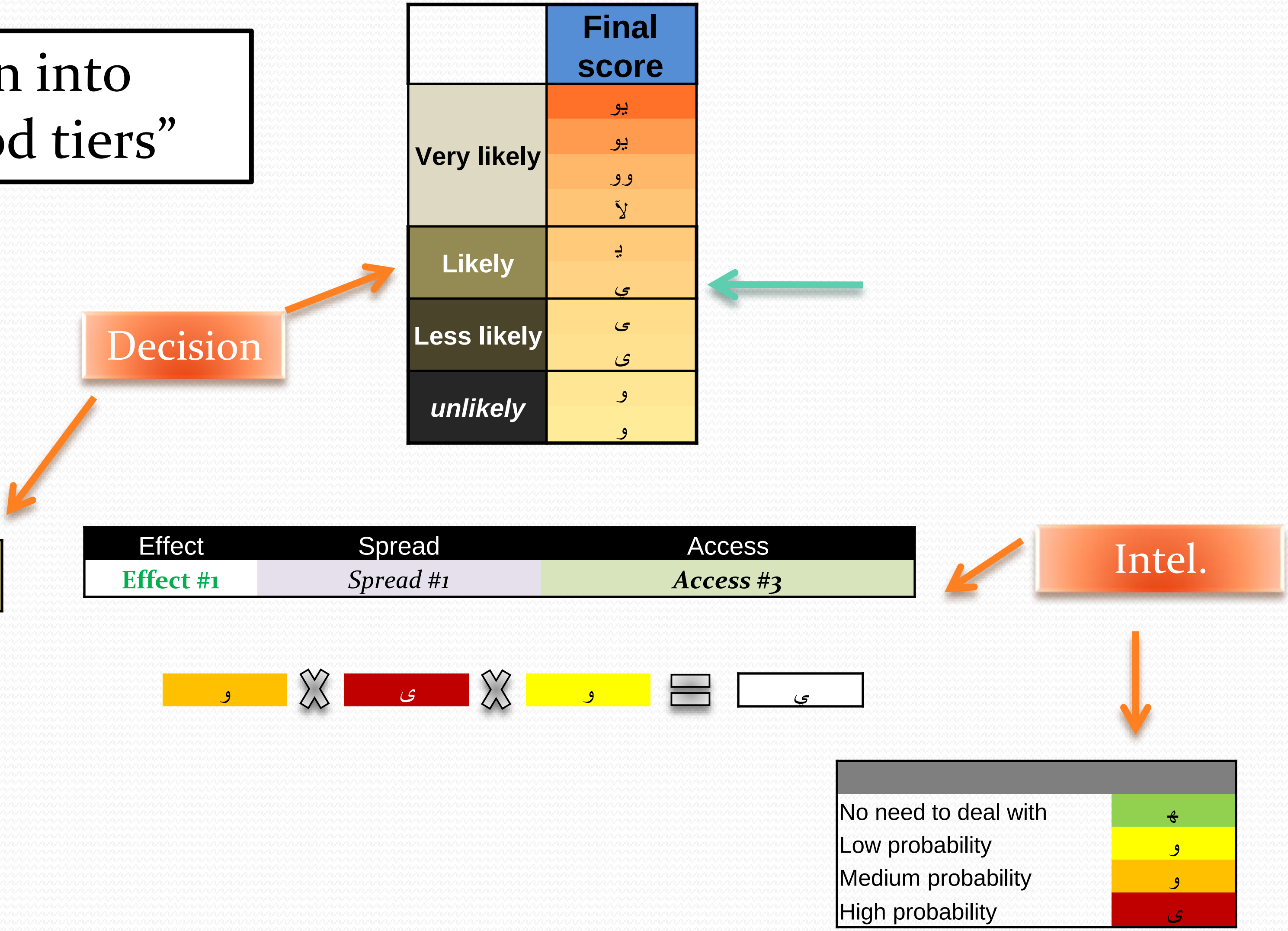
Access	
Access #1	و
Access #2	
Access #3	
Access #4	
Access #5	
Spread	
Spread #1	ى
Spread #2	
Spread #3	
Spread #4	
Effect	
Effect #1	
Effect #2	
Effect #3	و
Effect #4	

Effect	Spread	Access
Effect #3	*Spread #1*	*Access #1*

و × ى × و = ي

Determining the Attack Story likelihood

Division into
“likelihood tiers”



	Final score
Very likely	يو
	يو
	وو
	لآ
Likely	يـ
	ي
Less likely	ى
	ى
unlikely	و
	و

Decision

Likely

Effect	Spread	Access
Effect #1	*Spread #1*	***Access #3***

Intel.

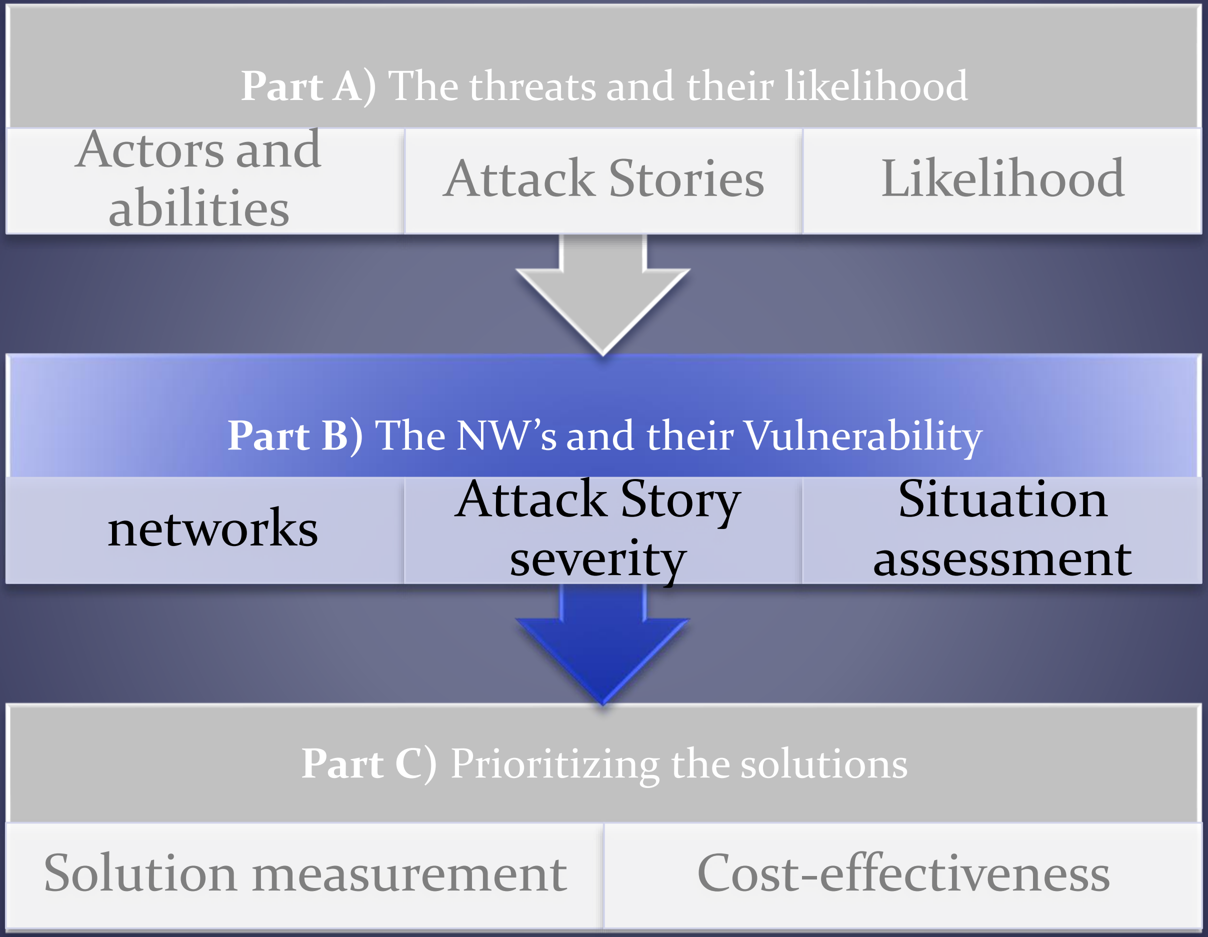
و X ى X و = ي

No need to deal with	ﻬ
Low probability	و
Medium probability	و
High probability	ى

Attack Story list – examples

Phase	Actor 4	Actor 3	Actor 2	Actor 1
Access				
Access #1	ی	ی	و	ی
Access #2	ی	ﮬ	ی	و
Access #3	ﮬ	ﮬ	ﮬ	ﮬ
Access #4	و	ﮬ	و	و
Access #5	و	و	و	و
Spread				
Spread #1	و	ﮬ	ی	ی
Spread #2	و	و	و	و
Spread #3	ﮬ	و	ﮬ	ی
Spread #4	و	ی	و	و
Effect				
Effect #1	ﮬ	ی	و	ی
Effect #2	و	ﮬ	و	ﮬ
Effect #3	و	ﮬ	و	ﮬ
Effect #4	ی	ﮬ	و	ی

TIER	max	Actor 4	Actor 3	Actor 2	Actor 1	Effect	Spread	Access	#
Very likely	یو	ﮬ	ﮬ	وو	یو	Effect #1	Spread #1	Access #1	و
	یو	یو	ﮬ	یو	لآ	Effect #4	Spread #1	Access #2	و
	وو	ﮬ	لآ	ی	وو	Effect #1	Spread #4	Access #5	ی
…									
Likely	ی	ی	ﮬ	ی	ﮬ	Effect #2	Spread #2	Access #1	ﮬو
…									
Less likely	ی	و	ﮬ	ی	ﮬ	Effect #3	Spread #1	Access #5	یی



Part A) The threats and their likelihood

Actors and abilities

Attack Stories

Likelihood

Part B) The NW's and their Vulnerability

networks

Attack Story severity

Situation assessment

Part C) Prioritizing the solutions

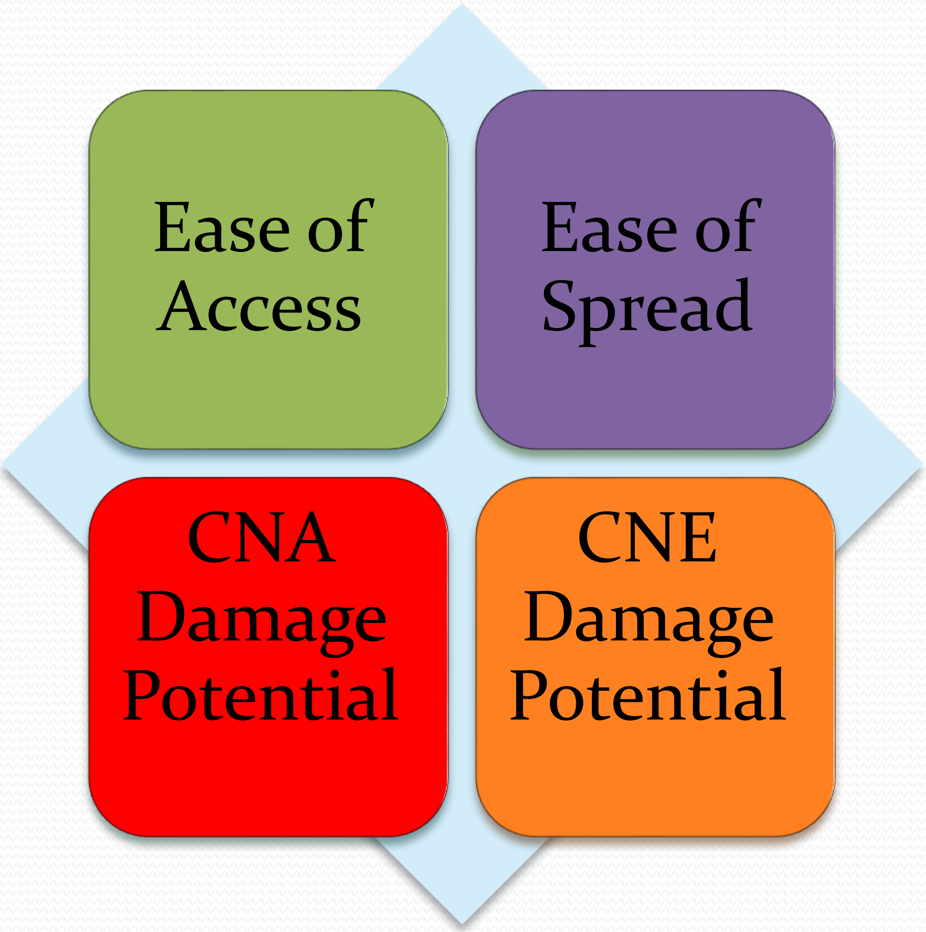
Solution measurement

Cost-effectiveness

Characterization of the important NW’s

- High level characterization of the NW’s by parameters relevant to cyber attacks.
- Focus on most important assets.
- We decided to focus on the NW’s, rather than on the operational processes:
  - The networks are the technological “Base Unit” for analysis.
  - The operational processes “live” in the NW’s, and determine their importance.
- There are a lot of important details, which is difficult to comprehend:
  - Constant “Elaboration & Contraction”

Network Parameters



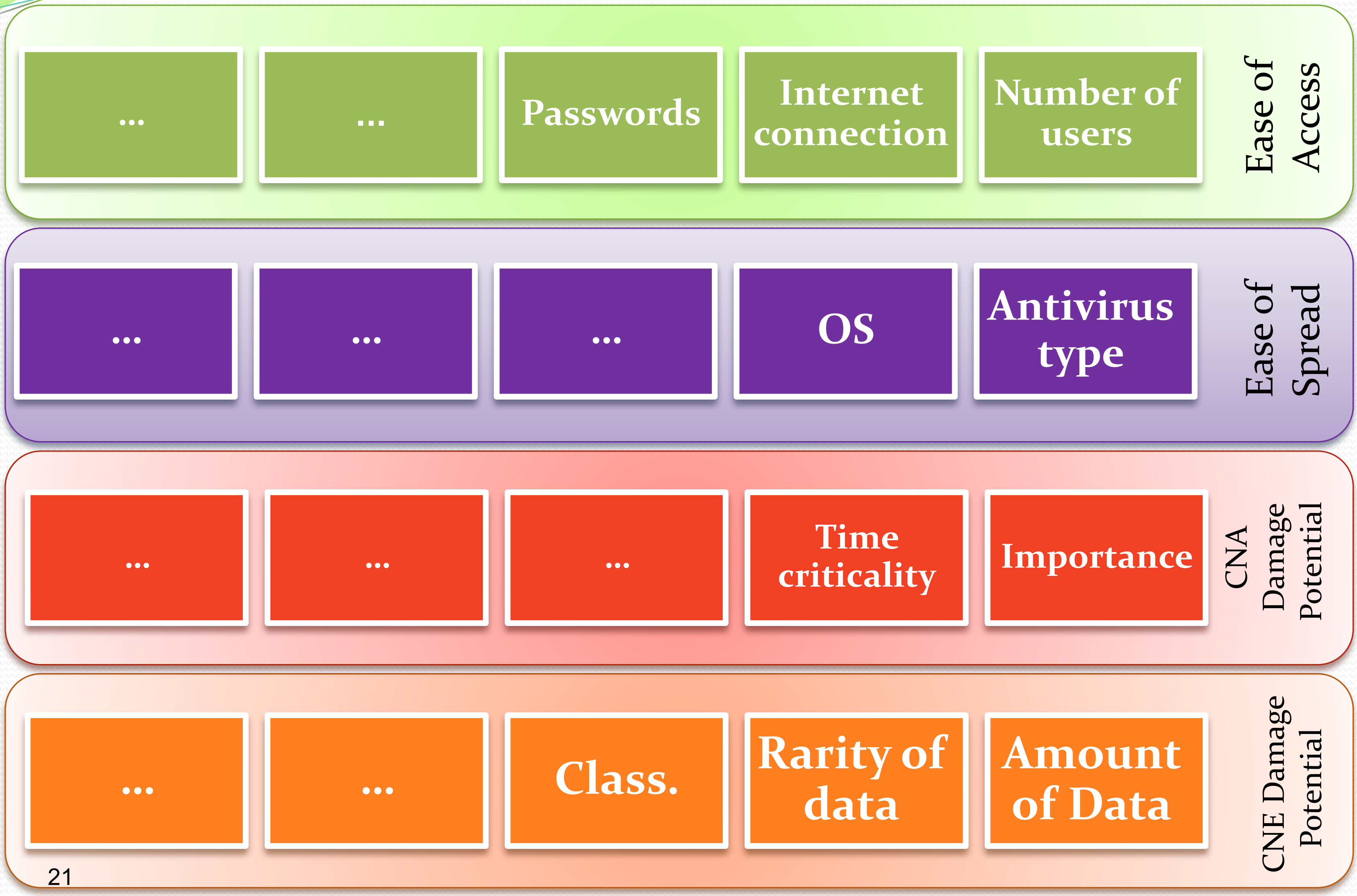
Ease of Access

Ease of Spread

CNA Damage Potential

CNE Damage Potential

Network Parameters



…	…	Passwords	Internet connection	Number of users	Ease of Access
…	…	…	OS	Antivirus type	Ease of Spread
…	…	…	Time criticality	Importance	CNA Damage Potential
…	…	Class.	Rarity of data	Amount of Data	CNE Damage Potential

Multi-stepped analysis

Full Attack Stories

Foothold Score

AS3	AS2	AS1	
Acc' #	Acc' #	Acc' #	
Spread #	Spread #	Spread #	
Local	Partial	All	NW A
Local	Extensive	none	NW B
All	Extensive	none	NW C

Severity of the AS in the NW

AS3	AS2	AS1	
Acc' #	Acc' #	Acc' #	
Spread #	Spread #	Spread #	
Effect #	Effect #	Effect #	
Severe	Severe	Light	NW A
Very Severe	Light	Very Severe	NW B
Severe	Medium	Medium	NW C

Attack Story Components

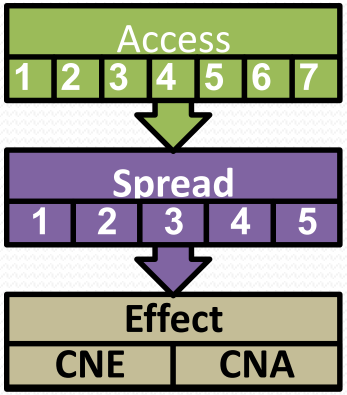
Success Scores

Acc' 7…	Acc' 2	Acc' 1	
succeed	hindered	fail	NW A
succeed	fail	hindered	NW B
Might succeed	succeed	Might succeed	NW C

Spread 5	Spread 2	Spread 1	
Might succeed	hindered	hindered	NW A
succeed	hindered	fail	NW B
Might succeed	fail	succeed	NW C

Damage Potential

CNA	CNE	
Severe	Light	NW A
Light	Very Severe	NW B
Medium	Medium	NW C


Access

1 2 3 4 5 6 7

Spread

1 2 3 4 5

Effect

CNE CNA

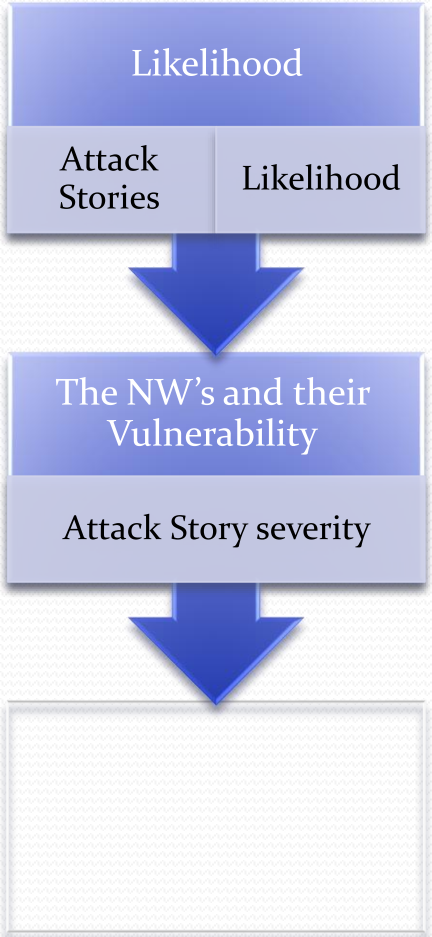
Networks and Parameters

Likelihood / Severity Table

For Example Only

NW	NW	NW	NW	NW	NW	NW	NW	NW	NW	NW	NW	NW		Likelihood	
ﻬ	و	و	ى	ى	ﻬ	ى	و	و	ى	ي	و	ﻬ	**Very likely**	يو	AS1
و	ي	و	و	و	و	ﻬ	ى	ى	ي	و	ى	ﻬ		يو	AS2
و	ى	ي	ى	و	ى	ي	ى	و	ﻬ	ى	و	ﻬ		يو	AS3
ى	ي	و	و	و	ى	و	ى	ى	ﻬ	و	و	ﻬ		يو	AS4
ي	ﻬ	ى	و	ى	ي	ى	ﻬ	و	ى	ى	ى	و		يو	AS5
ي	و	ى	و	ﻬ	ﻬ	ي	و	ى	ﻬ	و	ﻬ	ى		وو	AS6
ﻬ	ى	ى	و	ﻬ	ى	و	ي	و	ﻬ	ﻬ	ى	ﻬ		وو	AS7
ﻬ	ﻬ	و	و	ي	و	ى	ﻬ	ى	و	و	و	و		لآ	AS8
ﻬ	ى	ﻬ	ي	ي	ﻬ	و	و	ى	ى	و	ي	ي		لآ	AS9
ي	ي	ي	ى	ى	ﻬ	ﻬ	و	ى	ي	ى	ى	و	**likely**	ﻳ	AS10
و	و	ى	و	ي	ى	ى	ى	ى	ﻬ	ي	و	ي		ﻳ	AS11
ﻬ	ى	و	و	ى	ى	ي	ي	ي	ي	و	و	ى		ﻳ	AS12
ى	ى	ى	ي	ى	ﻬ	ﻬ	ى	و	و	ى	و	ى		ﻳ	AS13
ﻬ	و	ﻬ	ى	ى	و	ي	ي	ي	و	ى	ي	ي		ﻳ	AS14
و	ﻬ	و	ى	و	ﻬ	و	ى	و	ى	ى	و	و		ي	AS15
ﻬ	ى	ى	ﻬ	ي	ﻬ	ى	و	ى	و	ى	ى	ي		ي	AS16
ﻬ	و	ى	ى	و	و	ى	و	ي	و	ى	ى	ي		ى	AS17
ﻬ	ي	ى	و	ى	ى	و	ى	ى	ى	ي	و	و	**Less likely**	ى	AS18
ي	ي	ى	ى	ى	ﻬ	و	ى	ﻬ	ﻬ	ى	ﻬ	ﻬ		ى	AS19
و	و	و	ى	ي	ى	ﻬ	ي	و	و	ي	ى	ى		ى	AS20
ي	و	و	و	ي	ى	ى	ي	ى	ى	و	و	ي		ى	AS21
ى	ى	و	و	ﻬ	ى	ى	ى	و	و	و	ى	ﻬ		ى	AS22
ﻬ	ﻬ	ي	ى	ى	ى	ي	ﻬ	ي	ﻬ	ي	ى	ى		ى	AS23
ي	و	و	ى	ﻬ	و	و	و	ى	ى	ى	و	ى	***Un-likely***	و	AS24
و	ى	و	ى	و	و	ى	ى	و	ى	ى	و	ى		و	AS25

no damage	ﻬ
Very light damage	و
light damage	و
medium damage	ى
high damage	ى
very high damage	ي



Likelihood

Attack Stories

Likelihood

The NW’s and their Vulnerability

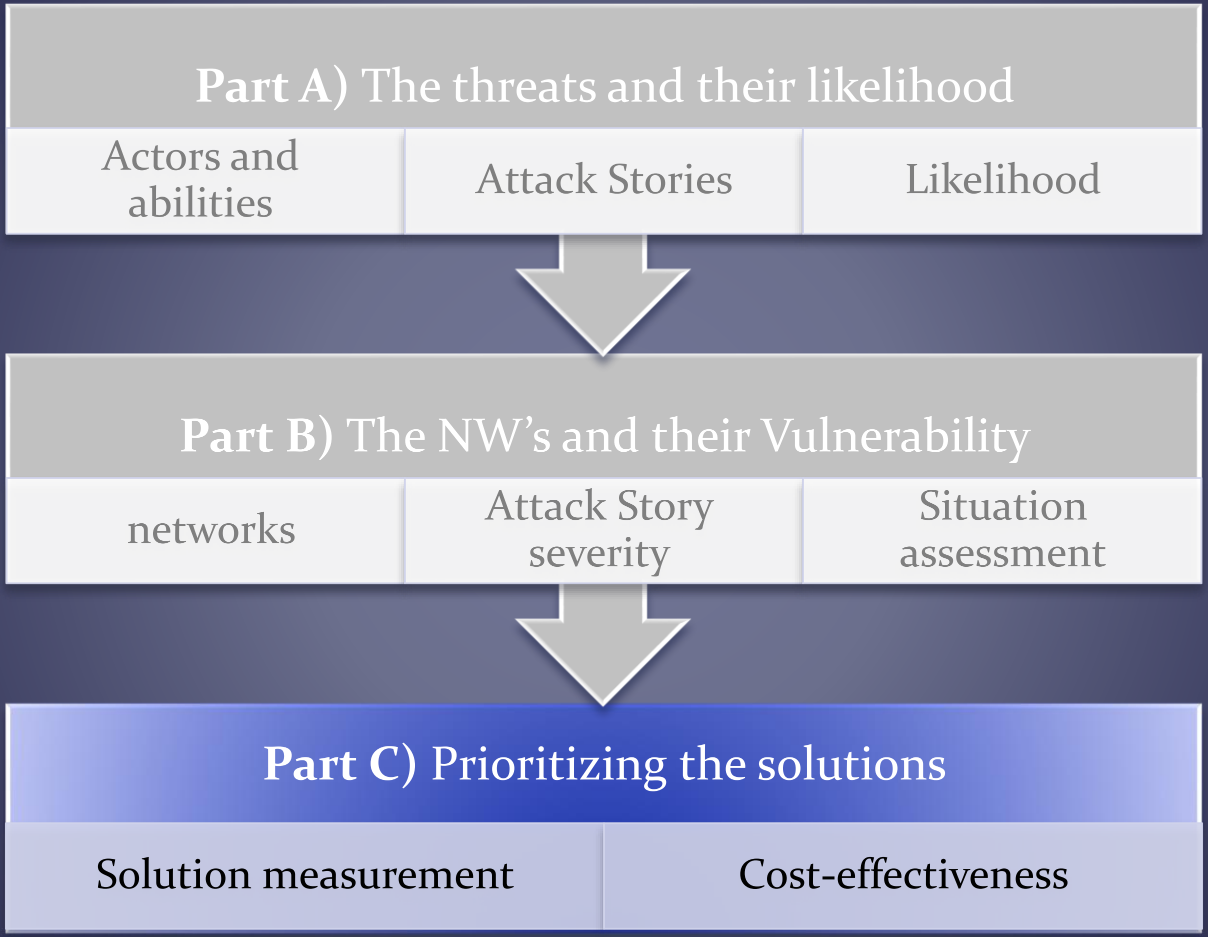
Attack Story severity

From networks to processes

Relevant NWs:

5, 12, 17

NW	NW	NW		Likelihood	
ﻬ	و	ﻬ	**Very likely**	يو	AS1
و	ي	ﻬ		يو	AS2
و	ى	ﻬ		يو	AS3
ى	ي	ﻬ		يو	AS4
ي	ﻬ	و		يو	AS5
ي	و	ى		وو	AS6
ﻬ	ى	ﻬ		وو	AS7
ﻬ	ﻬ	و		ﻵ	AS8
ﻬ	ى	ﻬ		ﻵ	AS9
ي	ي	و	**likely**	ﻳ	AS10
و	و	ي		ﻳ	AS11
ﻬ	ى	ى		ﻳ	AS12
ى	ى	ى		ﻳ	AS13
ﻬ	و	ي		ﻳ	AS14
و	ﻬ	و		ي	AS15
ﻬ	ى	ي		ي	AS16
ﻬ	و	ي		ي	AS17
ﻬ	ي	و	**Less likely**	ى	AS18
ي	ي	ﻬ		ى	AS19
و	و	ى		ى	AS20
ي	و	ي		ى	AS21
ى	ى	ﻬ		ى	AS22
ﻬ	ﻬ	ى		ى	AS23
ي	و	ى	***Un-likely***	و	AS24
و	ى	ى		و	AS25



Part A) The threats and their likelihood

Actors and abilities

Attack Stories

Likelihood

Part B) The NW’s and their Vulnerability

networks

Attack Story severity

Situation assessment

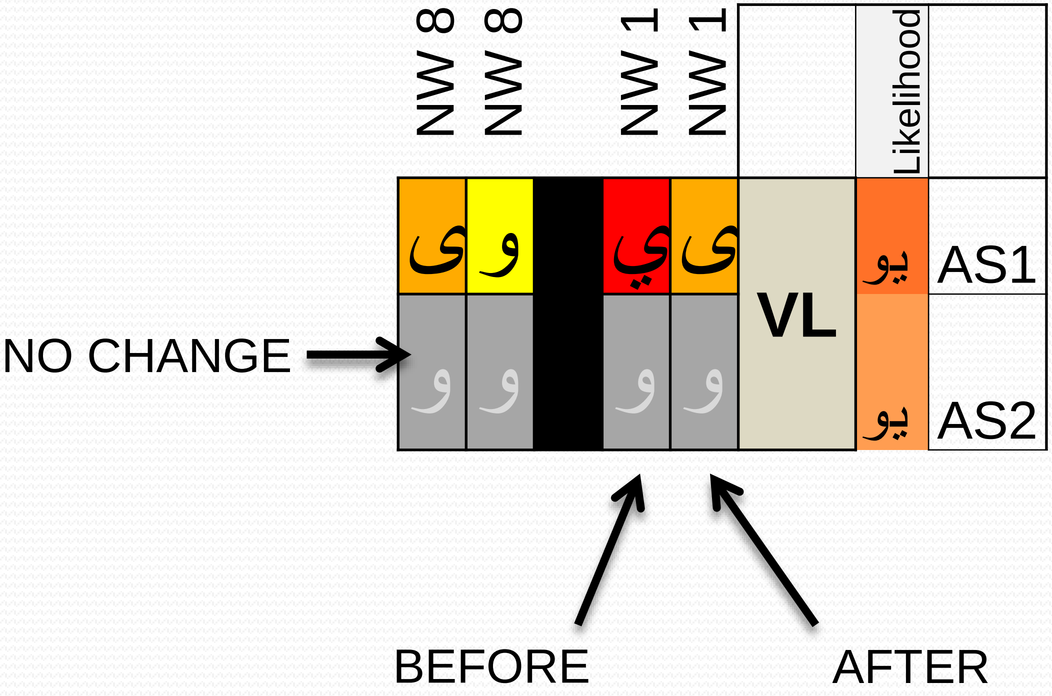
Part C) Prioritizing the solutions

Solution measurement

Cost-effectiveness

One Solution, multiple networks

Add “rules” to previous section to compute “BEFORE” and “AFTER”



NW 8	NW 8		NW 1	NW 1		Likelihood	
ى	و		ي	ى	VL	يو	AS1
و	و		و	و		يو	AS2

NO CHANGE

BEFORE

AFTER

NW 8	NW 8		NW 1	NW 1		Likelihood	
ى	و		ي	ى	Very likely	يو	AS1
و	و		و	و		يو	AS2
ى	ى		ـهـ	ـهـ		يو	AS3
و	ـهـ		ى	ـهـ		يو	AS4
و	و		ى	ى		يو	AS5
ـهـ	ـهـ		و	و		وو	AS6
و	ـهـ		ى	ـهـ		وو	AS7
ي	ي		ى	ى		لآ	AS8
ى	ى		و	و		لآ	AS9
ي	ى		و	و	likely	يـ	AS10
ي	ي		و	و		يـ	AS11
و	و		ي	ى		يـ	AS12
ي	و		ـهـ	ـهـ		يـ	AS13
ى	ى		و	و		يـ	AS14
ى	ى		و	و		ي	AS15
ى	ى		و	و		ي	AS16
ي	ي		ـهـ	ـهـ		ي	AS17
ـهـ	ـهـ		ـهـ	ـهـ	Less likely	ى	AS18
و	و		ـهـ	ـهـ		ى	AS19
ى	ى		ـهـ	ـهـ		ى	AS20
و	و		و	و		ى	AS21
و	و		ي	و		ى	AS22
و	و		ى	ى		ى	AS23
ى	ى		و	و	*Un-likely*	و	AS24
ى	و		ي	ى		و	يو AS25

One NW, many solutions

SOL 2 – takes care of an acute problem

SOL 1 + 5 - complimentary

SOL 3 – shadowed by 1

SOL 4 – powerful, in less-important areas

sol 5	sol 4	sol 3	sol 2	sol 1		NW		Likelihood	
ي	ي	ي	و	ي		ي	Very likely	يو	AS1
و	و	ﻬ	و	ﻬ		و		يو	AS2
ﻬ	ﻬ	ﻬ	ﻬ	ﻬ		ﻬ		يو	AS3
ى	ى	و	ى	و		ى		يو	AS4
و	ى	ى	ى	ى		ى		يو	AS5
ﻬ	و	و	و	و		و		وو	AS6
ى	ى	و	ى	و		ى		وو	AS7
و	ى	ى	ى	ى		ى		لآ	AS8
و	و	و	و	ﻬ		و		لآ	AS9
و	و	و	و	و		و	likely	ﻳ	AS10
و	و	و	و	و		و		ﻳ	AS11
ي	ي	ى	ي	ى		ي		ﻳ	AS12
ﻬ	ﻬ	ﻬ	ﻬ	ﻬ		ﻬ		ﻳ	AS13
و	و	و	و	و		و		ﻳ	AS14
و	ﻬ	ﻬ	و	و		و		ي	AS15
و	ﻬ	و	و	ﻬ		و		ي	AS16
ﻬ	ﻬ	ﻬ	ﻬ	ﻬ		ﻬ		ي	AS17
ﻬ	ﻬ	ﻬ	ﻬ	ﻬ		ﻬ	Less likely	ى	AS18
ﻬ	ﻬ	ﻬ	ﻬ	ﻬ		ﻬ		ى	AS19
ﻬ	ﻬ	ﻬ	ﻬ	ﻬ		ﻬ		ى	AS20
ﻬ	ﻬ	و	و	و		و		ى	AS21
ي	ﻬ	ي	ي	و		ي		ى	AS22
ى	ﻬ	ى	ى	ى		ى		ى	AS23
و	ﻬ	و	و	و		و	*Un-likely*	و	AS24
ي	ﻬ	و	ي	ي		ي		و	يو AS25

PRICE

- 3 types of prices:
  - One time (R&D, etc)
  - Per network
  - Per Computer

QUESTIONS?

An Automated method for Large Scale Comprehensive Risk Management of cyber-security