دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

مرکز پژوهشی آپا
دانشگاه صنعتی امیرکبیر

ایجاد درخت وابستگی مأموریتی و ارزیابی اثرات حمله

(گفتار دوم در موضوع: آگاهی از وضعیت امنیت سایبری با ابزار CyGraph)

ارائه دهنده
مطهره دهقان

اسفند ۹۹

فهرست مطالب

- مروری کوتاه بر گفتار اول
  - تعریف آگاهی از وضعیت
  - معرفی ابزار CyGraph
- متدلوژی RiskMAP برای ایجاد درخت وابستگی
- ایجاد خودکار و مبتنی بر آنتولوژی درخت وابستگی
- معرفی ابزار CMIA
- ارزیابی اثرات قطعی حملات
- ارزیابی اثرات غیر قطعی حملات

آگاهی از وضعیت [1]

- درک مفهوم آگاهی از وضعیت، نیازمند درک مفهوم آگاهی است.
- آگاهی، مفهومی نسبی است که می‌تواند بر حالتی درونی متمرکز شود.
- مفهوم آگاهی وابسته به علـوم مختلـف همچـون روانشناسـی، neuroscience و ... است.
- در واقع، تعریفی واضح و روشن برای مفهوم آگاهی وجود ندارد.
- به همین دلیل، نیاز به تبیین مفهوم آگاهی از وضعیت وجود دارد.

سناریوی کاربردی

آگاهی از وضعیت در کاربرد رانندگی

آگاهی از وضعیت [2]

- مدل اِندزلی: آگاهی از وضعیت (SA) عبارتست از درک عناصر محیط در یک فضا و زمان مشخص، فهم معانی (منظور) آن ها و پیش بینی یا تخمین وضعیت آن ها در آینده نزدیک.

- براساس این تعریف، آگاهی از وضعیت دارای سه سطح ادراک (Perception) ، فهم (Comprehension)، پیش بینی یا تخمین (Projection) است.

- تعاریف متفاوتی از آگاهی از وضعیت ارائه شده است که فرض کلی همه تعاریف این است که هرچه آگاهی از وضعیت بهتری وجود داشته باشد، تصمیم گیری نیز بهتر انجام می شود؛ زیرا اطلاعات، درک و فهم قبل از تصمیم گیری بهبود می یابد.

ابزار CyGraph [3]

- ابزارهای مختلفی برای تحلیل امنیت وجود دارد که نتیجه استفاده از این ابزارها در کنار هم، حجم بالای اطلاعات و عدم دستیابی به تحلیل درست از وضعیت امنیت سایبری است.

- آقای Steven Noel در دانشگاه George Mason و پس از آن در شرکت MITRE، سعی برآن داشته تا راهی برای تحلیل و ادغام اطلاعات بدست آمده از وضعیت امنیت سایبری را ایجاد نموده و گراف حاصل از اطلاعات بدست آمده را ایجاد کند، تا نتایج بهتری از تحلیل اطلاعات برای تشخیص فعالیت های موذی حاصل شود.

پشته دانش ابزار CyGraph [3]

وابستگی مأموریتی
- اهداف
- فعالیت ها
- وظایف

تهدیدات سایبری
- عامل
- حوادث
- شاخص ها
- اشخاص ثالث

مواضع سایبری
- پیکره بندی
- آسیب پذیری ها
- قوانین خط مشی

زیرساخت شبکه
- تقسیم بندی
- سنسور
- توپولوژی

مرتبط با جنگ سایبری و آمادگی مأموریتی

معماری ابزار CyGraph [3]

زیر ساخت شبکه

مواضع سایبری

تهدیدات سایبری

وابستگی مأموریتی

دریافت کردن

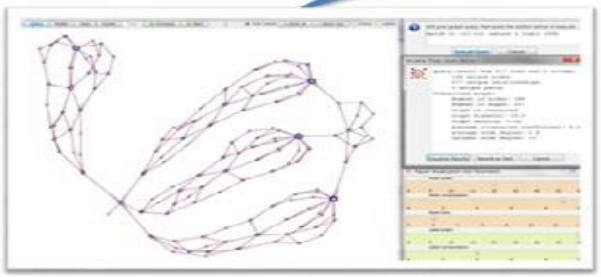
مدل نرمالیزه شده

تبدیل کردن

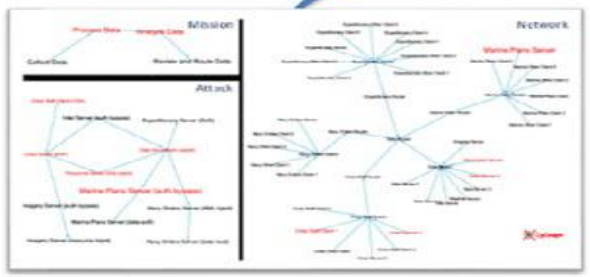
مدل گراف

تحلیل کردن

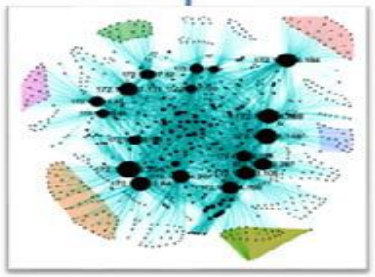
بصری سازی



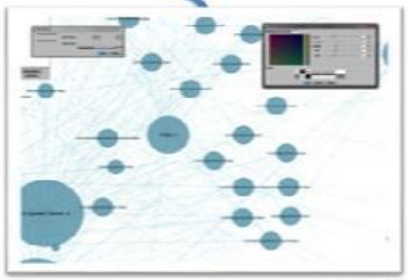
پویایی



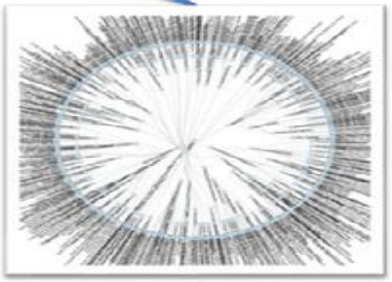
لایه بندی کردن



گروه بندی کردن

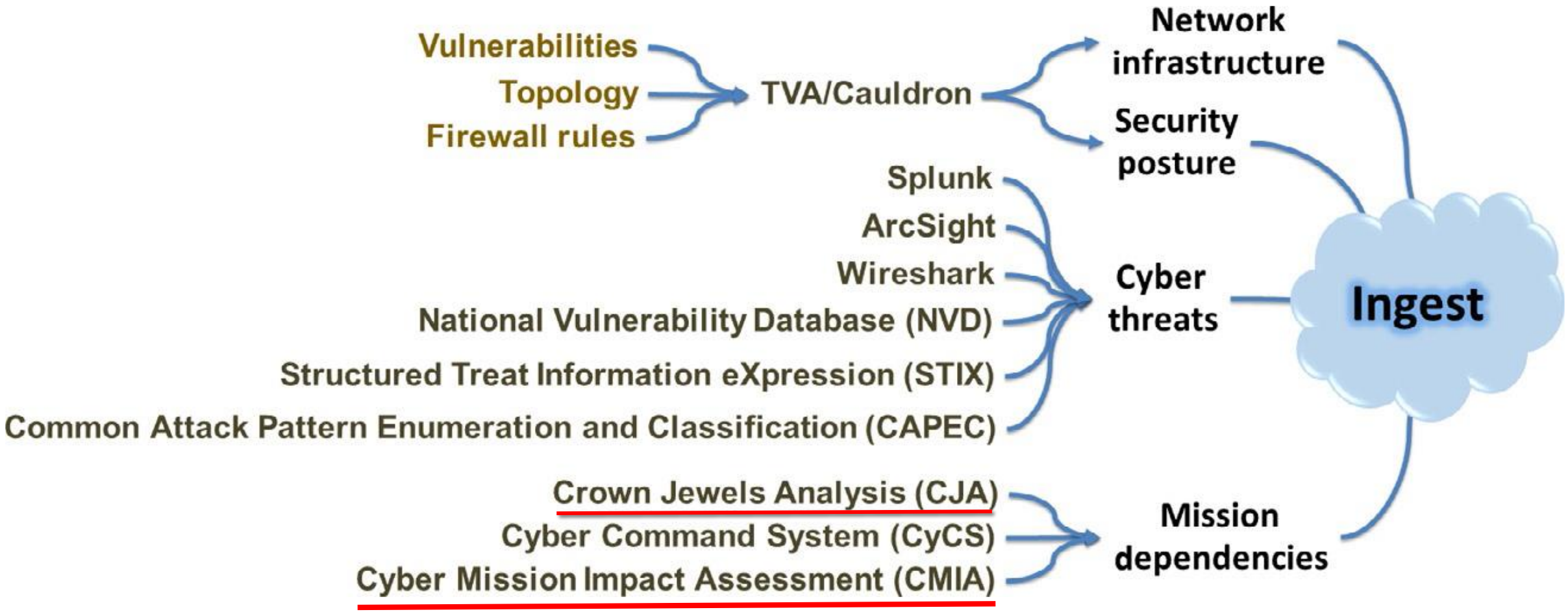


فیلترکردن

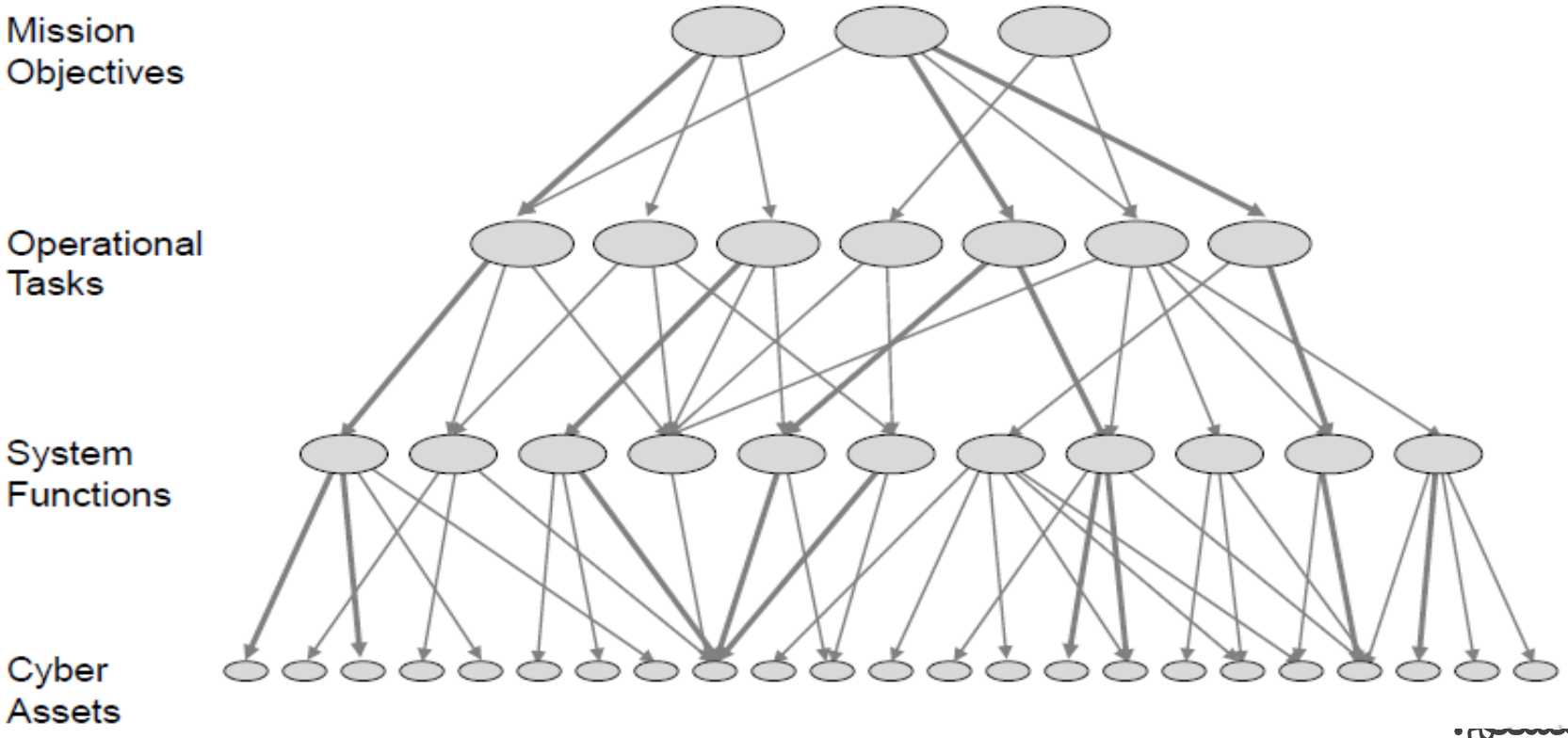


دیدهای سلسله مراتبی

نمونه ای از منابع داده مورد استفاده در CyGraph [3]



متدلوژی RiskMAP برای ایجاد درخت وابستگی [4]



متدلوژی برای

تلفیقی از دو مد

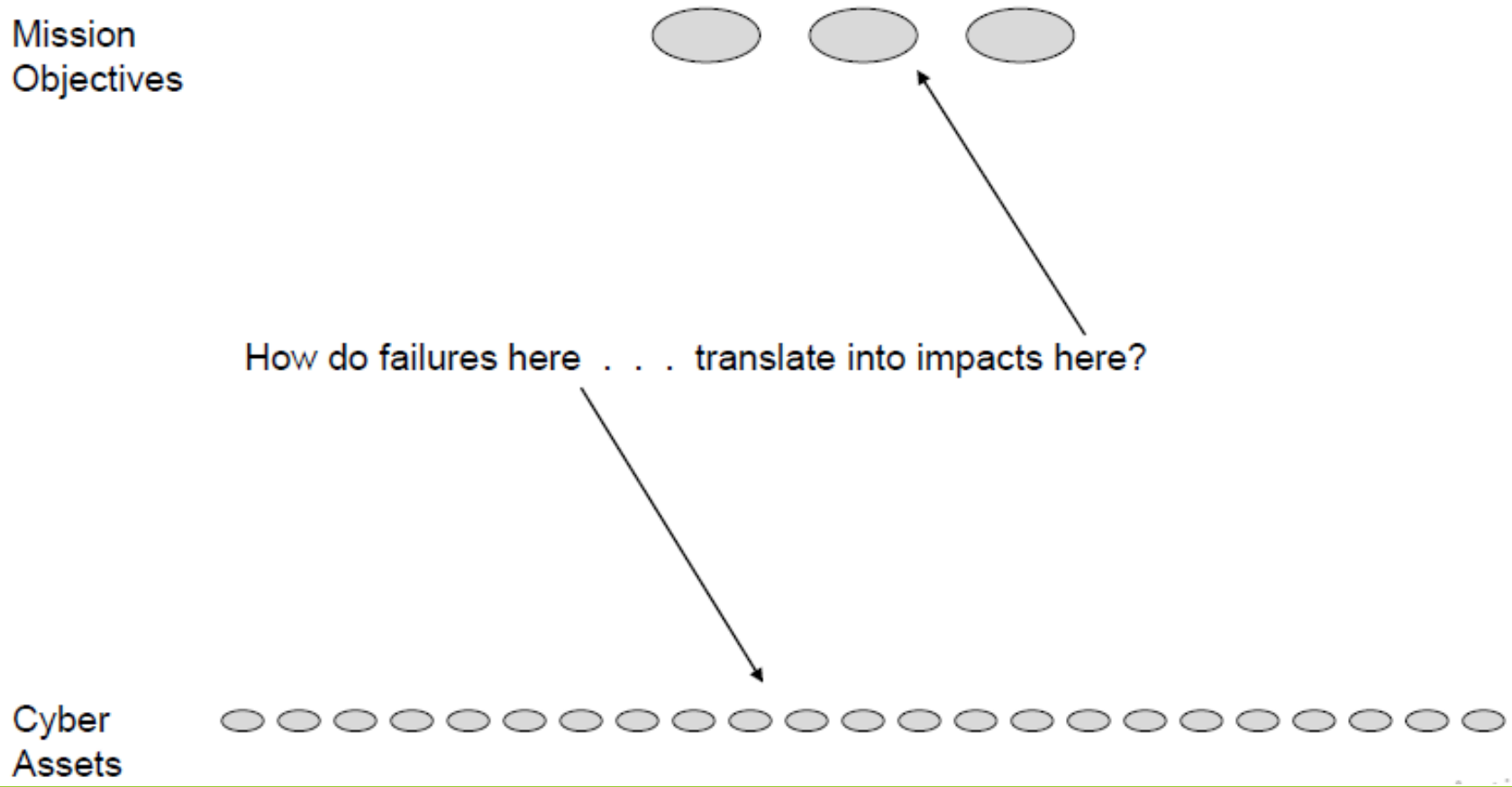
مدل کسب و ک

- شناسایی
- شناسایی
- شناسایی
- شناسایی

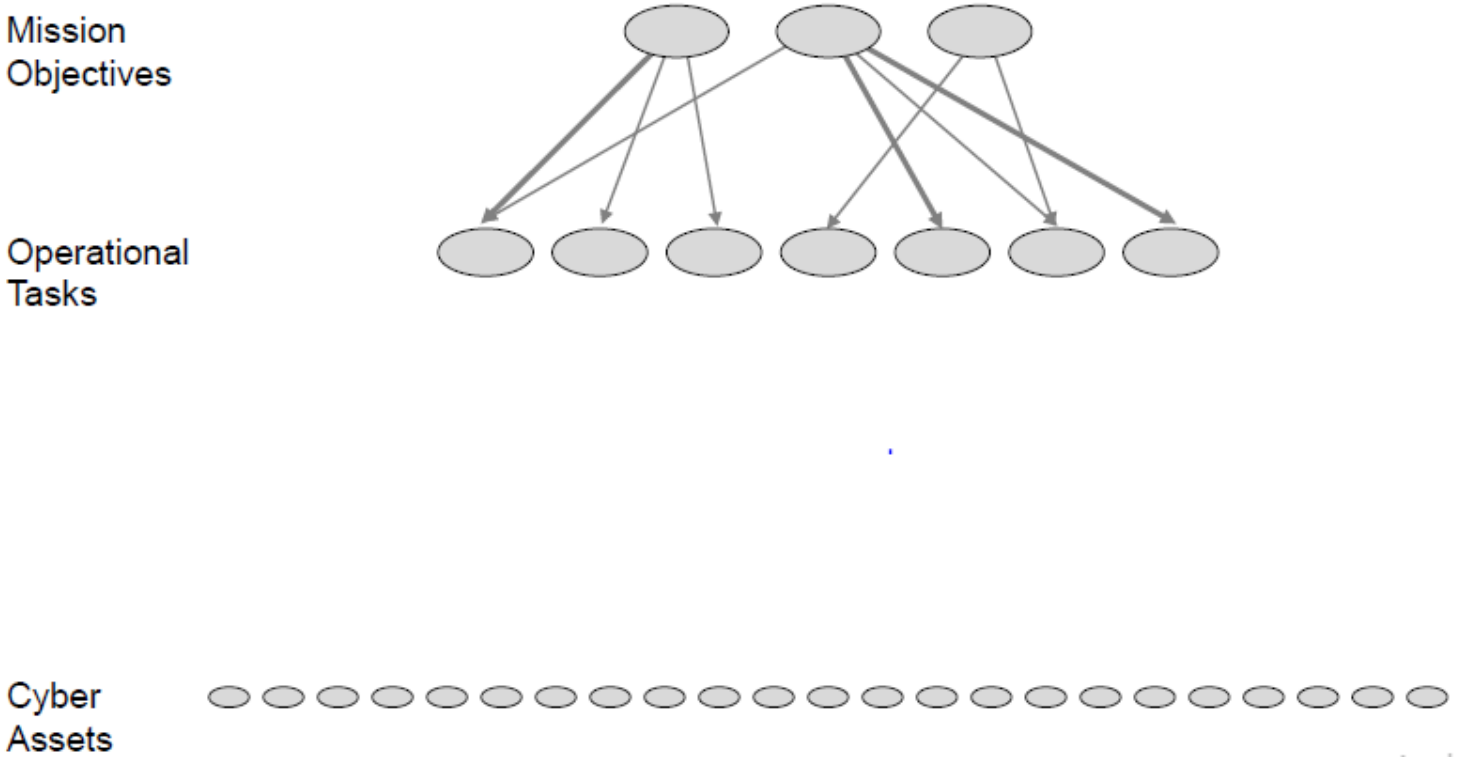
مدل ریسک سیستم.

- شناسایی دارایی های سایبری، ارزیابی تهدیدات و آسیب پذیری های آن ها، اندازه گیری ریسک دارایی های آن ها

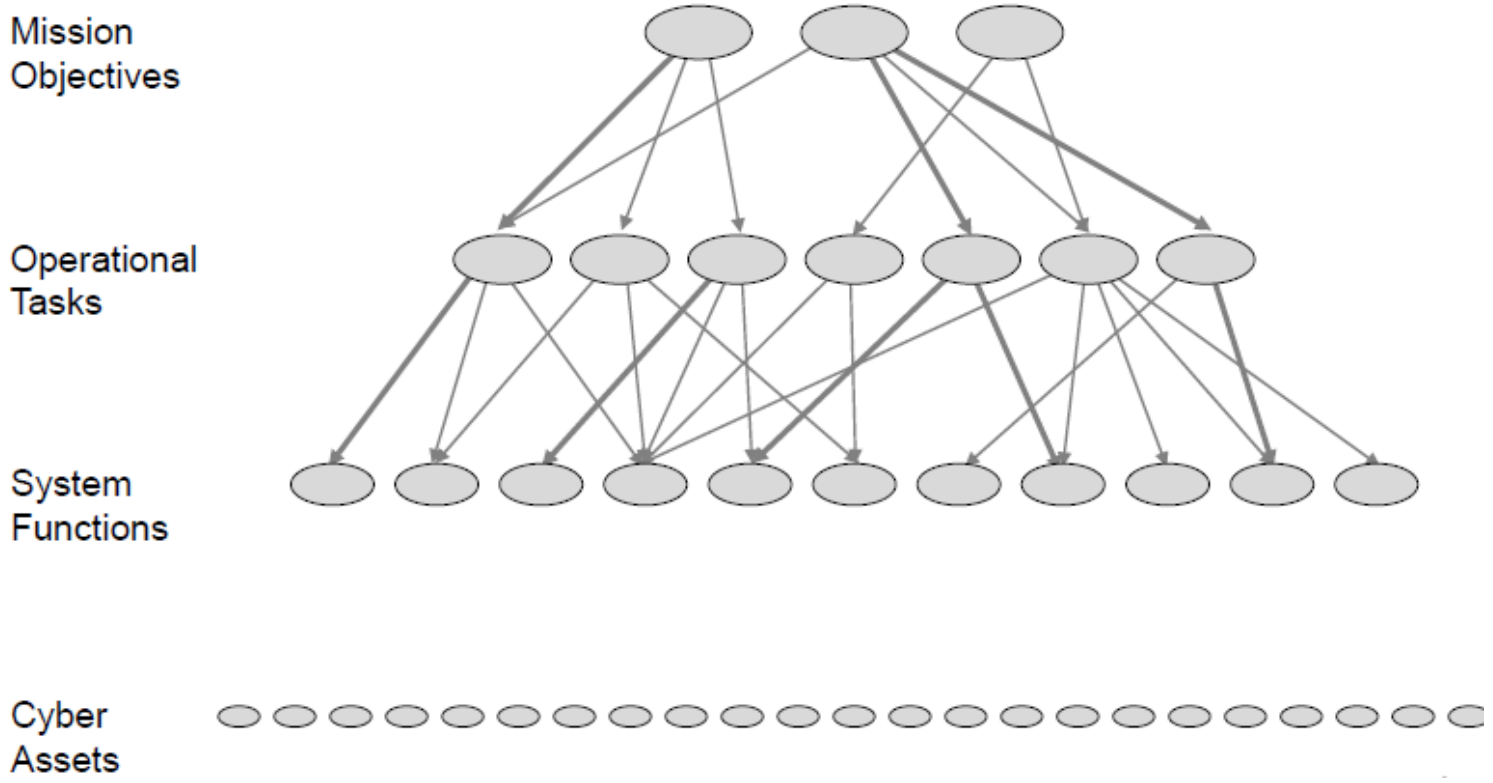
پاسخ به یک سوال کلیدی [4]



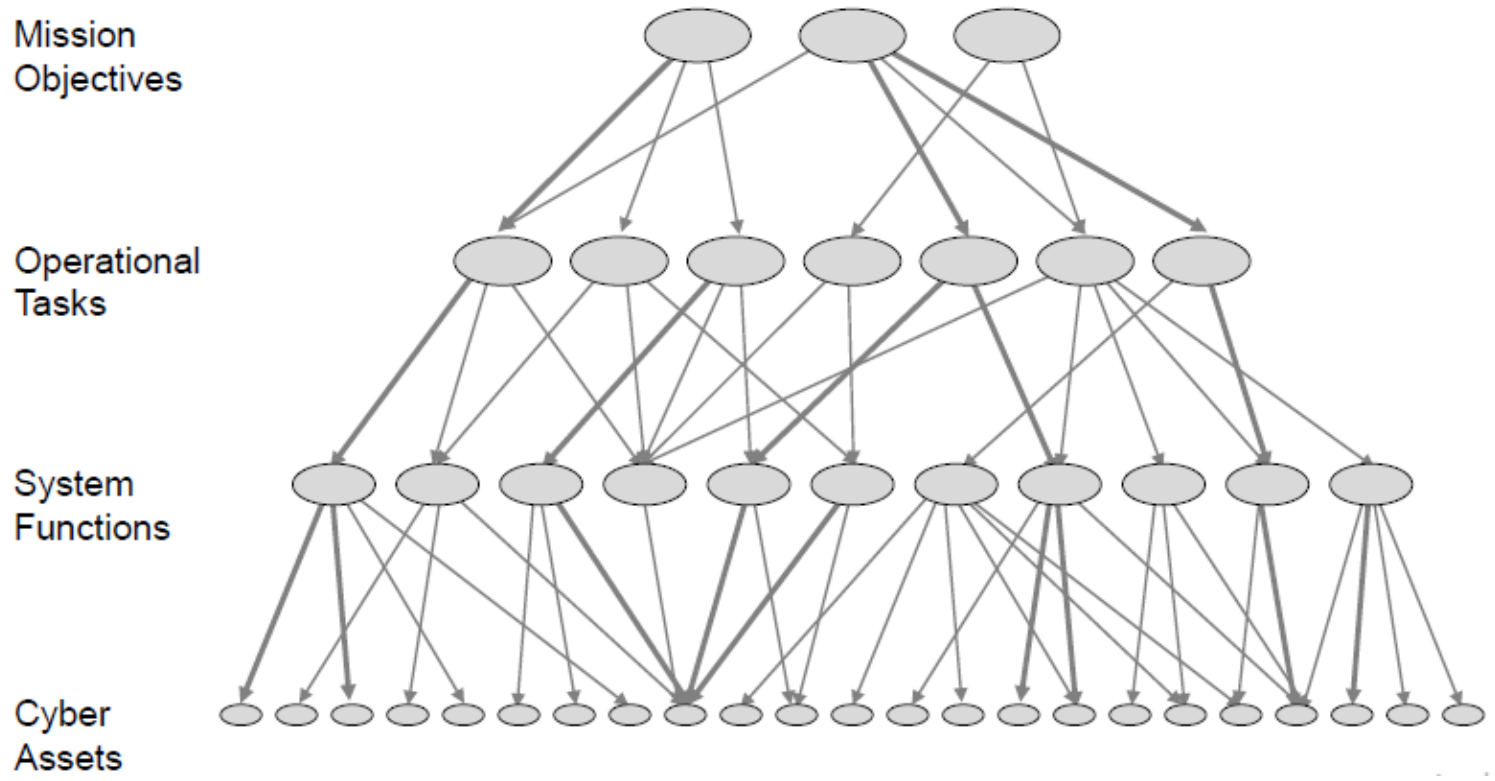
ایجاد مدل کسب و کار [4]
۱- شناسایی وظایف پشتیبان کننده اهداف مأموریتی



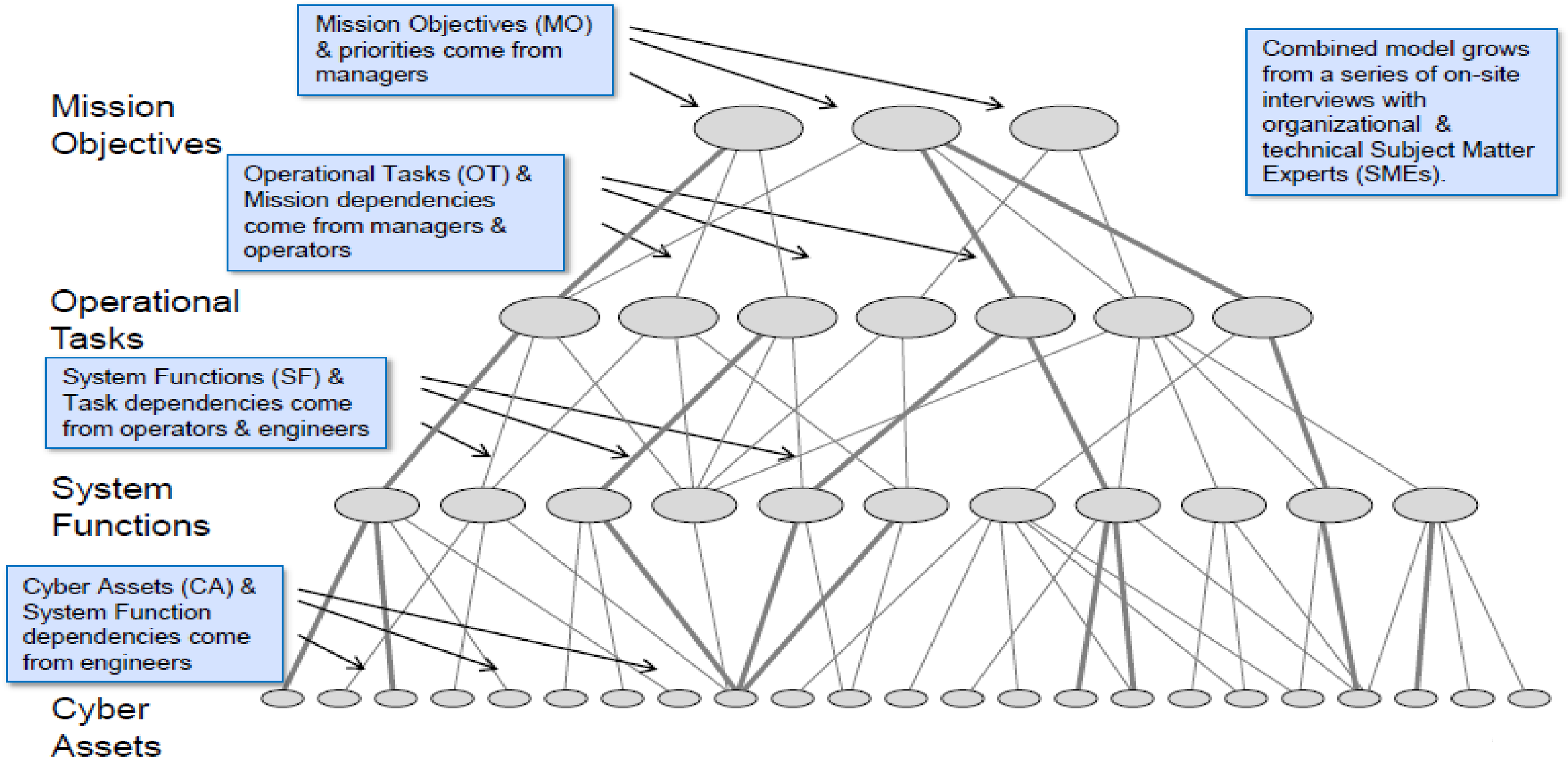
ایجاد مدل کسب و کار [4]
۲- شناسایی توابع سیستمی پشتیبان کننده وظایف



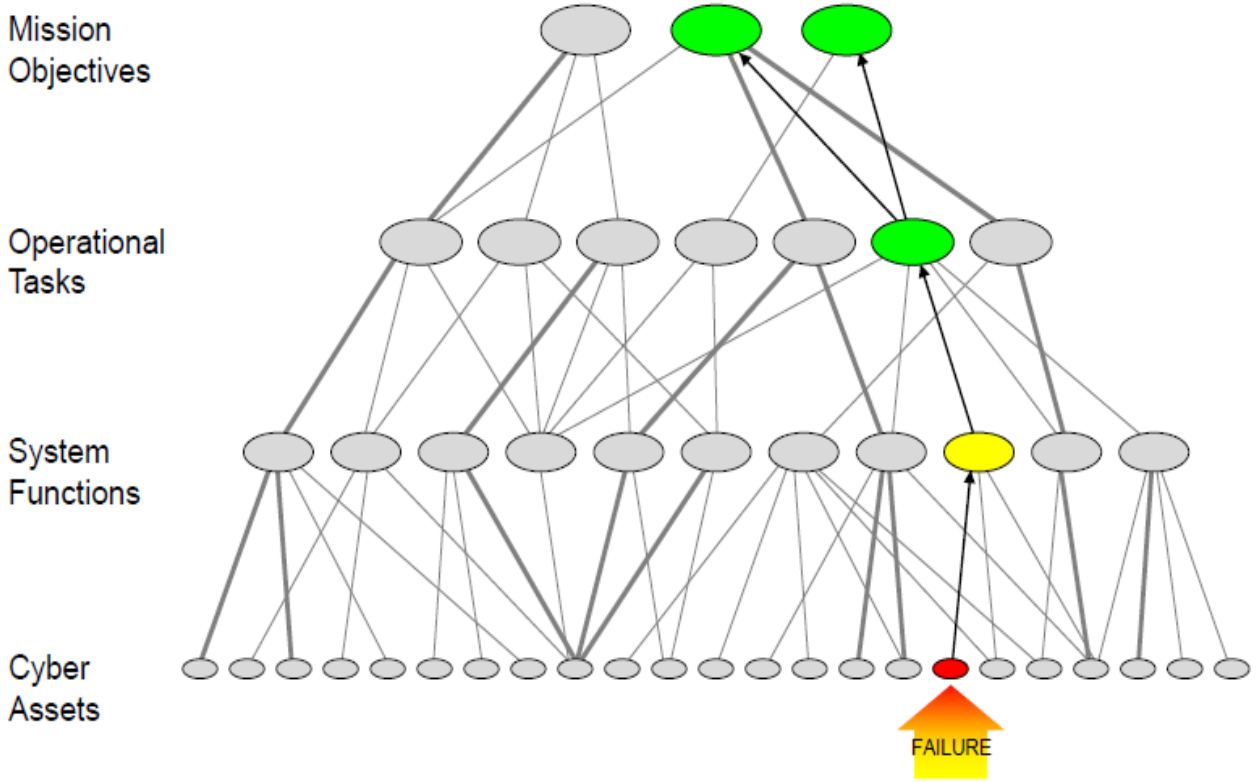
ایجاد مدل کسب و کار [4]
۳- شناسایی دارایی های پشتیبان کننده توابع سیستمی

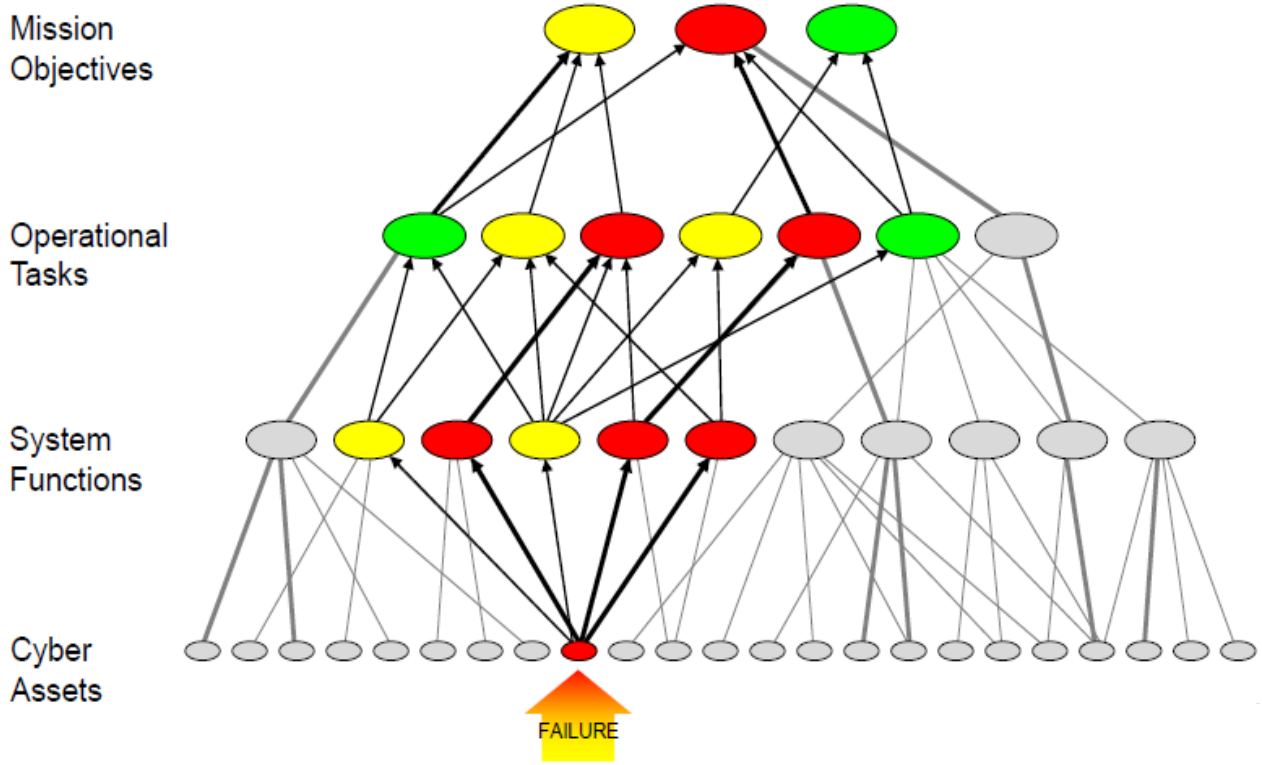


جمع آوری اطلاعات لایه ها [4]



استفاده از وابستگی ها برای پیش بینی اثرات شکست دارایی ها[4]





ایجاد مدل ریسک شبکه بر اساس [5]

۱- جمع آوری آسیب پذیری دارایی های سایبری

۲- اندازه گیری میزان تهدیدات براساس آسیب پذیری ها

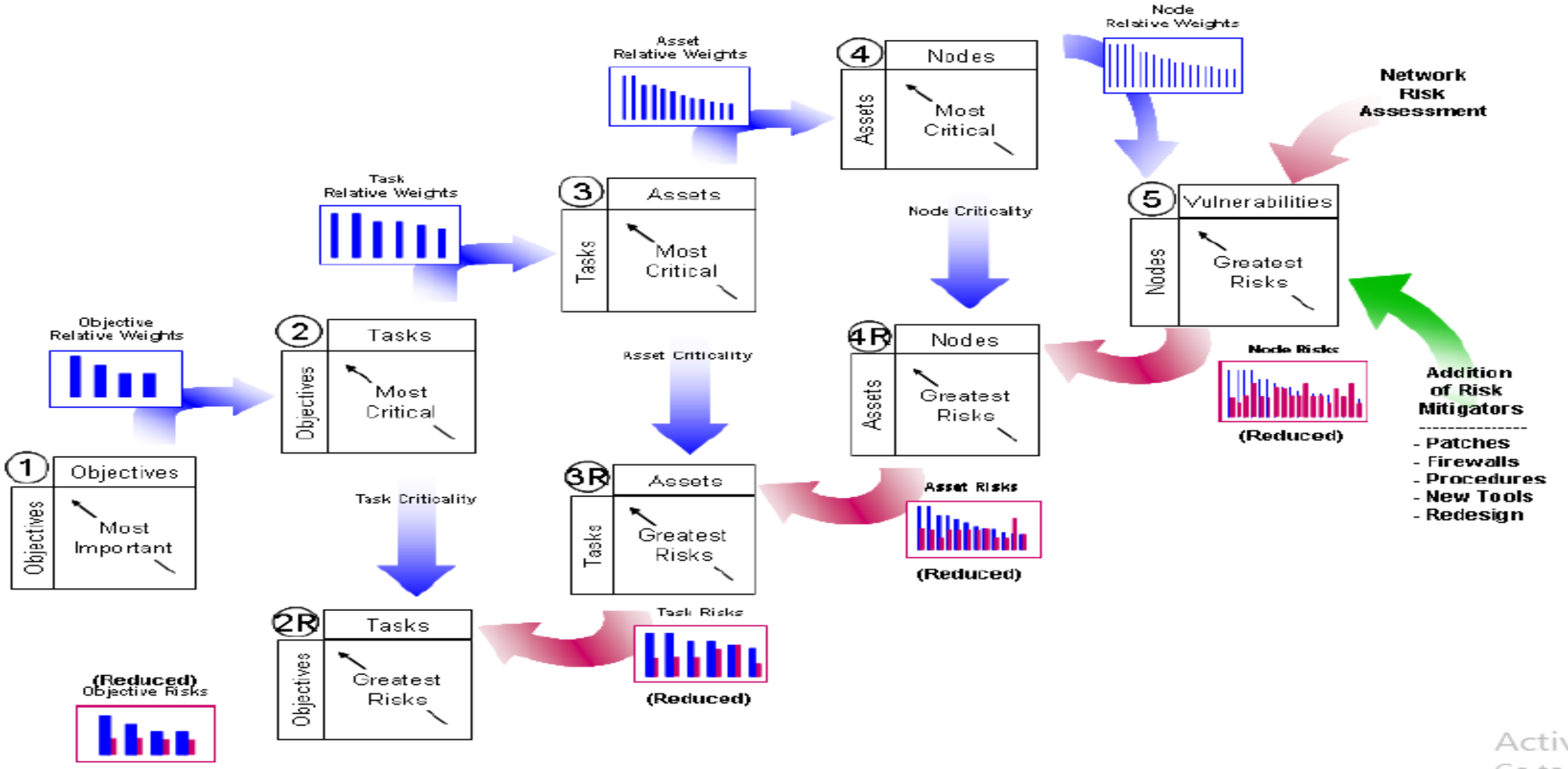
۳- تخمین سطح ریسک براساس آسیب پذیری ها و تهدیدات

۴- شناسایی اقدامات متقابلی که تاکنون مورد توجه قرار نگرفته است.

۵- تخمین مجدد سطح ریسک با در نظر گرفتن اقدامات متقابل گام قبل

۶- در نظر گرفتن بالاترین سطح ریسک برای گره با چندین آسیب پذیری

خلاصه ای از متدلوژی RiskMAP [5]



مثال– صنعت پالایش نفت [5]

SCALE: 1 = Row is EQUALLY IMPORTANT to Column 2 = Row is SLIGHTLY MORE IMPORTANT than Column 4 = Row is SIGNIFICANTLY MORE IMPORTANT than Column 8 = Row is FAR MORE IMPORTANT than Column (Use reciprocals for LESS IMPORTANT cases)	Stay safe	Stay profitable	Stay in compliance	Supply customers well	Sums	Normalized Relative Weights
Stay safe	1	1.25	1.75	2	6.000	0.348
Stay profitable	0.8	1	1.4	1.6	4.800	0.279
Stay in compliance	0.571	0.714	1	1.143	3.429	0.199
Supply customers well	0.5	0.625	0.875	1	3.000	0.174
				Total >>	17.229	1.000

ماتریس ۱– وزن نسبی اهداف مأموریتی

Mission Impact from Loss of Task:

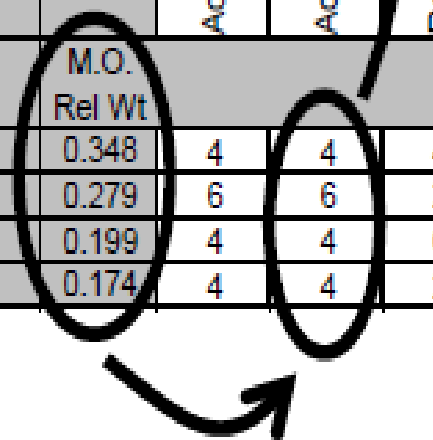
0 = No Impact on Achievement

2 = Objective Achievable Using Work Around

4 = Objective Degraded Even With Work Around

6 = Objective Not Achievable at all

			1	2	3	4	5	6	7	8	9	10	11	12	13	14
		Task Rel Wt	4.56	4.56	3.49	3.30	2.61	2.59	2.16	1.81	1.81	1.81	1.65	1.30	0.91	0.56
	Mission Objective	Task	Acquire Natural Gas	Acquire Water	Receive Caustic	Acquire Electrical Power	Quality Test During Loading	Impurity Removal	Blend & Load Lube Oils	Perform Fractional Distillation	Perform Hydro-Treating	Quality Test During Processing	Load Other Products	Unload & Store Crude	Bill for Product	Acceptance Test Crude
		M.O. Rel Wt														
1	Stay safe	0.348	4	4	4	2	0	4	0	0	0	0	0	0	0	0
2	Stay profitable	0.279	6	6	2	4	4	0	4	4	4	4	2	2	2	2
3	Stay in compliance	0.199	4	4	6	4	4	6	0	0	0	0	2	2	0	0
4	Supply customers well	0.174	4	4	2	4	4	0	6	4	4	4	4	2	2	0



ماتریس ۲- وزن نسبی وظایف نسبت به اهداف مأموریتی

ماتریس ۳- وزن نسبی دارایی های اطلاعاتی براساس بحرانی بودن آن ها برای وظایف

Task Impact from Loss of Asset:

0 = No Impact on Task

2 = Task Co

4 = Task De

6 = Task Cannot Be Done At All

	Tasks	Task Rel Wt	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	Asset Rel Wt		32.08	32.08	24.84	24.84	24.84	24.84	24.84	24.84	24.28	21.73	21.73	21.73	21.73	21.73	21.73	21.73	21.73	21.73	21.73	21.73	21.73	19.82	19.82	19.66	19.66	19.66	19.66	19.66	19.66	14.49
	Information Assets		Util Pump Safety Sensor Output	Util Pump Safety Command	Util Storage Safety Sensor Output	Util Storage Safety Command	Util Separators Control Sensor Outp	Util Separators Control Command	Util Compressors Safety Sensor Ou	Util Compressors Safety Command	Load Test Outcome (pass, fail)	HPU Pump Safety Sensor Output	HPU Pump Safety Command	HPU Fired Heater Safety Sensor O	HPU Fired Heater Safety Comman	HPU Special Safety Sensor Output	HPU Special Safety Command	HPU Compressors Safety Sensor C	HPU Compressors Safety Comman	Util Fired Heater Safety Sensor Out	Util Fired Heater Safety Command	Util Fired Heater Control Sensor Ou	Util Fired Heater Control Command	Util Electrical Safety Sensor Output	Util Electrical Safety Command	Util Pump Control Sensor Output	Util Pump Control Command	Util Storage Control Sensor Output	Util Storage Control Command	Util Compressors Control Sensor O	Util Compressors Control Command	HPU Pump Control Sensor Output
1	Acquire Natural Gas	4.557																														
2	Acquire Water	4.557																														
3	Receive Caustic	3.493																														
4	Acquire Electrical Power	3.303																						6	6							
5	Quality Test During Loading	2.607									6																					
6	Impurity Removal	2.587	4	4	4	4	4	4	4	4																2	2	2	2	2	2	
7	Blend & Load Lube Oils	2.159									4																					
8	Perform Fractional Distillation	1.811	6	6	4	4	4	4	4	4		6	6	6	6	6	6	6	6	6	6	6	6			4	4	4	4	4	4	4
9	Perform Hydrotreating	1.811	6	6	4	4	4	4	4	4		6	6	6	6	6	6	6	6	6	6	6	6			4	4	4	4	4	4	4
10	Quality Test During Processing	1.811																														
11	Load Other Products	1.652																														
12	Unload & Store Crude	1.303																														
13	Bill for Product	0.905																														
14	Acceptance Test Crude	0.557																														

Asset Impact from Loss of Node:

0 = No Impact on Asset

2 = Asset Available Using Work Around

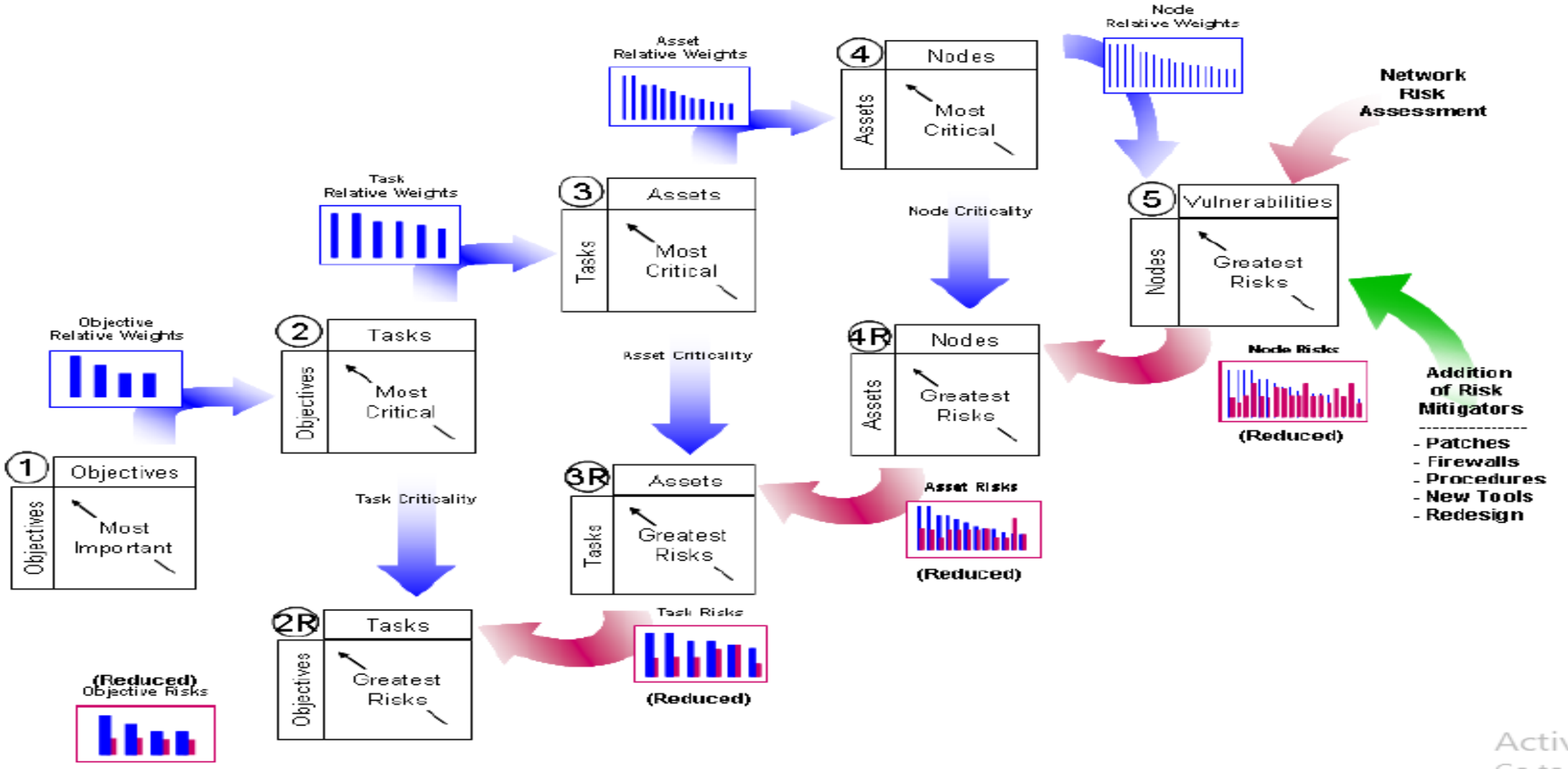
4 = Availability Degraded Even With Work Around

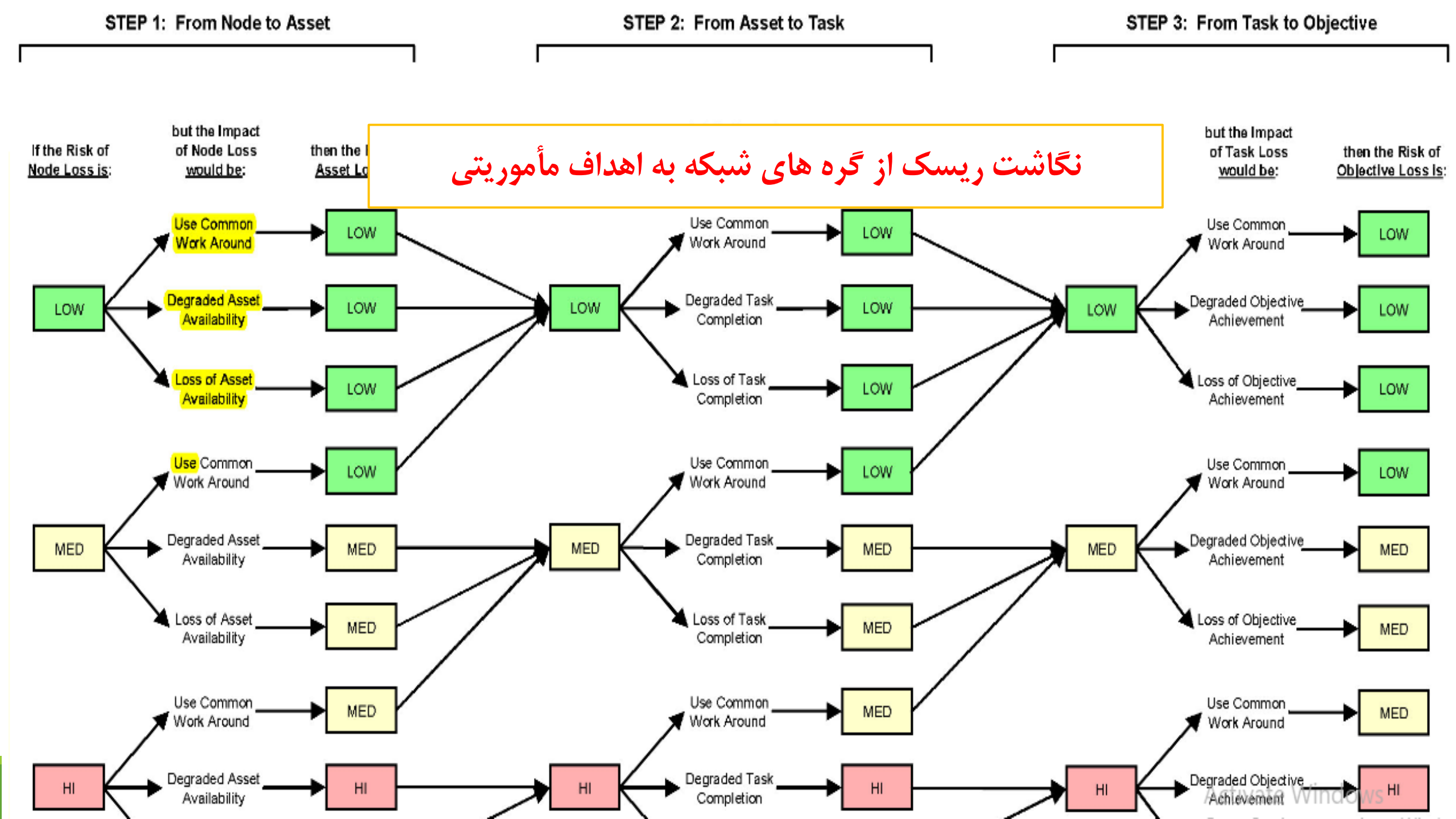
6 = Asset No

ماتریس ٤- وزن نسبی گره های شبکه براساس بحرانی بودن آن ها برای دارایی های اطلاعاتی

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
		Node Rel Wt	3,059	2,541	2,541	1,791	1,730	1,730	1,730	1,529	1,529	1,529	1,529	1,529	1,416	1,258	1,155	956	951	811	811	811	811	811	811	811	811	783	686	683	629	623
		Net	Network Interface	PLC Config Server	OPC Server	< brand z > Server 2	< brand x > Server	< brand x > Operator S	< brand x > Operator	Work Station 2	Printer 2	DCS Switch 1	DCS Switch 2	DCS Comm Processo	Work Station 3	Work Station 1	DCS Control Processo	< brand x > PLC 4	DCS Control Processo	< brand y > Operator	< brand y > Operator	< brand y > Operator	< brand y > Operator	< brand y > Operator	< brand y > Engineeri	< brand y > App Statio	Comm Processor	Plant LAN Router	DCS Control Processo	< brand x > PLC 5	Printer 1	DCS Control Processor 1
	Information Assets	Asset Rel Wt																														
1	Util Pump Safety Sensor Output	32.08		4	4	2	4	4	4																				6		
2	Util Pump Safety Command	32.08		4	4	2	4	4	4																				6		
3	Util Storage Safety Sensor Output	24.84		4	4	2	4	4	4																				6		
4	Util Storage Safety Command	24.84		4	4	2	4	4	4																				6		
5	Util Separators Control Sensor Output	24.84	4							2	2	2	2	2		4	6													2	
6	Util Separators Control Command	24.84	4							2	2	2	2	2		4	6													2	
7	Util Compressors Safety Sensor Output	24.84		4	4	2														4	4	4	4	4	4	4	4				
8	Util Compressors Safety Command	24.84		4	4	2														4	4	4	4	4	4	4	4				
9	Load Test Outcome (pass, fail)	24.28																										2			
10	HPU Pump Safety Sensor Output	21.73		4	4	2	4	4	4									6													
11	HPU Pump Safety Command	21.73		4	4	2	4	4	4									6													
12	HPU Fired Heater Safety Sensor Output	21.73		4	4	2	4	4	4									6													
13	HPU Fired Heater Safety Command	21.73		4	4	2	4	4	4									6													
14	HPU Special Safety Sensor Output	21.73		4	4	2	4	4	4									6													
15	HPU Special Safety Command	21.73		4	4	2	4	4	4									6													
16	HPU Compressors Safety Sensor Output	21.73		4	4	2														4	4	4	4	4	4	4	4				
17	HPU Compressors Safety Command	21.73		4	4	2														4	4	4	4	4	4	4	4				
18	Util Fired Heater Safety Sensor Output	21.73		4	4	2														4	4	4	4	4	4	4	4				
19	Util Fired Heater Safety Command	21.73		4	4	2														4	4	4	4	4	4	4	4				
20	Util Fired Heater Control Sensor Output	21.73	4							2	2	2	2	2															6		
21	Util Fired Heater Control Command	21.73	4							2	2	2	2	2															6		
22	Util Electrical Safety Sensor Output	19.82		4	4	2														4	4	4	4	4	4	4	4				
23	Util Electrical Safety Command	19.82		4	4	2														4	4	4	4	4	4	4	4				
24	Util Pump Control Sensor Output	19.66	4							2	2	2	2	2		4	6													2	
25	Util Pump Control Command	19.66	4							2	2	2	2	2		4	6													2	
26	Util Storage Control Sensor Output	19.66	4							2	2	2	2	2	4				6												
27	Util Storage Control Command	19.66	4							2	2	2	2	2	4				6												
28	Util Compressors Control Sensor Output	19.66	4							2	2	2	2	2		4	6													2	
29	Util Compressors Control Command	19.66	4							2	2	2	2	2		4	6													2	
30	HPU Pump Control Sensor Output	14.49	4							2	2	2	2	2	4																

خلاصه ای از متدلوژی RiskMAP [5]




STEP 1: From Node to Asset
STEP 2: From Asset to Task
STEP 3: From Task to Objective
If the Risk of Node Loss is:
but the Impact of Node Loss would be:
but the Impact of Task Loss would be:
then the Risk of Objective Loss is:
نگاشت ریسک از گره های شبکه به اهداف مأموریتی
LOW
MED
HI
Use Common Work Around
Degraded Asset Availability
Loss of Asset Availability
Degraded Task Completion
Loss of Task Completion
Degraded Objective Achievement
Loss of Objective Achievement

Risk of Node Loss:

1 = Low

3 = Medium

5 = High

ماتریس ۵- تخصیص سطح ریسک به گره های شبکه براساس آسیب پذیری های آن ها

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
			Vulnerability 5	Vulnerability 3	Vulnerability 13	Vulnerability 1	Vulnerability 2	Vulnerability 27	Vulnerability 22	Vulnerability 6	Vulnerability 10	Vulnerability 11	Vulnerability 14	Vulnerability 7	Vulnerability 15	Vulnerability 18	Vulnerability 12	Vulnerability 19	Vulnerability 20	Vulnerability 23	Vulnerability 24	Vulnerability 28	Vulnerability 4	Vulnerability 8	Vulnerability 16	Vulnerability 21	Vulnerability 29	
	Network Nodes	Node Rel Wt																										Max Node Risk
1	Network Interface	3,059	5	3		1																						5
2	PLC Config Server	2,541					1																					1
3	OPC Server	2,541					1																					1
4	< brand z > Server 2	1,791				3				3																		3
5	< brand x > Server	1,730			5		1						3	1									1					5
6	< brand x > Operator Station 1	1,730												1	1								1					1
7	< brand x > Operator Station 2	1,730									3	3			1													3
8	Work Station 2	1,529							1					1		3	1	3						1				3
9	Printer 2	1,529													1		1		1					1	1			1
10	DCS Switch 1	1,529																	1						1			1
11	DCS Switch 2	1,529							3								1			3								3
12	DCS Comm Processor	1,529																	1		1					1		1
13	Work Station 3	1,416																			1					1		1
14	Work Station 1	1,258						5														3						5
15	DCS Control Processor 9	1,155																			1						1	1
16	< brand x > PLC 4	958																									1	1

Risk of Asset Loss:

1 = Low

3 = Medium

5 = High

ماتریس 4R- نگاشت ریسک گره های شبکه به ریسک دارایی ها

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
		Max Node Risk	5	1	1	3	5	1	3	3	1	1	3	1	1	5	1	1		1	1											
		Nodes	Network Interf	PLC Config Se	OPC Server	< brand z > Se	< brand x > Se	< brand x > Op	< brand x > Op	Work Station 2	Printer 2	DCS Switch 1	DCS Switch 2	DCS Comm P	Work Station 3	Work Station 4	DCS Control F	< brand x > P	DCS Control F	< brand y > O	< brand y > O	< brand y > O	< brand y > O	< brand y > O	< brand y > O	< brand y > E	< brand y > A	Comm Processor	Plant LAN Router	DCS Control Processor 2	< brand x > PLC 5	Printer 1	DCS Control Processor 1
	Information Assets	Max Asset Risk																														
1	Util Pump Safety Sensor Output	5		1	1	1	5	1	3																							
2	Util Pump Safety Command	5		1	1	1	5	1	3																							
3	Util Storage Safety Sensor Output	5		1	1	1	5	1	3																							
4	Util Storage Safety Command	5		1	1	1	5	1	3																							
5	Util Separators Control Sensor Output	5	5							1	1	1	1	1		5	1															
6	Util Separators Control Command	5	5							1	1	1	1	1		5	1															
7	Util Compressors Safety Sensor Output	1		1	1	1														1	1											
8	Util Compressors Safety Command	1		1	1	1														1	1											
9	Load Test Outcome (pass, fail)																															
10	HPU Pump Safety Sensor Output	5		1	1	1	5	1	3									1														
11	HPU Pump Safety Command	5		1	1	1	5	1	3									1														
12	HPU Fired Heater Safety Sensor Output	5		1	1	1	5	1	3									1														
13	HPU Fired Heater Safety Command	5		1	1	1	5	1	3									1														
14	HPU Special Safety Sensor Output	5		1	1	1	5	1	3									1														
15	HPU Special Safety Command	5		1	1	1	5	1	3									1														
16	HPU Compressors Safety Sensor Output	1		1	1	1														1	1											
17	HPU Compressors Safety Command	1		1	1	1														1	1											
18	Util Fired Heater Safety Sensor Output	1		1	1	1														1	1											
19	Util Fired Heater Safety Command	1		1	1	1														1	1											
20	Util Fired Heater Control Sensor Output	5	5							1	1	1	1	1																		
21	Util Fired Heater Control Command	5	5							1	1	1	1	1																		
22	Util Electrical Safety Sensor Output	1		1	1	1														1	1											
23	Util Electrical Safety Command	1		1	1	1														1	1											
24	Util Pump Control Sensor Output	5	5							1	1	1	1	1		5	1															
25	Util Pump Control Command	5	5							1	1	1	1	1		5	1															
26	Util Storage Control Sensor Output	5	5							1	1	1	1	1	1																	
27	Util Storage Control Command	5	5							1	1	1	1	1	1																	
28	Util Compressors Control Sensor Output	5	5							1	1	1	1	1		5	1															
29	Util Compressors Control Command	5	5							1	1	1	1	1		5	1															
30	HPU Pump Control Sensor Output	5	5							1	1	1	1	1	1																	

Risk of Task Loss:

1 = Low

3 = Medium

5 = High

ماتریس 3R- نگاشت ریسک دارایی ها به ریسک وظایف

			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
		Max Asset Risk	5	5	5	5	5	5	1	1		5	5	5	5	5	5	1	1	1	1	5	5	1	1	5	5	5	5	5	5	5
		Information A	Util Pump Safety Sensor Outp	Util Pump Safety Command	Util Storage Safety Sensor Ou	Util Storage Safety Command	Util Separators Control Senso	Util Separators Control Comm	Util Compressors Safety Sens	Util Compressors Safety Com	Load Test Outcome (pass, fai	HPU Pump Safety Sensor Ou	HPU Pump Safety Command	HPU Fired Heater Safety Sen	HPU Fired Heater Safety Com	HPU Special Safety Sensor O	HPU Special Safety Comman	HPU Compressors Safety Se	HPU Compressors Safety Co	Util Fired Heater Safety Sens	Util Fired Heater Safety Comm	Util Fired Heater Control Sens	Util Fired Heater Control Com	Util Electrical Safety Sensor C	Util Electrical Safety Comman	Util Pump Control Sensor Out	Util Pump Control Command	Util Storage Control Sensor Output	Util Storage Control Command	Util Compressors Control Sensor Output	Util Compressors Control Command	HPU Pump Control Sensor Output
	Tasks	Max Task Risk																														
1	Acquire Natural Gas																															
2	Acquire Water																															
3	Receive Caustic	1																														
4	Acquire Electrical Power	3																						1	1							
5	Quality Test During Loading																															
6	Impurity Removal	5	5	5	5	5	5	5	1	1																3	3	3	3	3	3	
7	Blend & Load Lube Oils																															
8	Perform Fractional Distillation	5	5	5	5	5	5	5	1	1		5	5	5	5	5	5	1	1	1	1	5	5			5	5	5	5	5	5	5
9	Perform Hydrotreating	5	5	5	5	5	5	5	1	1		5	5	5	5	5	5	1	1	1	1	5	5			5	5	5	5	5	5	5
10	Quality Test During Processing																															
11	Load Other Products	3																														
12	Unload & Store Crude	3																														
13	Bill for Product																															
14	Acceptance Test Crude																															

ماتریس 2R- نگاشت ریسک وظایف به ریسک اهداف مأموریتی

Risk of Business Objective Loss:

1 = Low

3 = Medium

5 = High

			1	2	3	4	5	6	7	8	9	10	11	12	13	14
		Max Task Risk			1	3		5		5	5		3	3		
		Task	Acquire Natural Gas	Acquire Water	Receive Caustic	Acquire Electrical Power	Quality Test During Loading	Impurity Removal	Blend & Load Lube Oils	Perform Fractional Distillation	Perform Hydrotreating	Quality Test During Processing	Load Other Products	Unload & Store Crude	Bill for Product	Acceptance Test Crude
	Business Objective	Max Obj. Risk														
1	Stay safe	5			1	1		5								
2	Stay profitable	5			1	3				5	5		1	1		
3	Stay in compliance	5			1	3		5					1	1		
4	Supply customers well	5			1	3				5	5		3	1		
5																

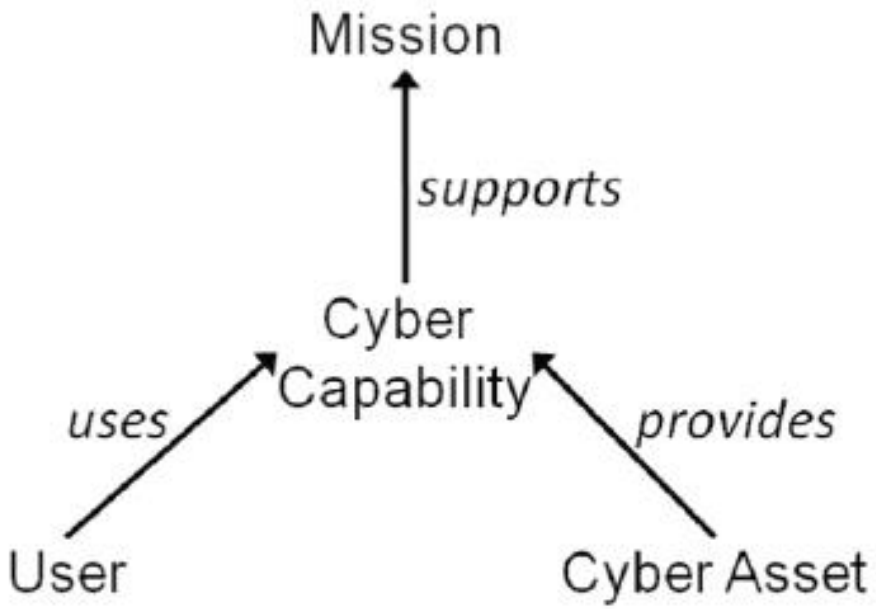
ایجاد خودکار و مبتنی بر آنتولوژی درخت وابستگی [5]

- خودکار نمودن نگاشت دارایی های سایبری به مأموریت ها
- طراحی عناصر، روابط و ویژگی های آن ها توسط متخصصـان و ایجـاد دیـاگرام ERA
- تبدیل ERA ایجاد شده به آنتولوژی
- ترکیب آنتولوژی های مختلف برای ایجاد درخت وابستگی کامل
- طراحی ابزارهایی همچون CAMUS, PCAMM

آنتولوژی [6]

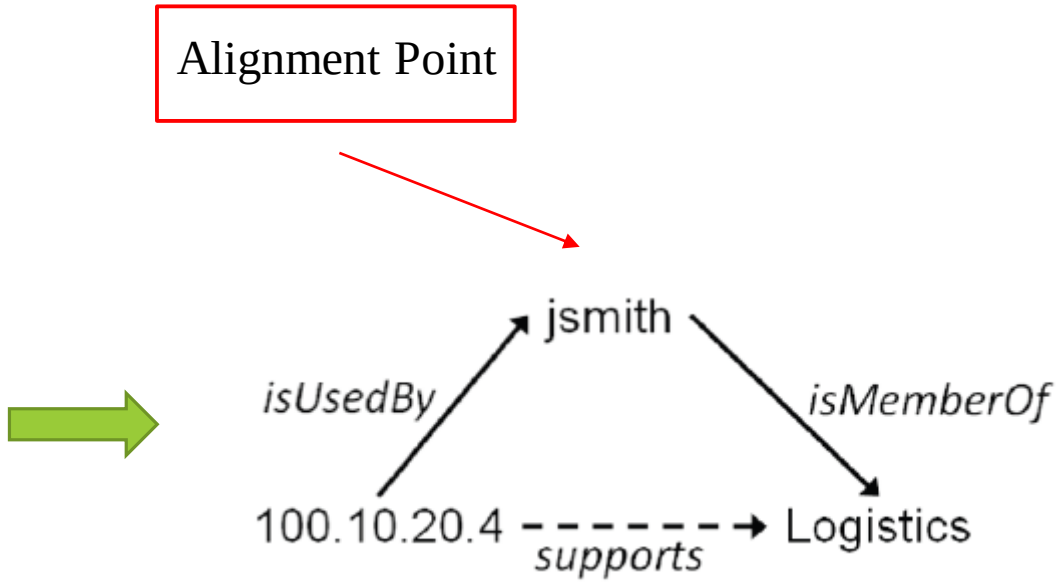
- مطالعه در رابطه با موجودیت اشیا در جهان و ارتباطاتی که آنها با یکدیگر دارند.
- موجودیت به چیزی می گوییم که وجود دارد. این موجودیت مـی توانـد انتزاعـی یـا واقعی، فیزیکی یا غیر فیزیکی باشد.
- شامل جزئیات ساختار سلسله مراتبی اشیا می شود.
- در رابطه با دسته بندی اشیا با توجه به شباهت و تفاوت های آنها نسبت به یکـدیگر صحبت می کند.

ابزار CAMUS [6]



ابزار CAMUS [6]

FTP Log	LDAP query
… jsmith@100.10.20.4 …	…jsmith|Logistics…
… sjones@100.10.20.6 …	…llaurel|Adminstrative…
… llaurel@100.10.20.9 …	…sjones|Finance…
…	…



ابزار CAMUS [6]

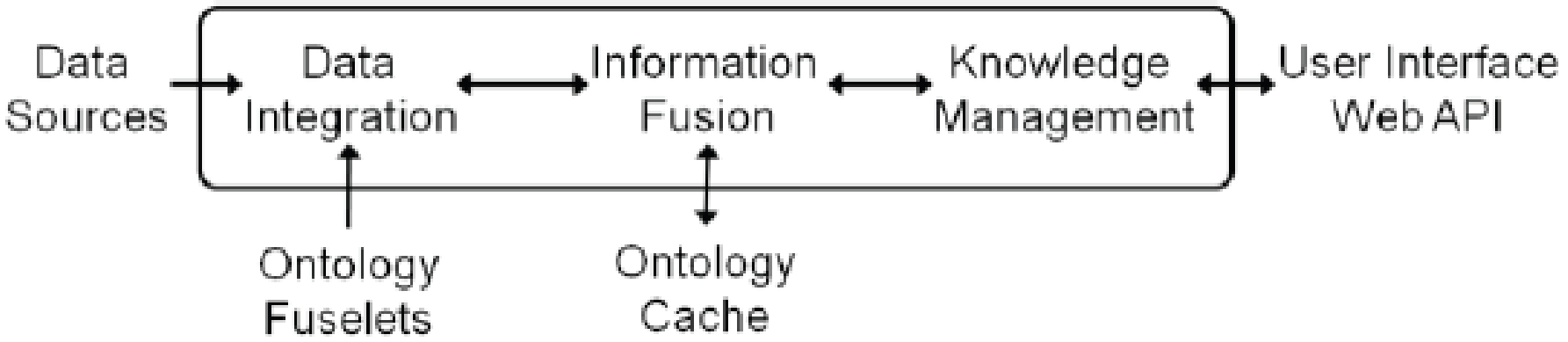
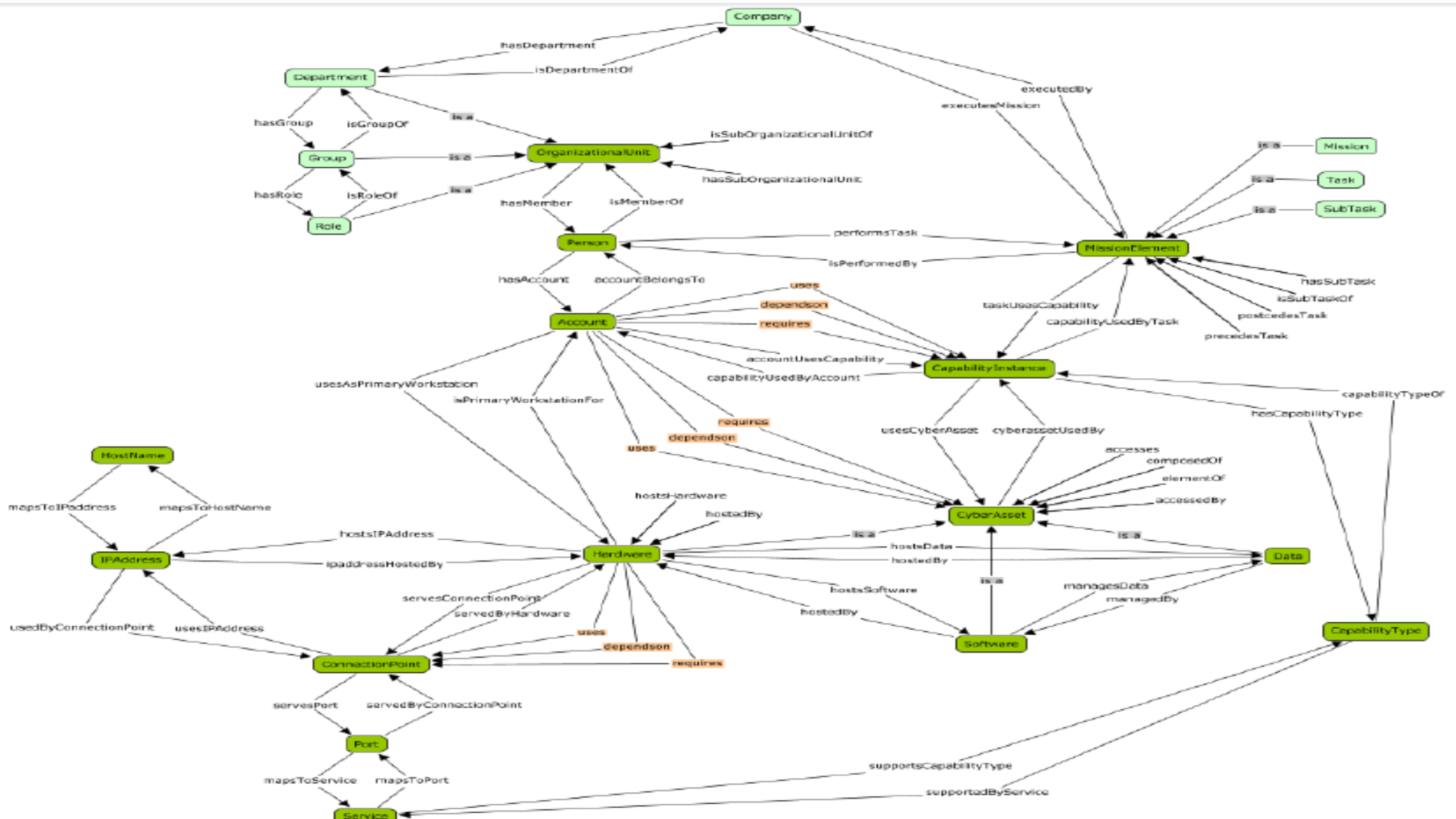


TABLE I. FOUNDATION ONTOLOGY: RESOURCES

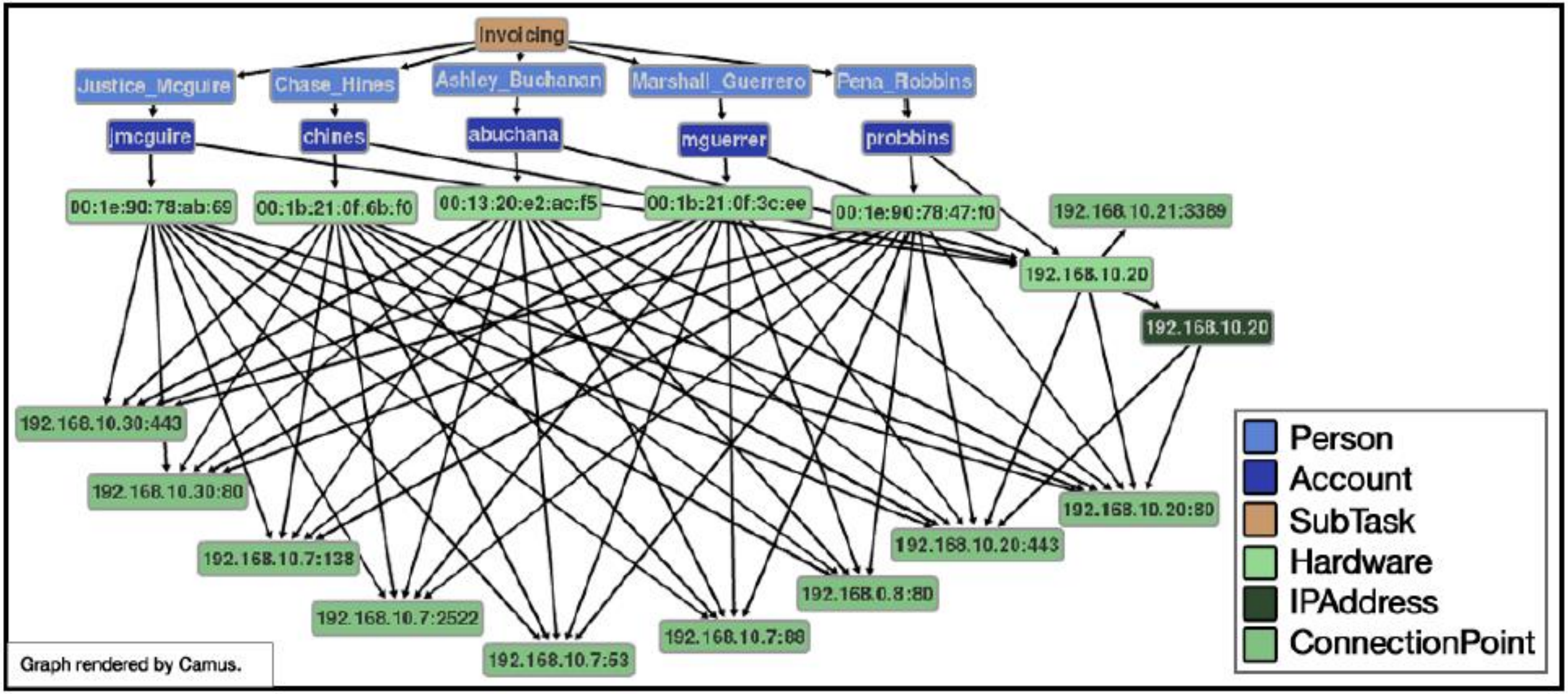
Resource	Type	Description
OrganizationalUnit	User	A collection of User related resources. An OrganizationalUnit can contain other OrganizationalUnits
Person	User	A single human resource
Account	User	A single identity on a cyber resource
MissionElement	Mission	A single tasking element
CapabilityInstance	Capability	A single instance of the ability to execute a specific action
CapabilityType	Capability	A classification of abilities to perform an action
CyberAsset	Asset	A non-human resource accessible from the network
Hardware	Asset	A physical computing device, element of a computing device, or peripheral of a computing device
Software	Asset	A program that performs a specific function directly for a user or system
Data	Asset	Distinct pieces of digital information that have been formatted a specific way
HostName	Asset	A label assigned to a computing device on a network
IPAddress	Asset	An Internet Protocol address
ConnectionPoint	Asset	A pairing of a specific IP address and Port for the purposes of communication
Port	Asset	A port number associated with a communication endpoint used by the Internet Protocol suite
Service	Asset	A software capability or process typically associated with a Port

TABLE II. FOUNDATION ONTOLOGY: PROPERTIES

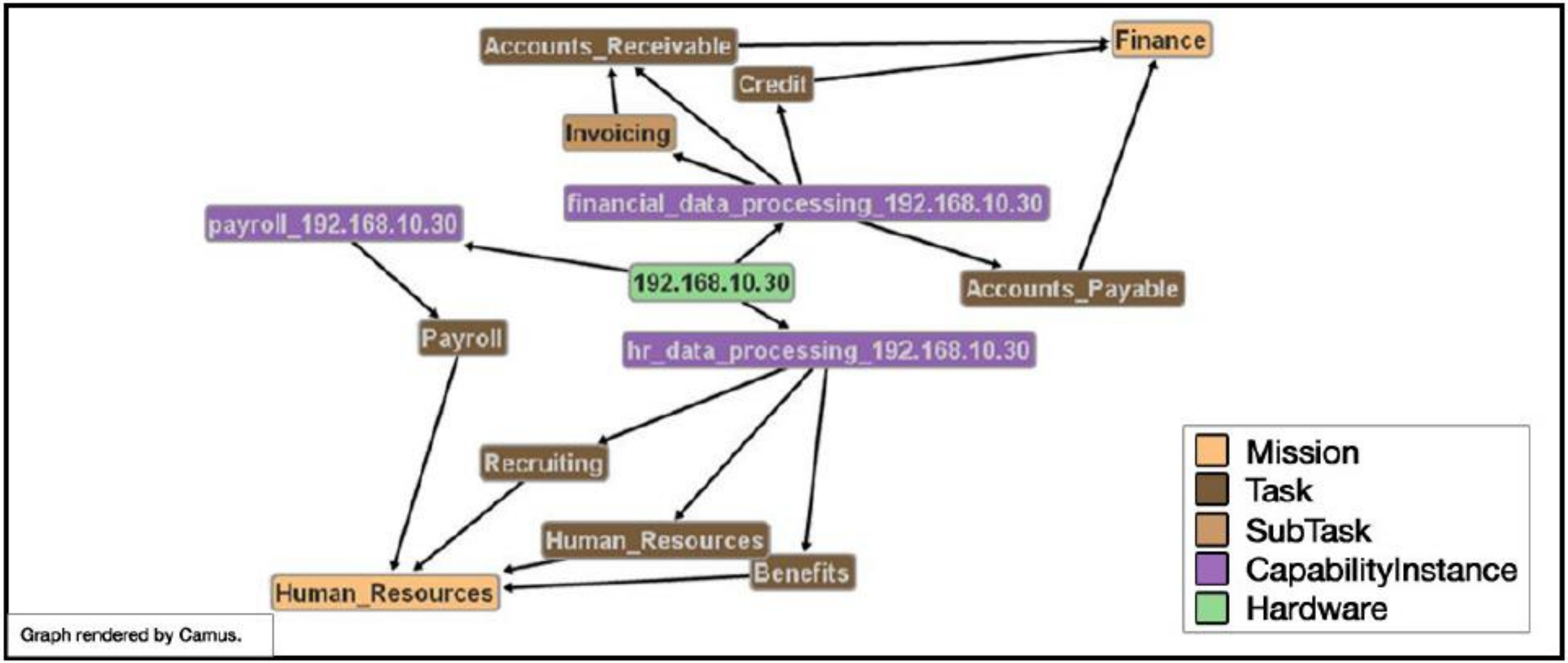
Property	Relates
HasSubOrganizationalUnit	OrganizationalUnit->OrganizationalUnit
isSubOrganizationalUnitOf	OrganizationalUnit->OrganizationalUnit
hasMember	OrganizationalUnit->Person
isMemberOf	Person-> OrganizationalUnit
has Account	Person->Account
accountBelongsTo	Account->Person
hasSubTask	MissionElement->MissionElement
isSubTaskOf	MissionElement->MissionElement
precedesTask	MissionElement->MissionElement
postcedesTask	MissionElement->MissionElement
performsTask	Person->MissionElement
isPerformedBy	MissionElement->Person
taskUsesCapability	MissionElement->CapabilityInstance
capabilityUsedByTask	CapabilityInstance->MissionElement
accountUsesCapability	Account-> CapabilityInstance
capabilityUsedByAccount	CapabilityInstance->Account
usesCyberAsset	CapabilityInstance->CyberAsset
cyberAssetUsedBy	CyberAsset-> CapabilityInstance
hostsIPAddress	Hardware->IPAddress
ipaddressHostedBy	IPAddress->Hardware
hostsSoftware	Hardware->Software
softwareHostedBy	Software->Hardware
hostsData	Hardware->Data
dataHostedBy	Data->Hardware
managesData	Software->Data
dataManagedBy	Data->Software
mapsToIPAddress	HostName->IPAddress
mapsToHostName	IPAddress->HostName


Company
hasDepartment
isDepartmentOf
Department
executedBy
executesMission
hasGroup
isGroupOf
is a
isSubOrganizationalUnitOf
Group
OrganizationalUnit
hasSubOrganizationalUnit
is a
Mission
is a
Task
is a
SubTask
hasRole
isRoleOf
is a
hasMember
isMemberOf
Role
Person
performsTask
isPerformedBy
MissionElement
hasSubTask
isSubTaskOf
precedesTask
postcedesTask
hasAccount
accountBelongsTo
uses
dependson
requires
Account
taskUsesCapability
capabilityUsedByTask
accountUsesCapability
capabilityUsedByAccount
CapabilityInstance
capabilityTypeOf
hasCapabilityType
usesAsPrimaryWorkstation
isPrimaryWorkstationFor
usesCyberAsset
cyberassetUsedBy
HostName
mapsToIPaddress
mapsToHostName
hostsHardware
hostedBy
accesses
composedOf
elementOf
accessedBy
CyberAsset
hostsIPAddress
ipaddressHostedBy
IPAddress
Hardware
is a
hostsData
hostedBy
Data
hostsSoftware
hostedBy
is a
managesData
managedBy
servesConnectionPoint
servedByHardware
usedByConnectionPoint
usesIPAddress
Software
CapabilityType
ConnectionPoint
servesPort
servedByConnectionPoint
Port
supportsCapabilityType
mapsToService
mapsToPort
supportedByService
Service

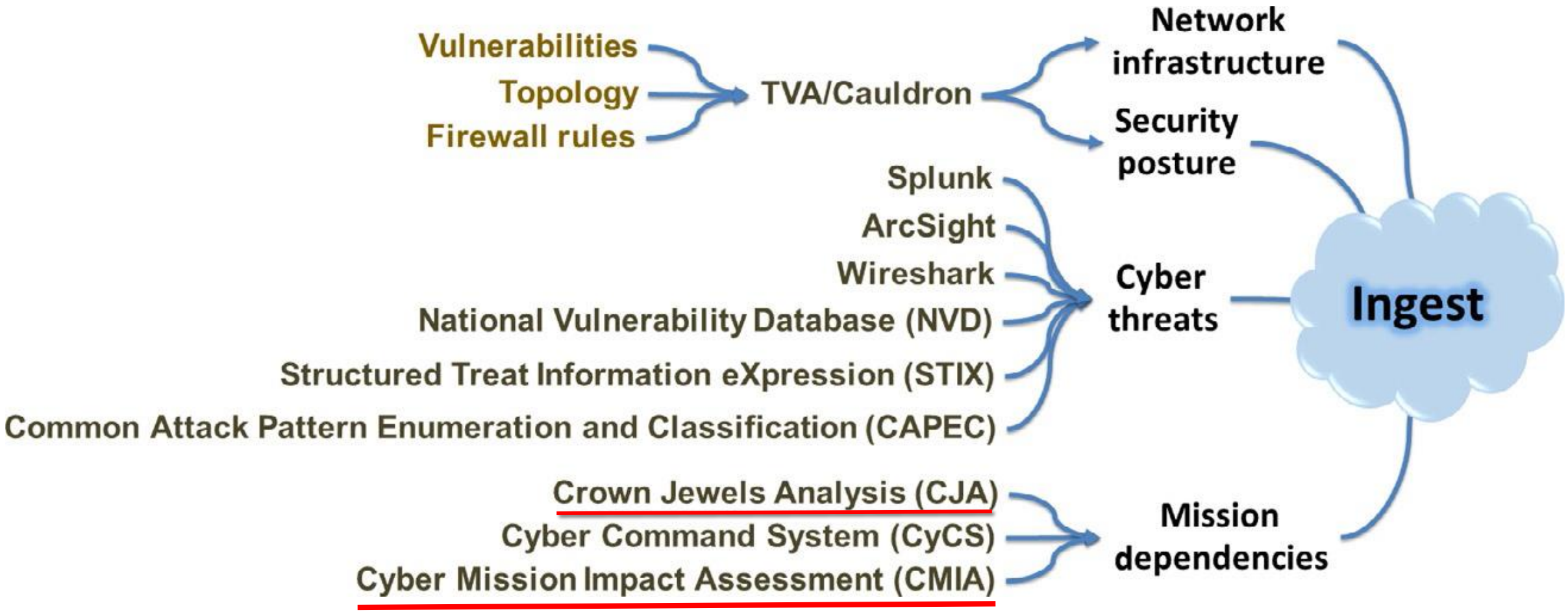
Example: “What is needed for the Invoicing Subtask?” [7]



What missions does the IP address 102.168.10.30 support?[7]



نمونه ای از منابع داده مورد استفاده در CyGraph [3]

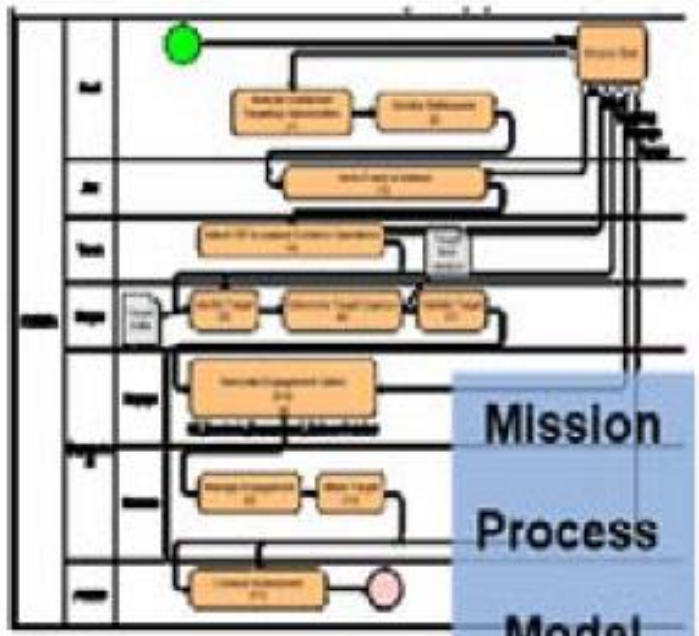


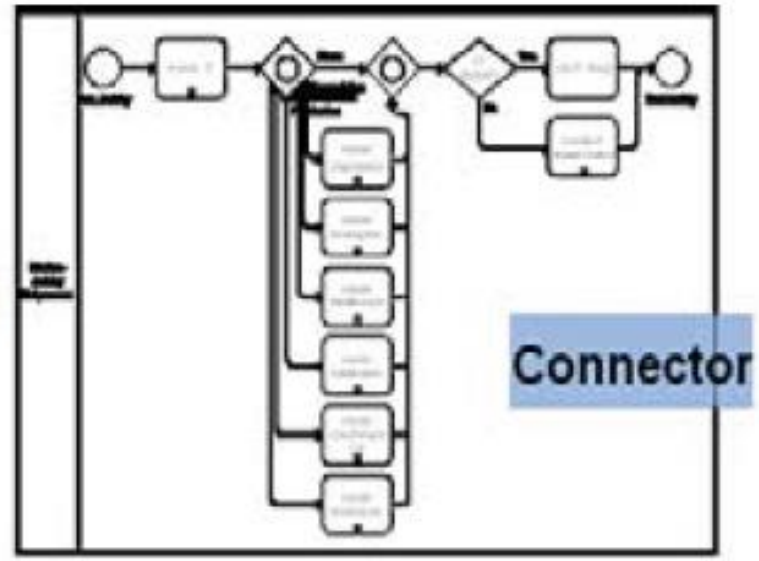
Mission Impact Assessment- MIA [8-11]

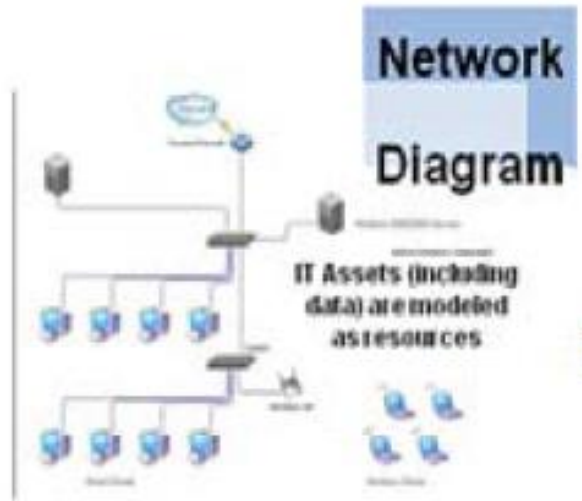
- در لایه وابستگی مأموریتی ابزار CyGraph، اثـر حمـلات سـایبری بـر روی مأموریـت هـا ارزیابی می شود.
- در این لایه، وابستگی های سلسله مراتبی بین مؤلفه های مأموریتی و دارایی هـای IT کـه آن ها را پشتیبانی می کنند بدست می آید. سپس، اثر حملات سایبری بر روی مأموریت هـا براساس وابستگی مأموریت ها به دارایی های IT، ارزیابی می شود.
- ابزار CMIA محیطی برای شبیه سازی حملات بر روی مأموریت ها و ارزیـابی اثـرات آن ها ارائه می دهد.

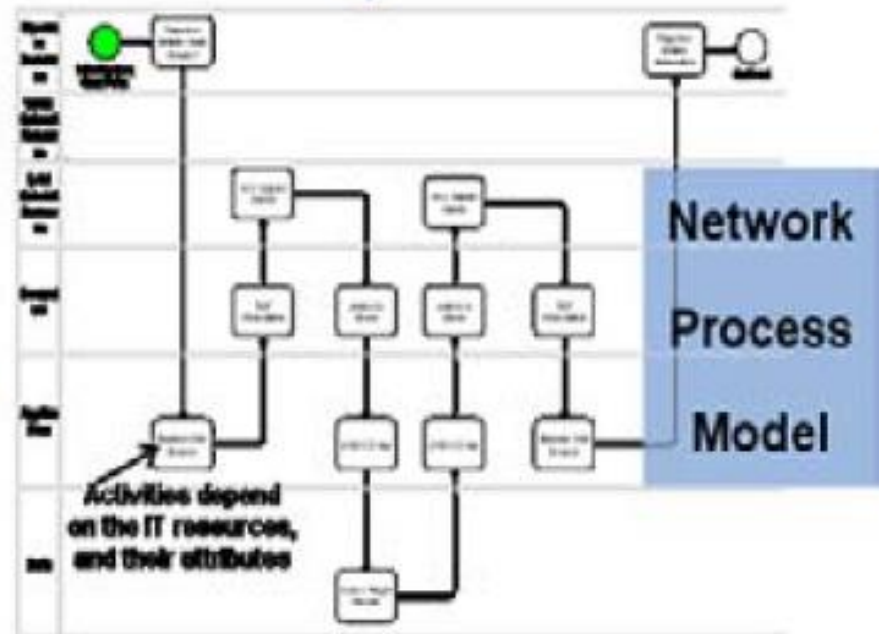
CMIA- Cyber Mission Impact Assessment [8-11]

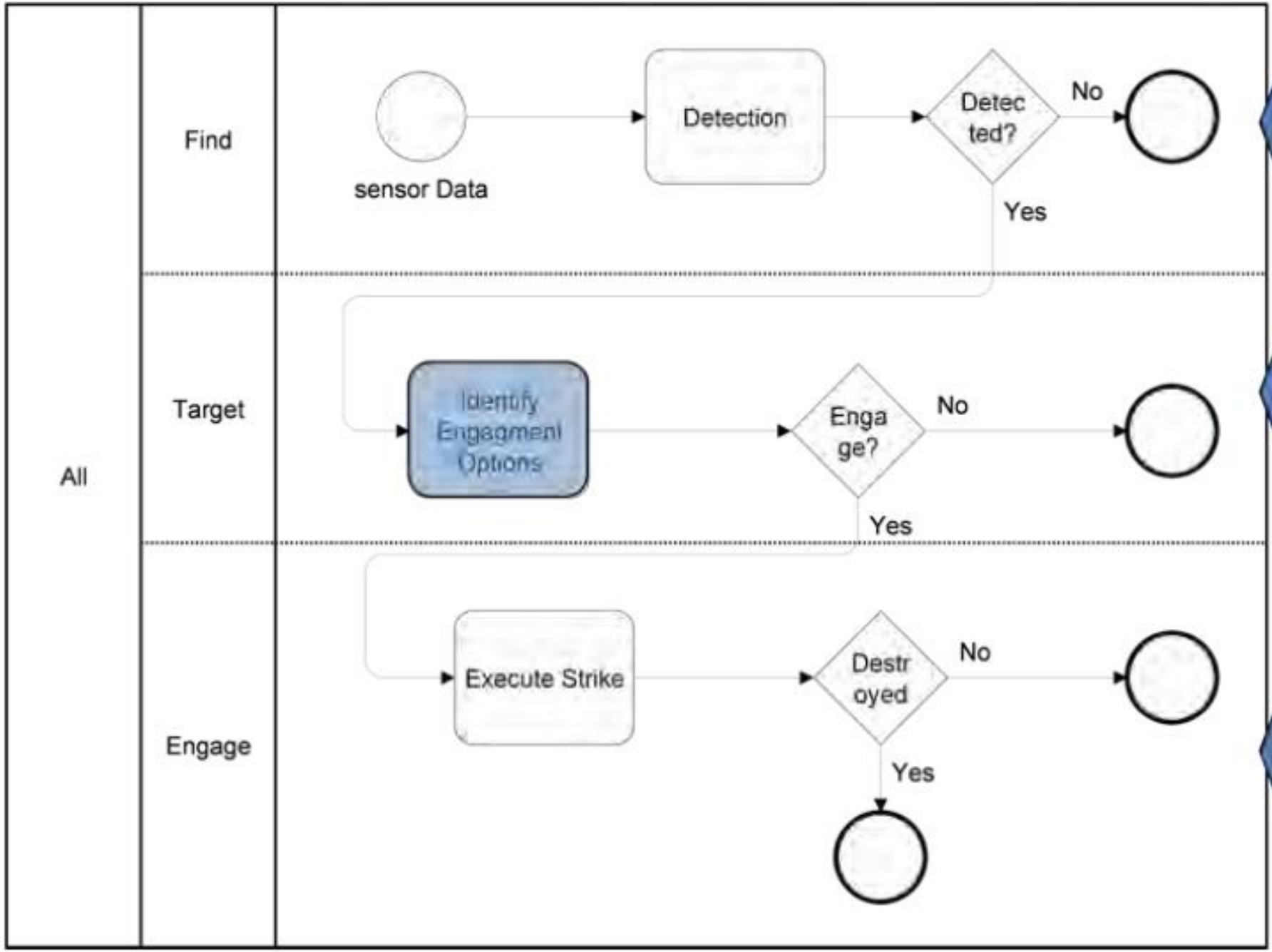
- شبیه سازی اثرات حمله بر روی مأموریت سیستم
- شناسایی دارایی های حیاتی (Crown Jewels)
- ارزیابی میزان حساسیت سیستم ها به اثرات مختلف حمله
- ارزیابی کارکرد روش های مقابله


Mission
Process
Model


Connector


Network
Diagram
IT Assets (including data) are modeled as resources

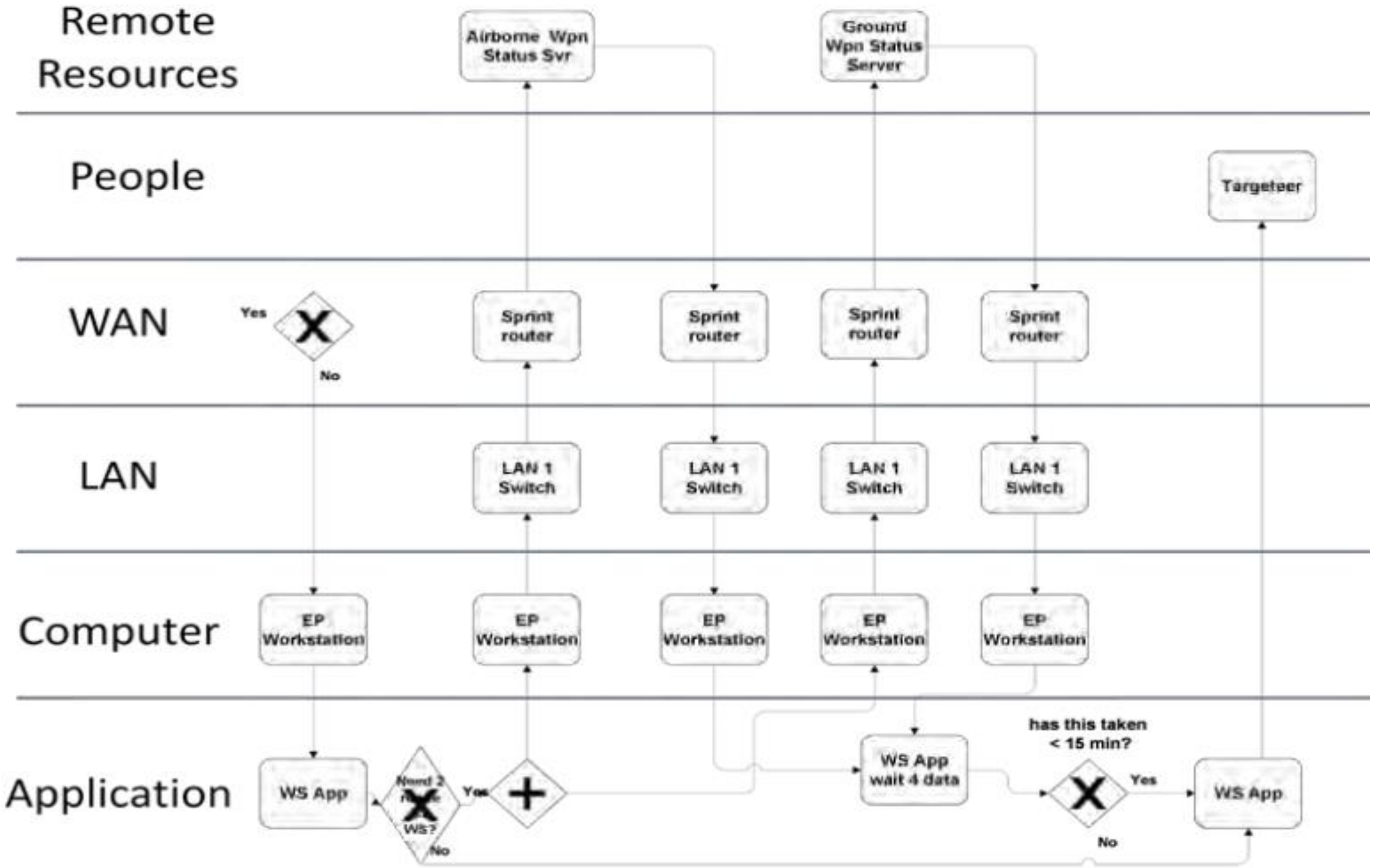

Network
Process
Model
Activities depend on the IT resources, and their attributes

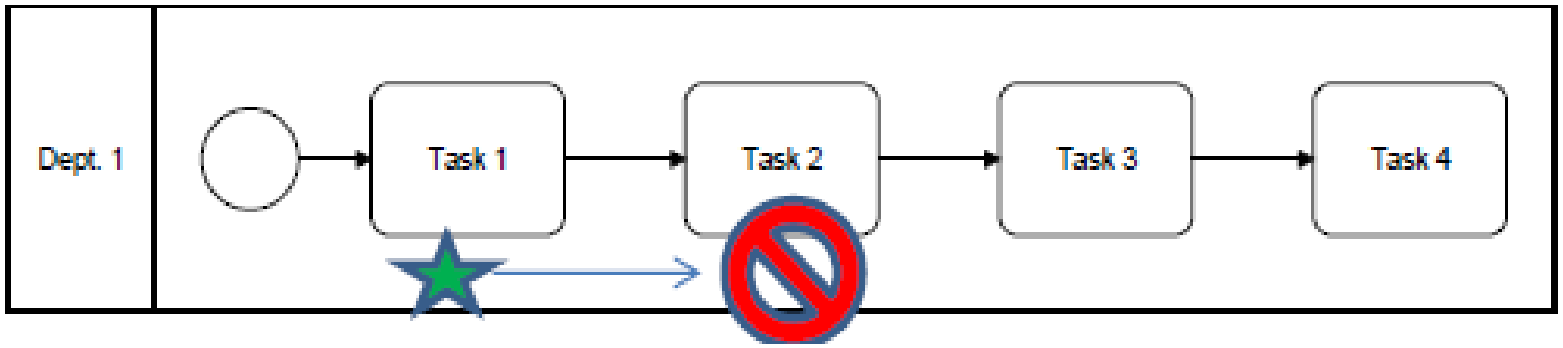


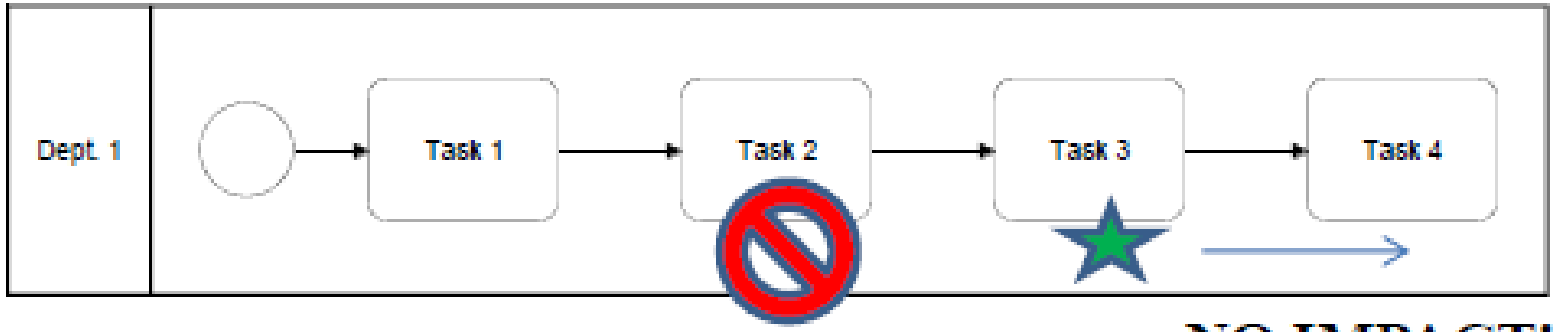
Sensors search the AOI, looking for targets.

Identify Engagement Options identifies the available weapons for engaging the target and selects the "best" one.

The actual strike is executed.

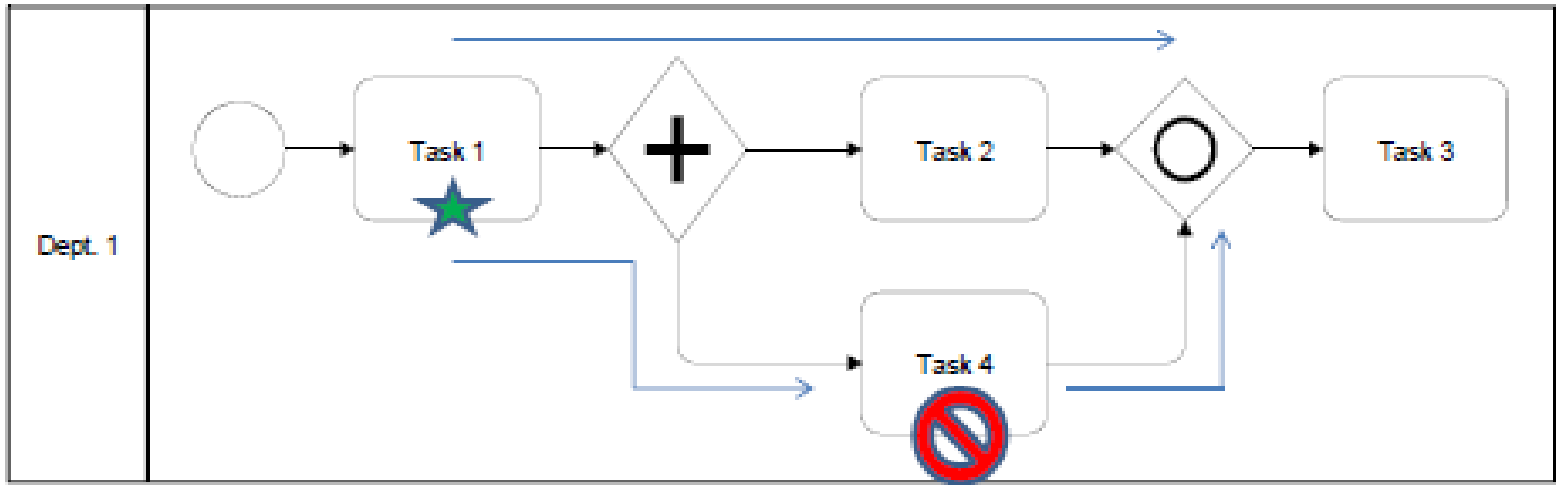

Remote Resources
People
WAN
LAN
Computer
Application
Airborne Wpn Status Svr
Ground Wpn Status Server
Targeteer
Yes
No
Sprint router
Sprint router
Sprint router
Sprint router
LAN 1 Switch
LAN 1 Switch
LAN 1 Switch
LAN 1 Switch
EP Workstation
EP Workstation
EP Workstation
EP Workstation
EP Workstation
WS App
Need 2
WS?
Yes
No
WS App wait 4 data
has this taken < 15 min?
Yes
No
WS App





NO IMPACT!

NO IMPACT



CMIA [8-11]

از آن جا که تمرکز اصلی رویکرد CMIA بر ارزیابی اثر بر روی مأموریت ها است، مدل ایجاد شده توسط این ابزار، شامل جزئیات بیشتری است که در سایر مدل های ارزیابی ریسک وجود ندارد. این جزئیات شامل موارد زیر است:

گردش کار: دنباله ای از وظایف تشکیل دهنده مأموریت

خط زمانی: مدت زمان انجام وظایف که می توان با مدت زمان انجام حمله مقایسه نمود.

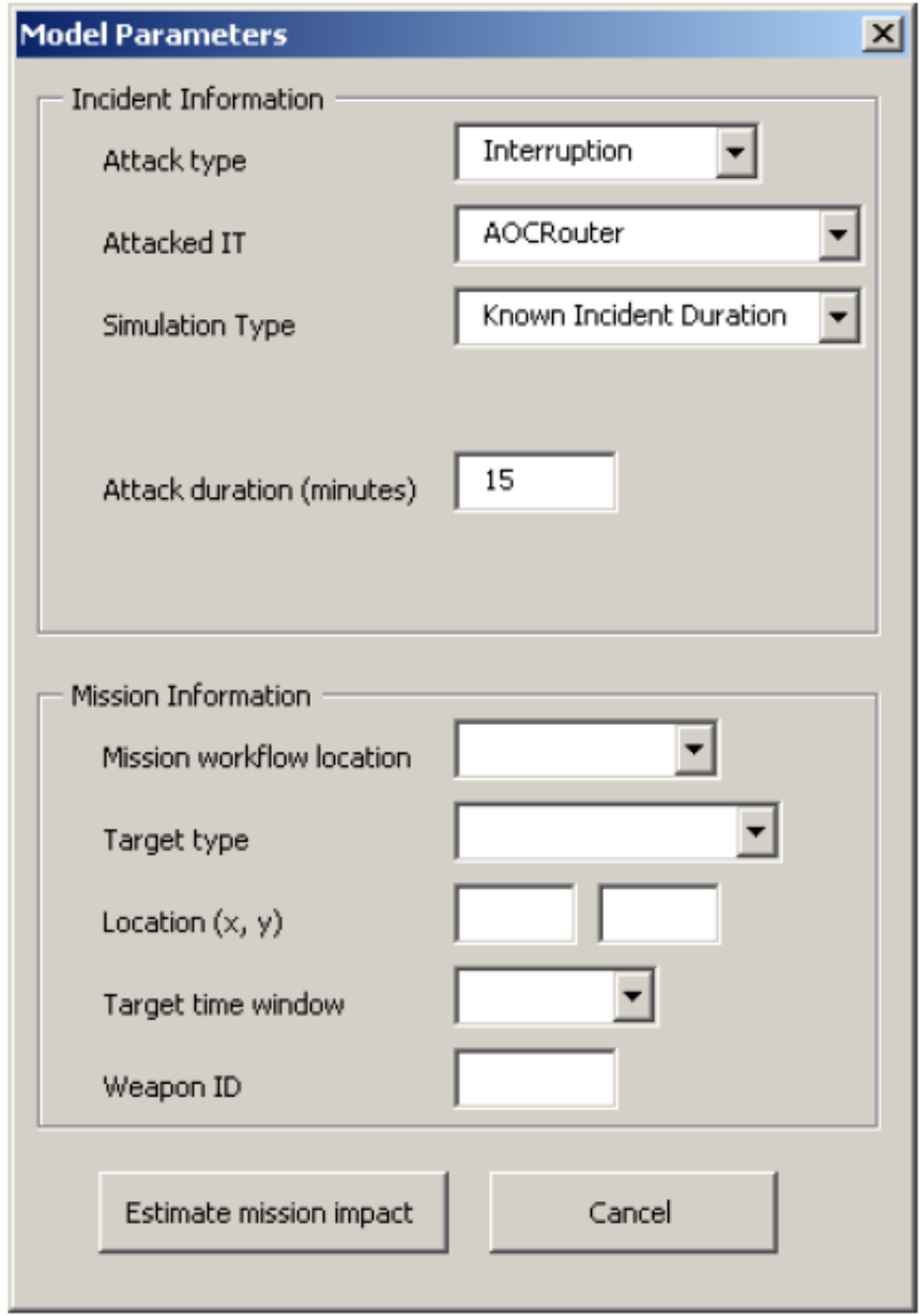
اثرات حمله: دسته بندی حملات سایبری به شش کلاس از اثرات سایبری

(Degradation, Interruption, Modification, Fabrication, Unauthorized Use, Interception).

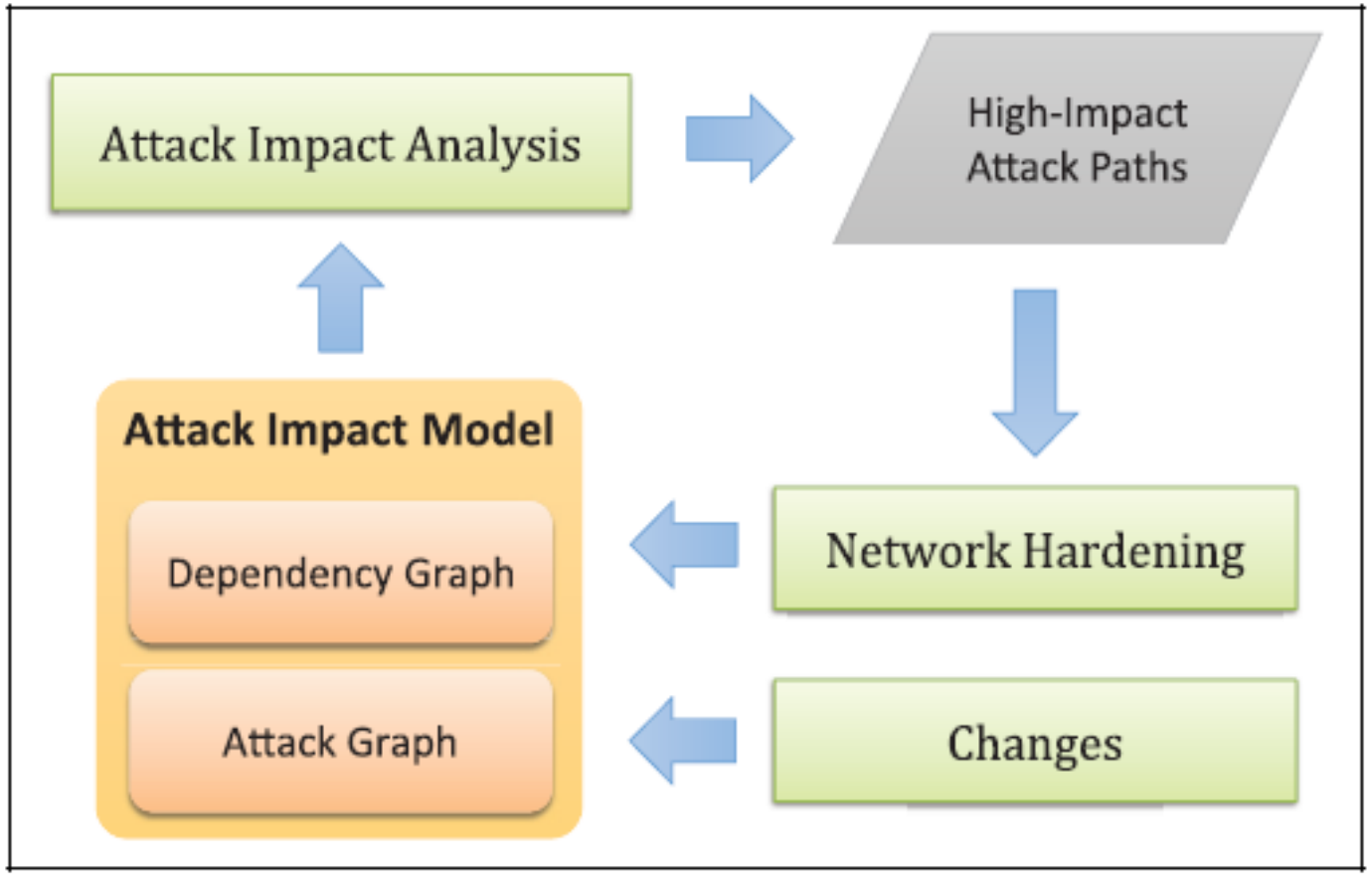
CMIA [8-11]

شبیه سازی حملات و ارزیابی اثرات آن ها

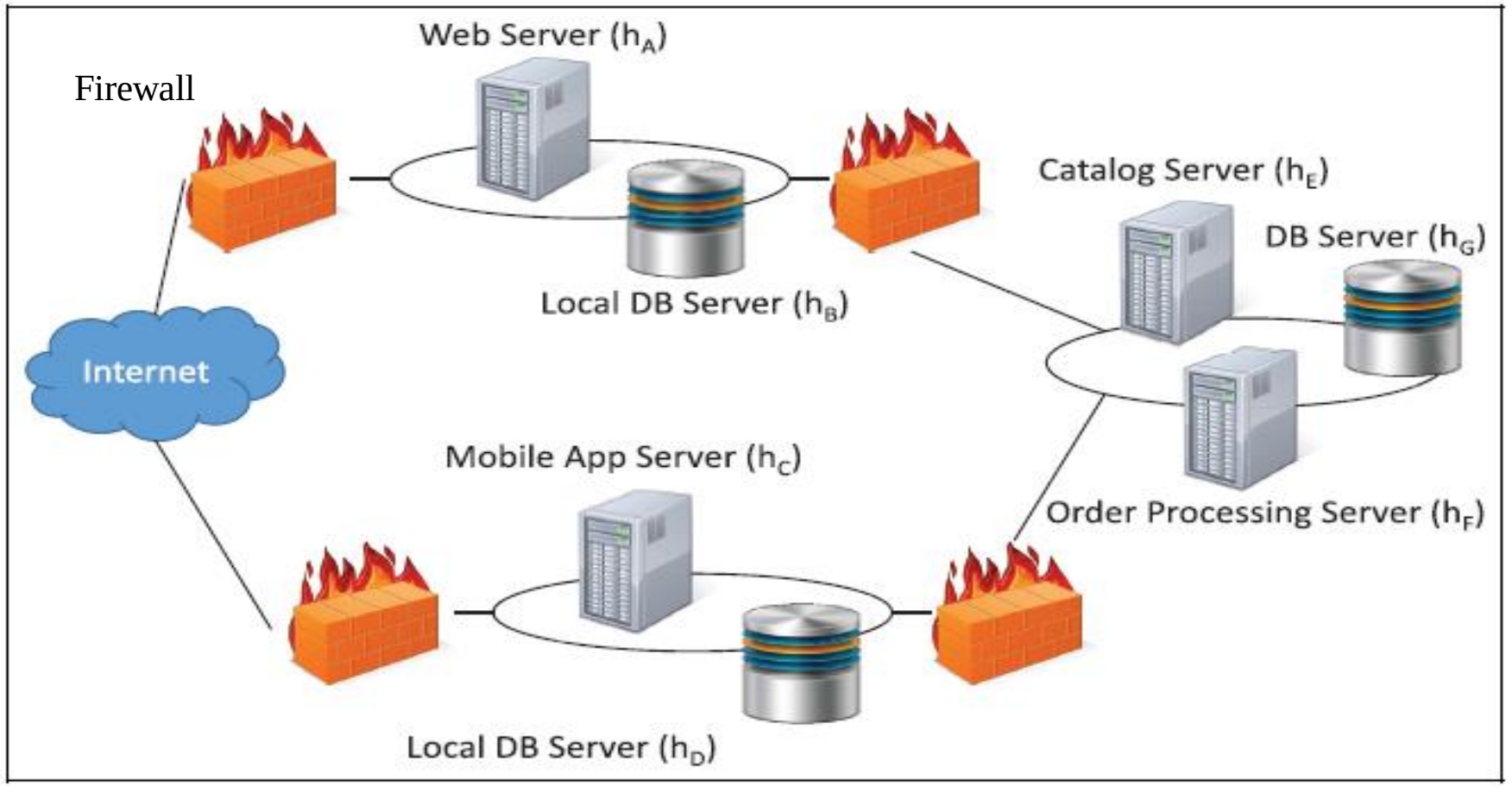
- هر منبع IT، دارای ویژگی هایی است که منعکس کننده این است که آیا منبع مـورد نظـر تحـت تاثیر رخداد سایبری قرار گرفته است یا خیر.
- اجرای مدل فرایند حمله به موازات مدل فرایند مأموریت
- نمایش هر فعالیت مأموریت وابسته به IT با وابستگی های خودش
- اندازه گیری پارامتر MoE با/ بدون اثرات حمله سایبری

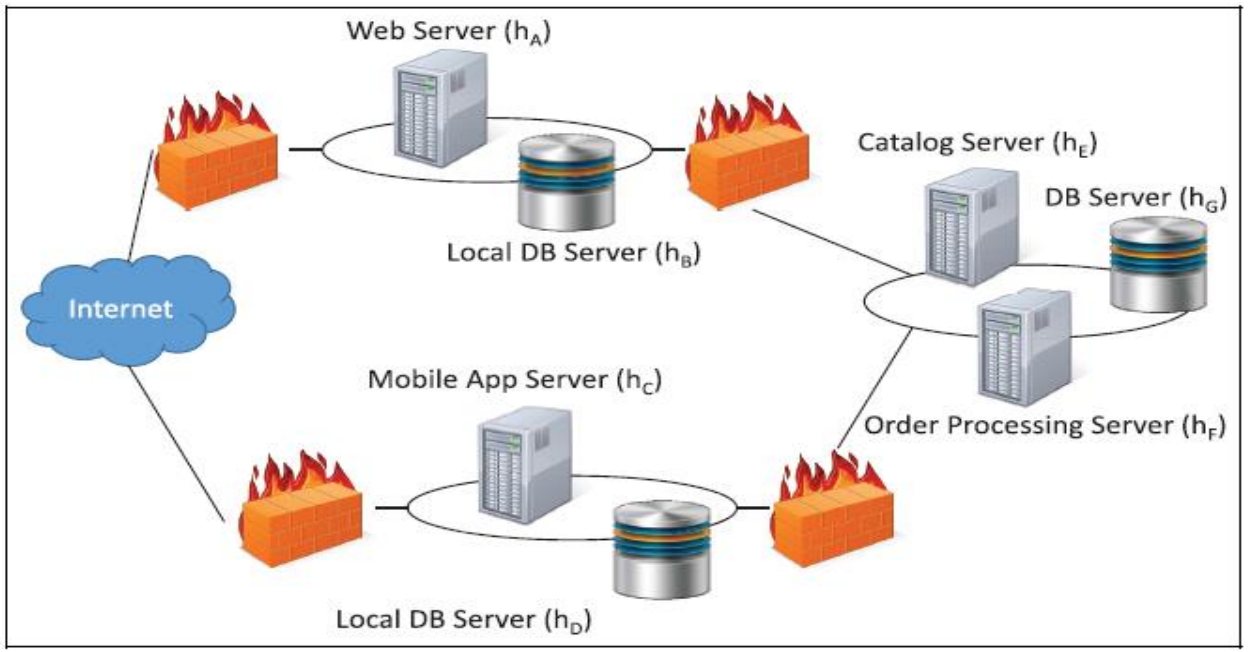

Model Parameters
Incident Information
Attack type
Interruption
Attacked IT
AOCRouter
Simulation Type
Known Incident Duration
Attack duration (minutes)
15
Mission Information
Mission workflow location
Target type
Location (x, y)
Target time window
Weapon ID
Estimate mission impact
Cancel

نحوه ارزیابی اثرات حمله [12]

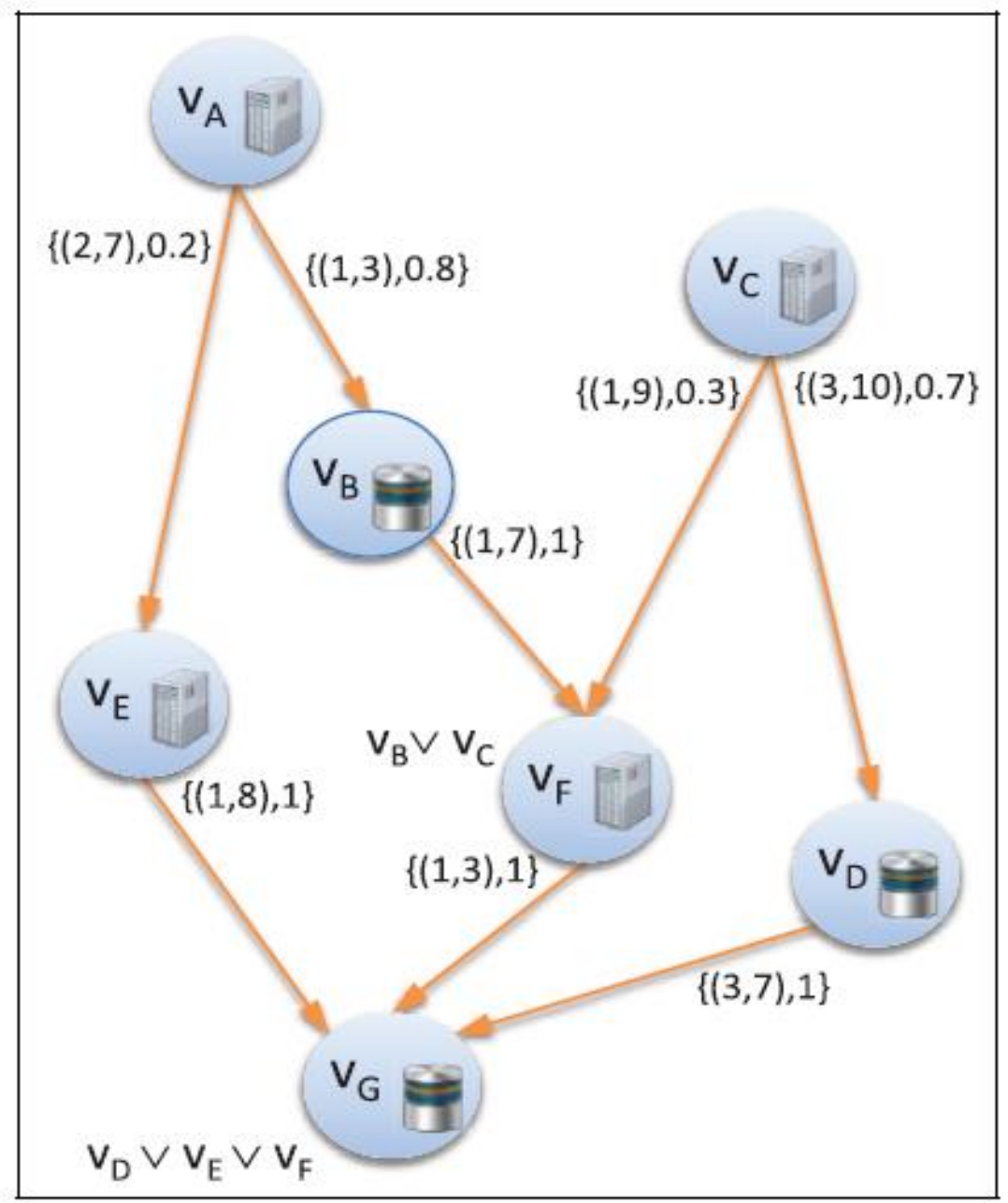


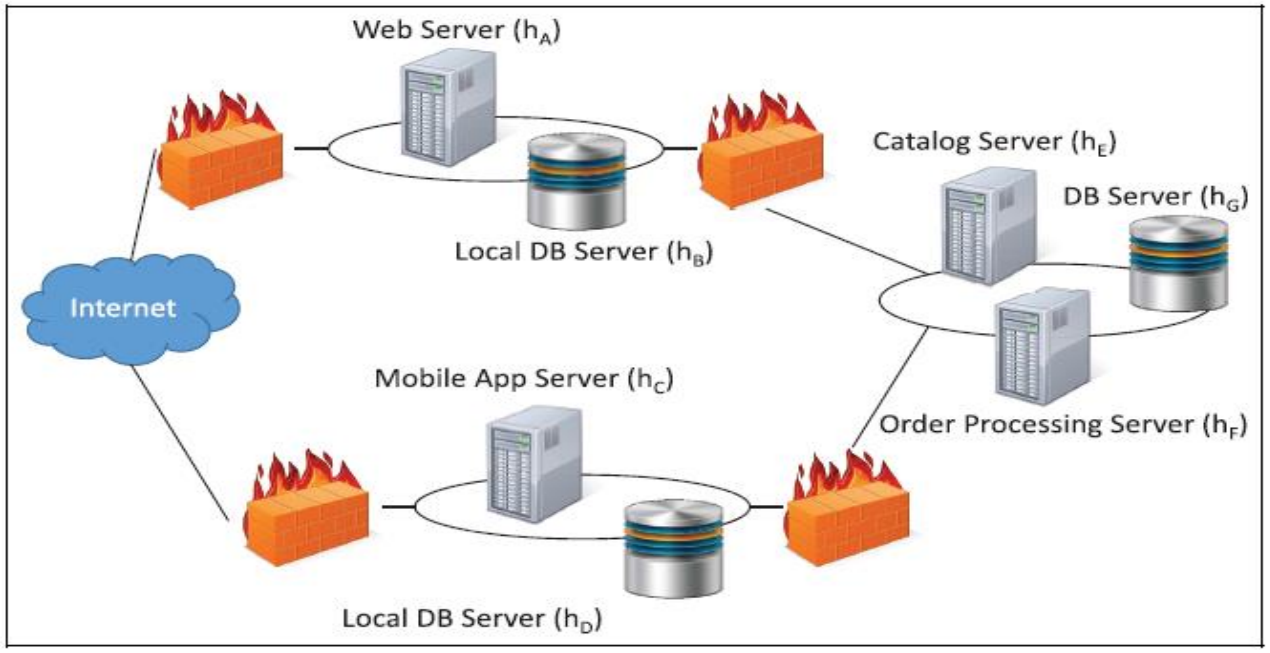
مثال- ارائه سرویس های خرید آنلاین و پیگیری سفارش [12]



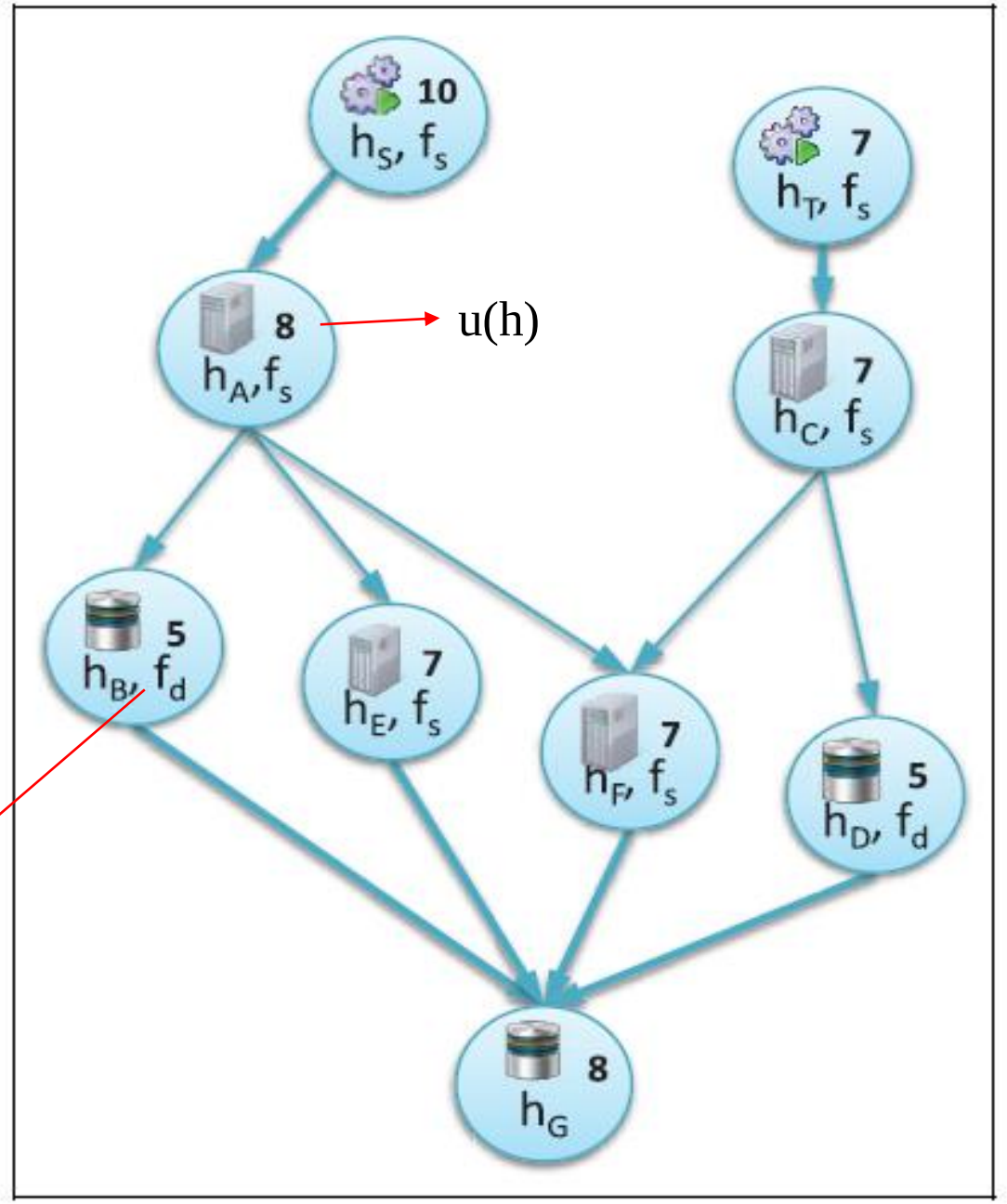


Probabilistic Temporal Attack Graph

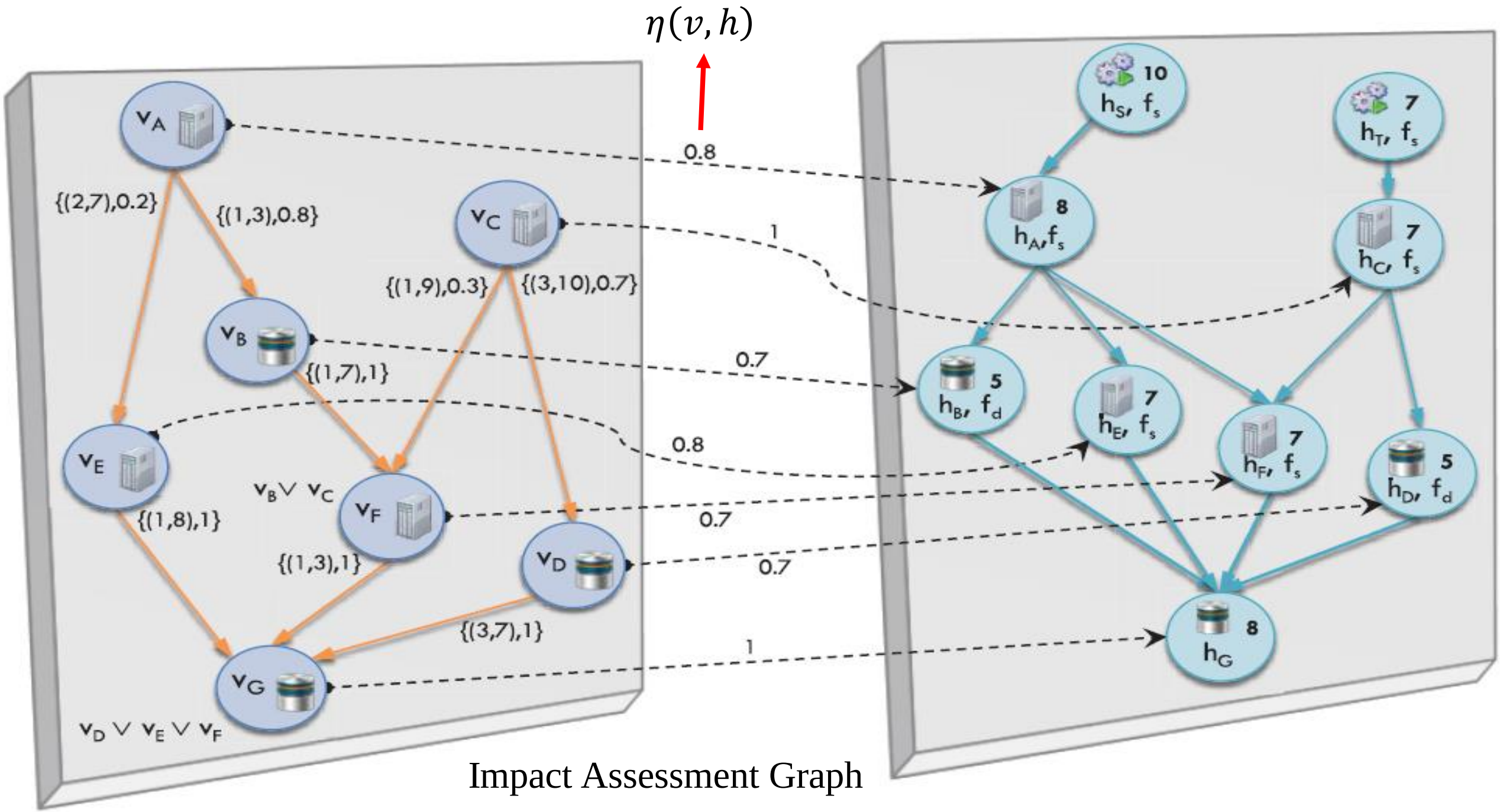




Dependency Graph



Dependency Type



Impact Assessment Graph

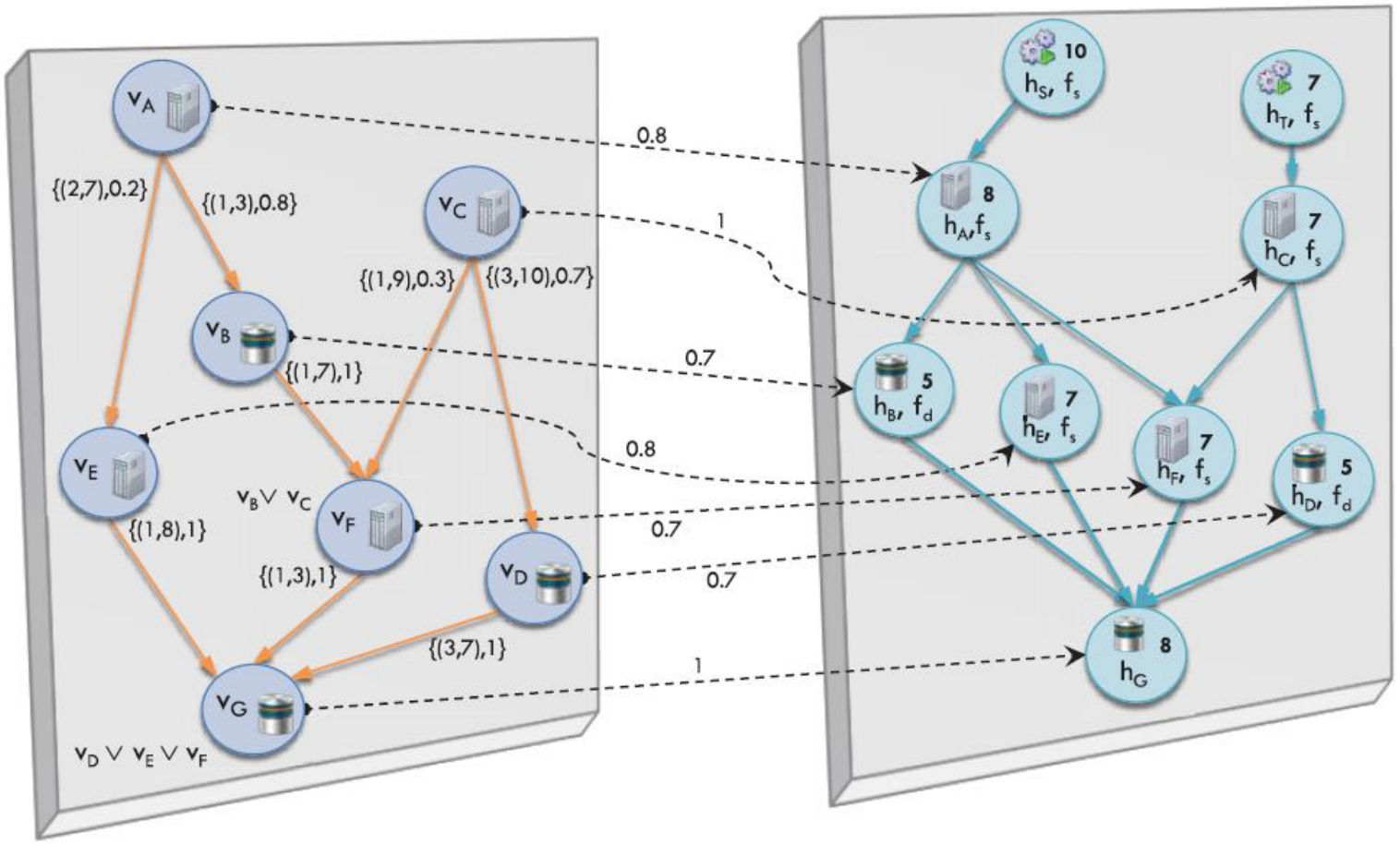
مثال– ادامه

$$s_i(h) = \big(1 - \eta(v,h)\big).s_{i-1}(h)$$

$$u_i(h) = s_i(h).u(h)$$

$$\triangle\, impact_i = \sum_{h \in H} \big(s_{i-1}(h) - s_i(h)\big).u(h) = \sum_{h \in H} \big(u_{i-1}(h) - u_i(h)\big)$$

مثال– ادامه



فرض کنید کـه $\forall h \in H, s_0(h) = 1$ و یـک حملـه کننـده در زمان t_1 از آسیب پذیری v_C بهره برداری می کند.

$$\Delta impact_1 = (1-0) \times 7 + (1-0) \times 7 = 14$$

$$\triangle\, impact_i = \sum_{h \in H} \big(s_{i-1}(h) - s_i(h)\big).u(h)$$

مثال– ادامه

در زمان t_2، حمله کننده ممکن است یکی از دو گام زیر را اجرا کند:
بهره برداری از v_D (با احتمال ۰.۷) یا v_F (با احتمال ۰.۳).

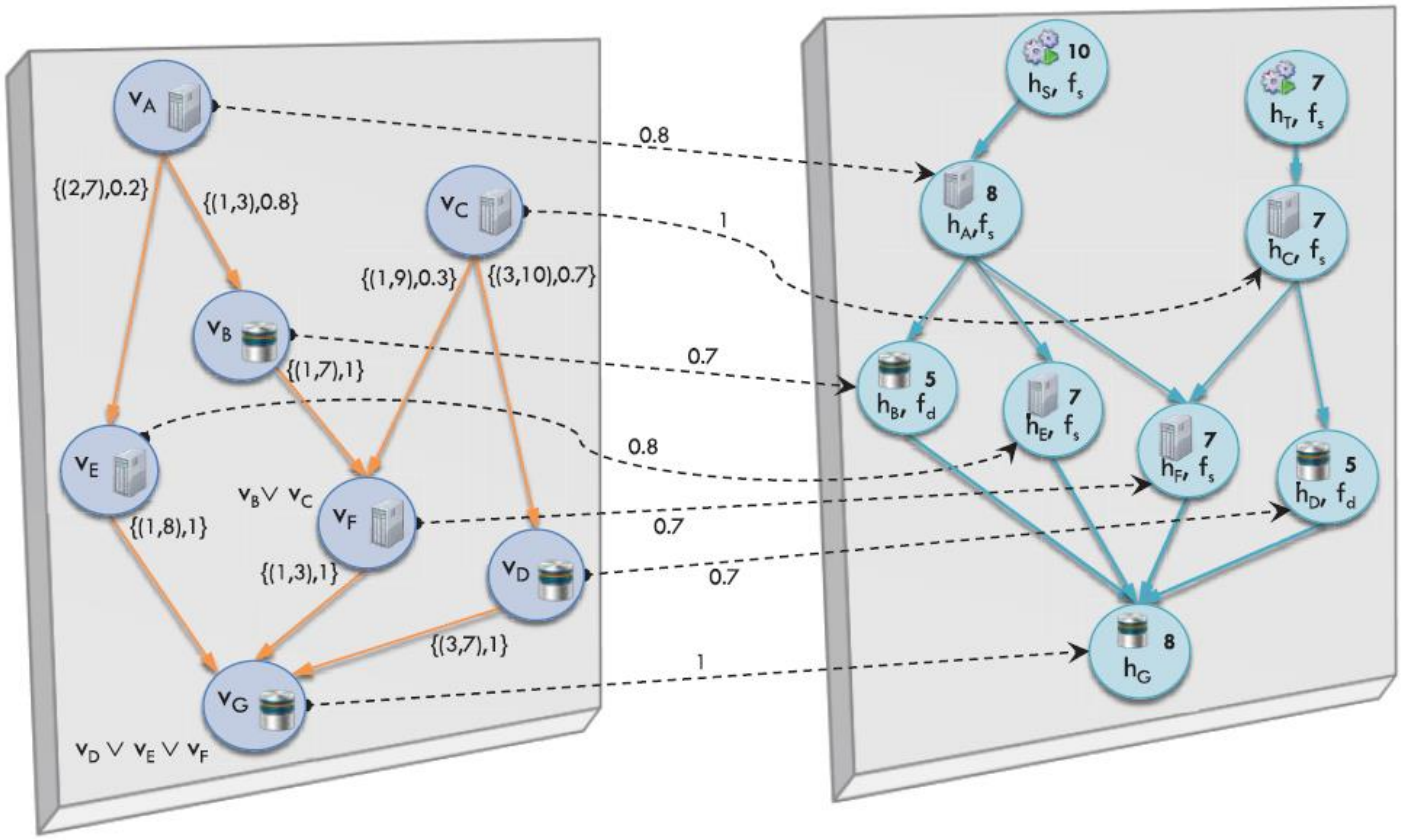
در حالت اول،

$$\Delta impact_1 = 0.7 \times 5 = 3.5$$

در حالت دوم،

$$\Delta impact_2 = 0.7 \times 7 + 8 + 10 = 22.9$$

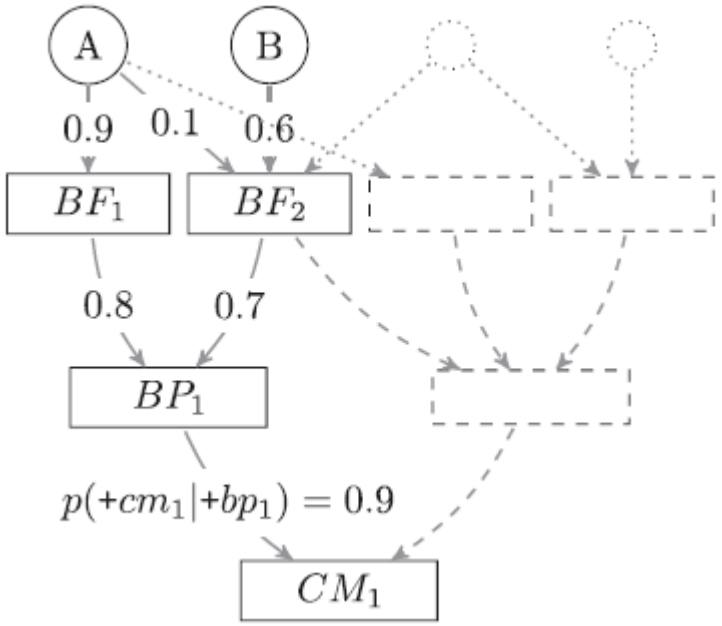
در نتیجه، حالت دوم علیرغم اینکه احتمال رخداد کمتری دارد اما اثرات بیشتری از خود برجا می گذارد.



Probabilistic Mission Impact Assessment (PMIA) [13]

- زمانی که عدم قطعیت ورودی وجود دارد، از ارزیابی اثرات احتمالی بر روی مأموریت استفاده می شود.
- برای ارزیابی از روش (شبیه سازی) مونته کارلو استفاده می شود.
- شبیه‌سازی مونته کارلو برای توصیف روشی جهت انتشار عدم قطعیت‌های موجود در ورودی مدل به عدم قطعیت‌ها در خروجی مدل، به کار می‌رود.

PMIA [13]



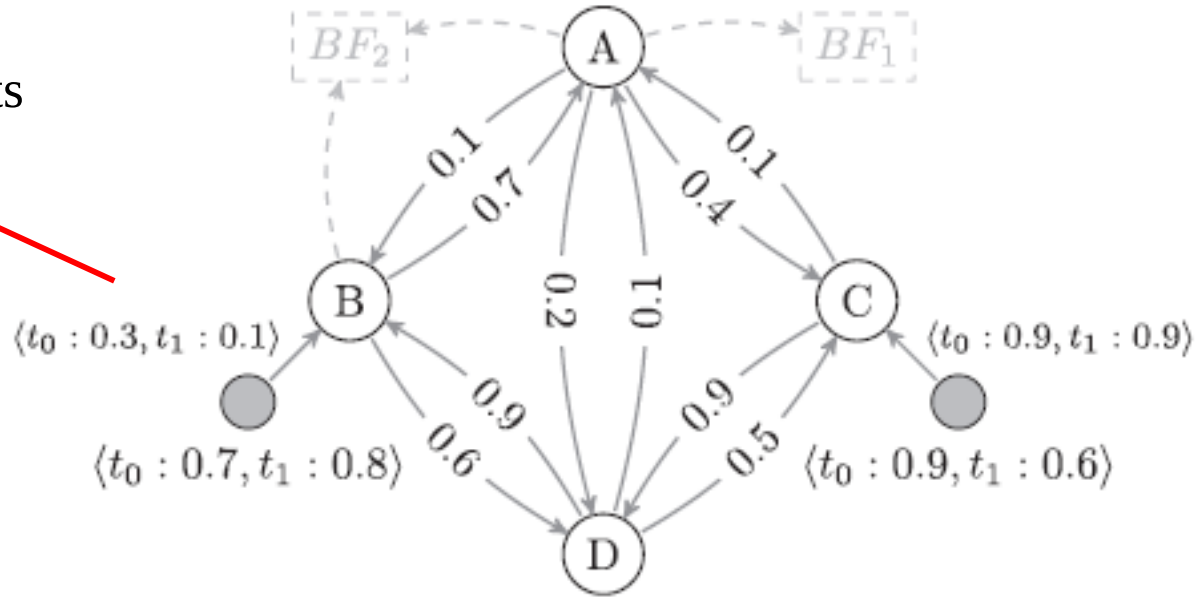
$$P(CM_1, BP_1, BF_1, BF_2, A, B) = P(CM_1|BP_1) \cdot P(BP_1|BF_1, BF_2) \cdot P(BF_1|A) \cdot P(BF_2|A, B) \cdot P(A) \cdot P(B),$$

$$P(+cm_1|+a) = \alpha \cdot \sum_{BP_1} \sum_{BF_1} \sum_{BP_2} P(+cm_1, BP_1, BF_1, BF_2, +a, \neg b),$$

Mission Dependency Model

PMIA [13]

Temporal Aspects, Shock Events

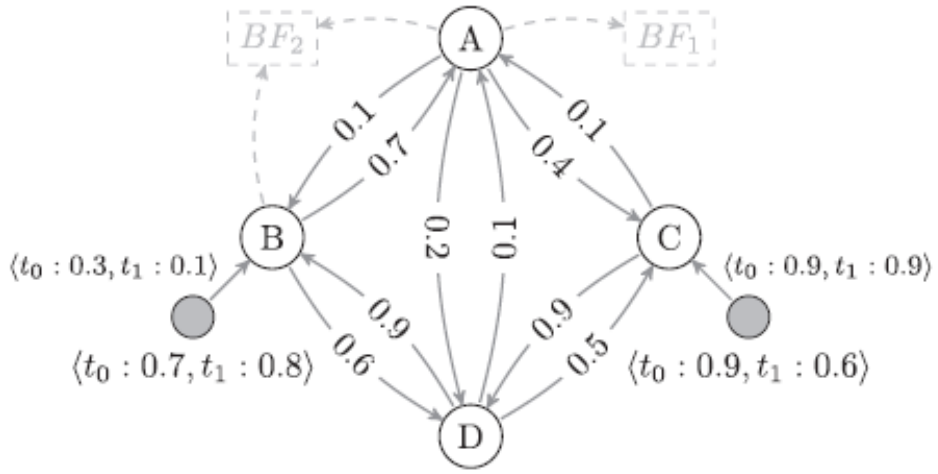


Resource Dependency Model

Algorithm to the MIA Problem [13]

$$w_0^A = \{p(+a|+b), p(+b|+se_B)\}$$
$$w_1^A = \{p(+a|+b), p(+b|+d), p(+d|+c), p(+c|+se_C)\}$$
$$w_2^A = \{p(+a|+c), p(+c|+se_C)\}$$
$$w_3^A = \{p(+a|+c), p(+c|+d), p(+d|+b), p(+b|+se_B)\}$$

→ Probabilistic Proofs

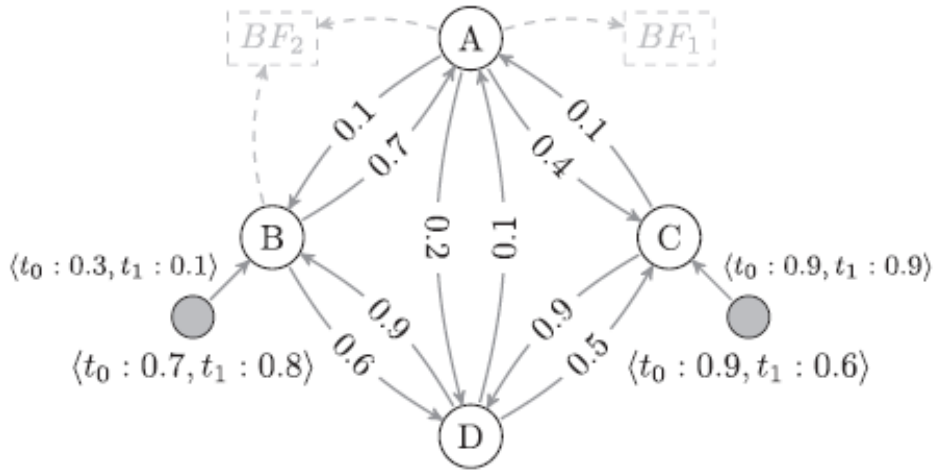


Algorithm to the MIA Problem [13]

$$w_0^A = \{p(+a|+b), p(+b|+se_B)\}$$
$$w_1^A = \{p(+a|+b), p(+b|+d), p(+d|+c), p(+c|+se_C)\}$$
$$w_2^A = \{p(+a|+c), p(+c|+se_C)\}$$
$$w_3^A = \{p(+a|+c), p(+c|+d), p(+d|+b), p(+b|+se_B)\}$$

→ Probabilistic Proofs

$$\begin{aligned} P(+a|+se_C, +se_B) &= \mathbf{P}(w_0^A) \cup \mathbf{P}(w_1^A) \cup \mathbf{P}(w_2^A) \cup \mathbf{P}(w_3^A) \\ &= P(w_0^A) + P(w_1^A) + P(\mathbf{w_2^A}) + P(w_3^A) \\ &\quad - P(w_0^A, w_1^A) - P(w_0^A, w_2^A) - P(w_0^A, w_3^A) \\ &\quad - P(w_1^A, w_2^A) - \mathbf{P}(w_1^A, w_3^A) - P(w_2^A, w_3^A) \\ &\quad + P(w_0^A, w_1^A, w_2^A) + P(w_0^A, w_1^A, w_3^A) \\ &\quad + P(w_1^A, \mathbf{w_2^A}, w_3^A) - P(w_0^A, w_1^A, w_2^A, w_3^A) \end{aligned}$$

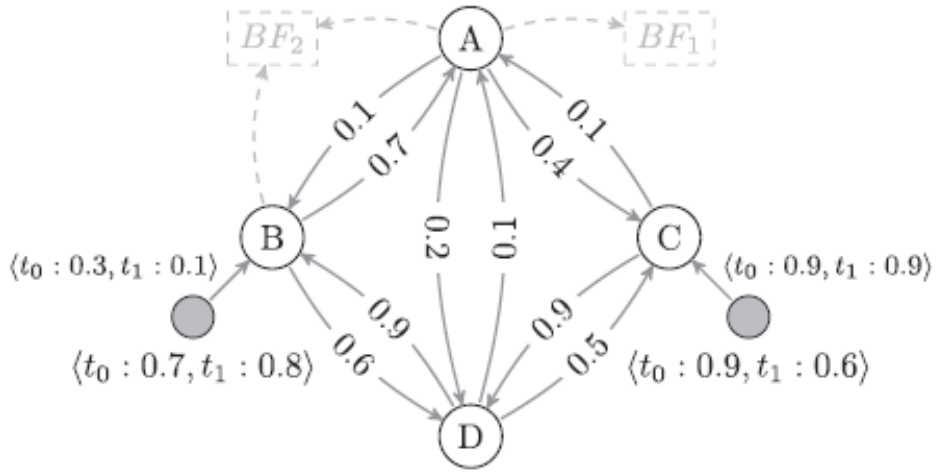


Algorithm to the MIA Problem [13]

$$w_0^A = \{p(+a|+b), p(+b|+se_B)\}$$
$$w_1^A = \{p(+a|+b), p(+b|+d), p(+d|+c), p(+c|+se_C)\}$$
$$w_2^A = \{p(+a|+c), p(+c|+se_C)\}$$
$$w_3^A = \{p(+a|+c), p(+c|+d), p(+d|+b), p(+b|+se_B)\}$$

→ Probabilistic Proofs

$$\begin{aligned} P(+a|+se_C, +se_B) &= \mathbf{P}(w_0^A) \cup \mathbf{P}(w_1^A) \cup \mathbf{P}(w_2^A) \cup \mathbf{P}(w_3^A) \\ &= P(w_0^A) + P(w_1^A) + P(\mathbf{w_2^A}) + P(w_3^A) \\ &\quad - P(w_0^A, w_1^A) - P(w_0^A, w_2^A) - P(w_0^A, w_3^A) \\ &\quad - P(w_1^A, w_2^A) - \mathbf{P}(w_1^A, w_3^A) - P(w_2^A, w_3^A) \\ &\quad + P(w_0^A, w_1^A, w_2^A) + P(w_0^A, w_1^A, w_3^A) \\ &\quad + P(w_1^A, \mathbf{w_2^A}, w_3^A) - P(w_0^A, w_1^A, w_2^A, w_3^A) \end{aligned}$$



RV=<p(+a|+b), p(+b|+se$_B$), p(+a|+b), p(+b|+d), p(+d|+c), p(+c|+se$_C$), p(+a|+c), p(+c|+se$_C$), p(+a|+c), p(+c|+d), p(+d|+b), p(+b|+se$_B$)>

RV= <+, +, +, -, -, -, +, -, +,…>

$$P(+mn|+se_C, +se_B) \approx \frac{hit_{MN}}{n_S}$$

→ Monte Carlo Simulation

منابع و مراجع

[1]. https://en.wikipedia.org/wiki/Awareness

[2]. Endsley MR, Garland DJ, editors. 2000 Jul 1, Situation awareness analysis and measurement. *CRC Press*.

[3]. Noel, S., Harley, E., Tam, K.H., Limiero, M. and Share, M., 2016. CyGraph: graph-based analytics and visualization for cybersecurity. In *Handbook of Statistics* (Vol. 35, pp. 117-167). Elsevier.

[4]. J. Watters, "RiskMAP — Tool for building a business case for investing in security", The Institute for Information Infrastructure Protection, http://www.thei3p.org/publications/

[5]. Kertzner, P., Watters, Bodeau, D., Hahn, A., 2008. Process Control System Security Technical Risk Assessment Methodology & Technical Implementation. MITRE CORP MCLEAN VA MCLEAN United States.

[6]. Goodall, J.R., D'Amico, A. and Kopylec, J.K., 2009, October. Camus: automatically mapping cyber assets to missions and users. *In MILCOM 2009-2009 IEEE Military Communications Conference* (pp. 1-7). IEEE.

[7]. Buchanan, L., Larkin, M. and D'Amico, A., 2012, November. Mission assurance proof-of-concept: Mapping dependencies among cyber assets, missions, and users. In *2012 IEEE Conference on Technologies for Homeland Security (HST)* (pp. 298-304). IEEE.

منابع و مراجع

[8]. Musman, S. and Temin, A., 2015, April. A cyber mission impact assessment tool. In *2015 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-7). IEEE.

[9]. Musman, S., Tanner, M., Temin, A., Elsaesser, E. and Loren, L., 2011, April. A systems engineering approach for crown jewels estimation and mission assurance decision making. In *2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)* (pp. 210-216). IEEE.

[10]. Musman, S., Temin, A., Tanner, M., Fox, D. and Pridemore, B., 2010, July. Evaluating the impact of cyber attacks on missions. In *Proceedings of the 5th International Conference on Information Warfare and Security* (pp. 446-456).

[11]. Musman, S., Tanner, M., Temin, A., Elsaesser, E. and Loren, L., 2011, April. Computing the impact of cyber attacks on complex missions. In *2011 IEEE International Systems Conference* (pp. 46-51). IEEE.

[12]. Albanese, M. and Jajodia, S., 2018. A graphical model to assess the impact of multi-step attacks. *The Journal of Defense Modeling and Simulation*, *15*(1), pp.79-93.

[13]. Motzek, A. and Möller, R., 2017. Context-and bias-free probabilistic mission impact assessment. *computers & security*, *65*, pp.166-186.

پیامبر اکرم(ص) فرمودند:

دانش گنجینه ای است که کلید آن پرسش است.
پس خدایتان رحمت کند بپرسید که با اینکار چهار نفر اجر میبرند:
پرسشگر، پاسخگو، شنونده و دوستداران آنان.

منتخب میزان الحکمه:۲۶۰