JUMP Tactical Cyber Mission Planning

Tim Dudman, Sowdagar Badesha
Riskaware
Bristol
UNITED KINGDOM
tim.dudman@riskaware.co.uk
sowdagar.badesha@riskaware.co.uk

Marco Casassa Mont
BMT Defence & Security UK
Bath
UNITED KINGDOM
mcasassamont@bmtdsl.co.uk

The contents of this paper/presentation should not be interpreted as representing the views of the UK MOD, nor should it be assumed that they reflect any current or future UK MOD policy. The UK MOD contact for the JUMP programme is Steve Barrington, Dstl, Salisbury, UNITED KINGDOM, sjbarrington@dstl.gov.uk.

BMT Defence Services
"Where will our knowledge take you?"

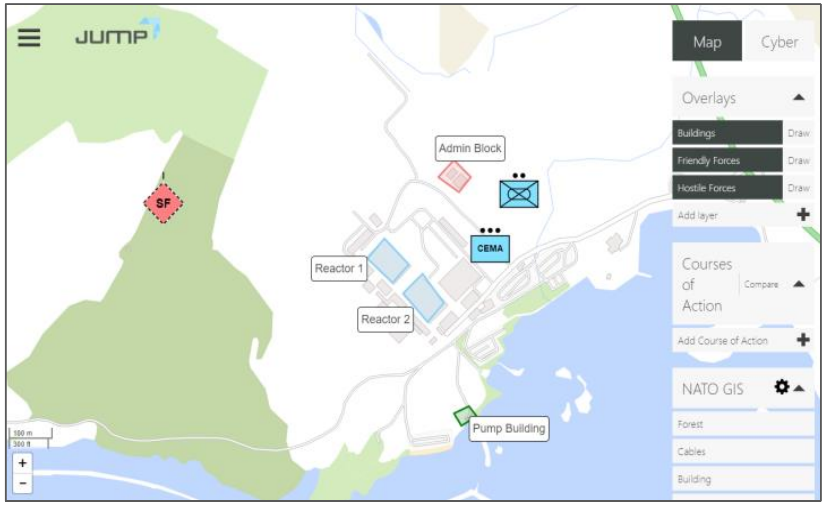
Riskaware
capability through technology

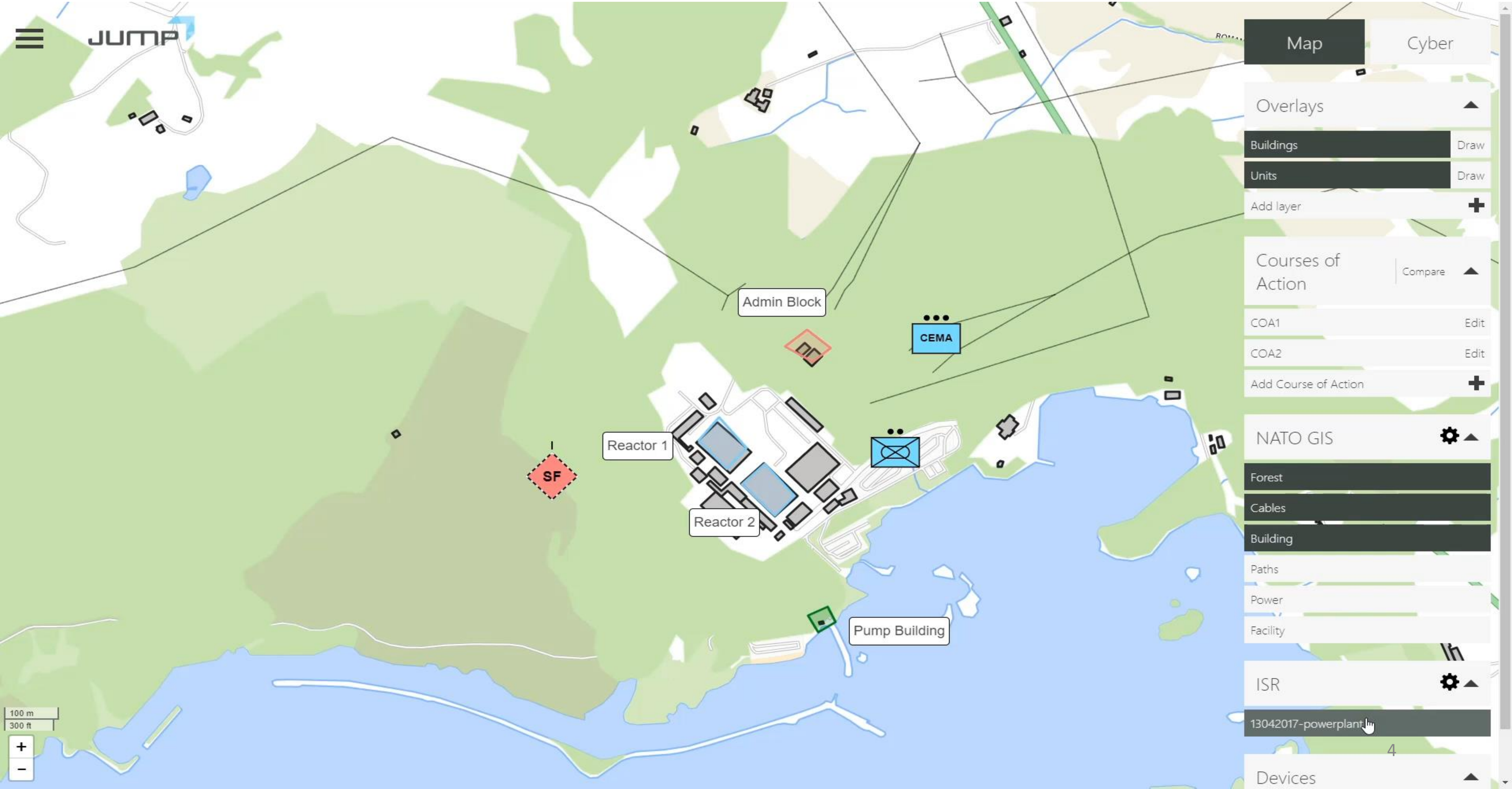
Overview

- **JUMP**: **J**oint **U**ser **M**ission **P**lanning - Concept demonstration environment.
- Research and Development (R&D) prototype tool.
- Enables understanding of the impact of land, air and maritime activities on the cyber domain and vice versa for joint force missions.
- Uses state-of-the-art analytics and interactive visualisations.
- Provides underpinning research to the defence community on where analytics and visualisation can be implemented to best effect within a coherent tactical mission planning context.
- At the end of the programme of work it will provide:
    - Detail required for a requirements document for tools and techniques to support a military commander to accomplish a wide-range of mission-planning tasks
    - Support mission rehearsal immediately ahead of the mission, re-planning during the live mission, and following the mission as part of de-briefing

Interfaces - Cyber Commander

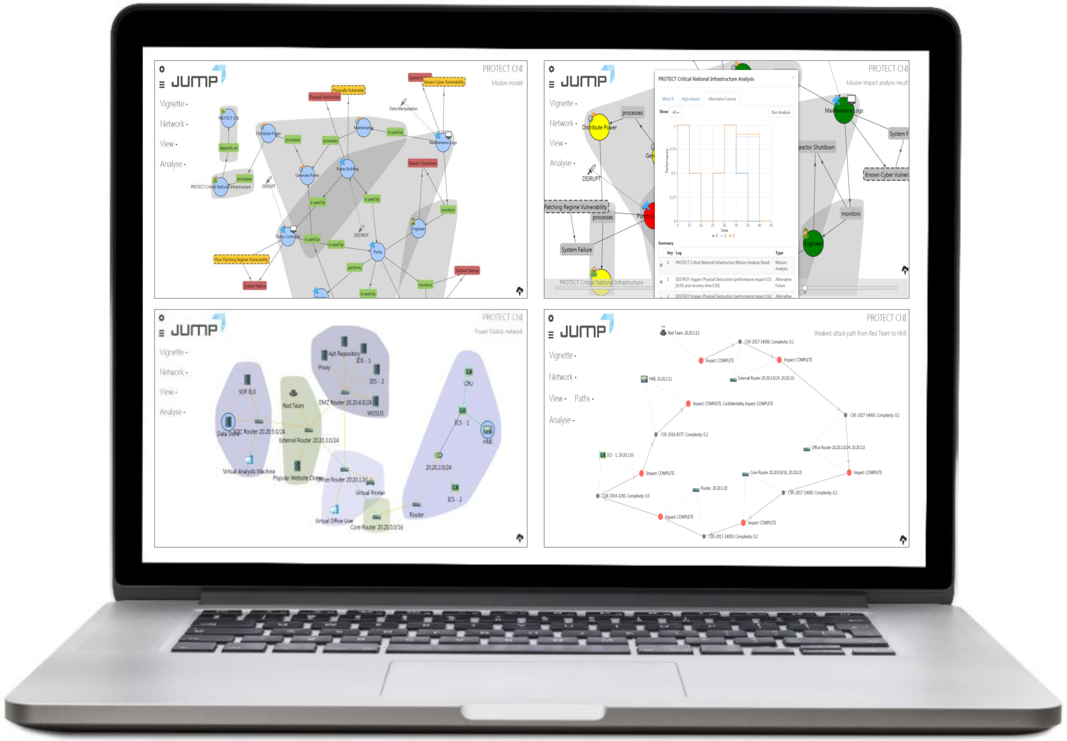
- **Cyber Commander:** provides cyber situational awareness, cyber directions and contributes to the definition of Courses of Action (CoA) within a mission.
- Access and analyse a broad range of cyber and physical information in order to make informed decisions and explore suitable trade-offs when defining CoAs.
- JUMP supports a Cyber Commander’s activities by providing a rich set of touch-enabled integrated views, including:
  - **Map view:** utilises the NATO Core Geographic Services System to provide geographical insights
  - **Cyber-physical view:** cyber infrastructure of relevance in respect to physical location
  - **Network view:** device technical information and topological layout
  - **CoA view:** mission risk and CoA trade-off analysis




JUMP
Map
Cyber
Overlays
Buildings
Draw
Units
Draw
Add layer
Courses of Action
Compare
COA1
Edit
COA2
Edit
Add Course of Action
NATO GIS
Forest
Cables
Building
Paths
Power
Facility
ISR
13042017-powerplant
Devices
Admin Block
CEMA
Reactor 1
SF
Reactor 2
Pump Building
100 m
300 ft
+
−

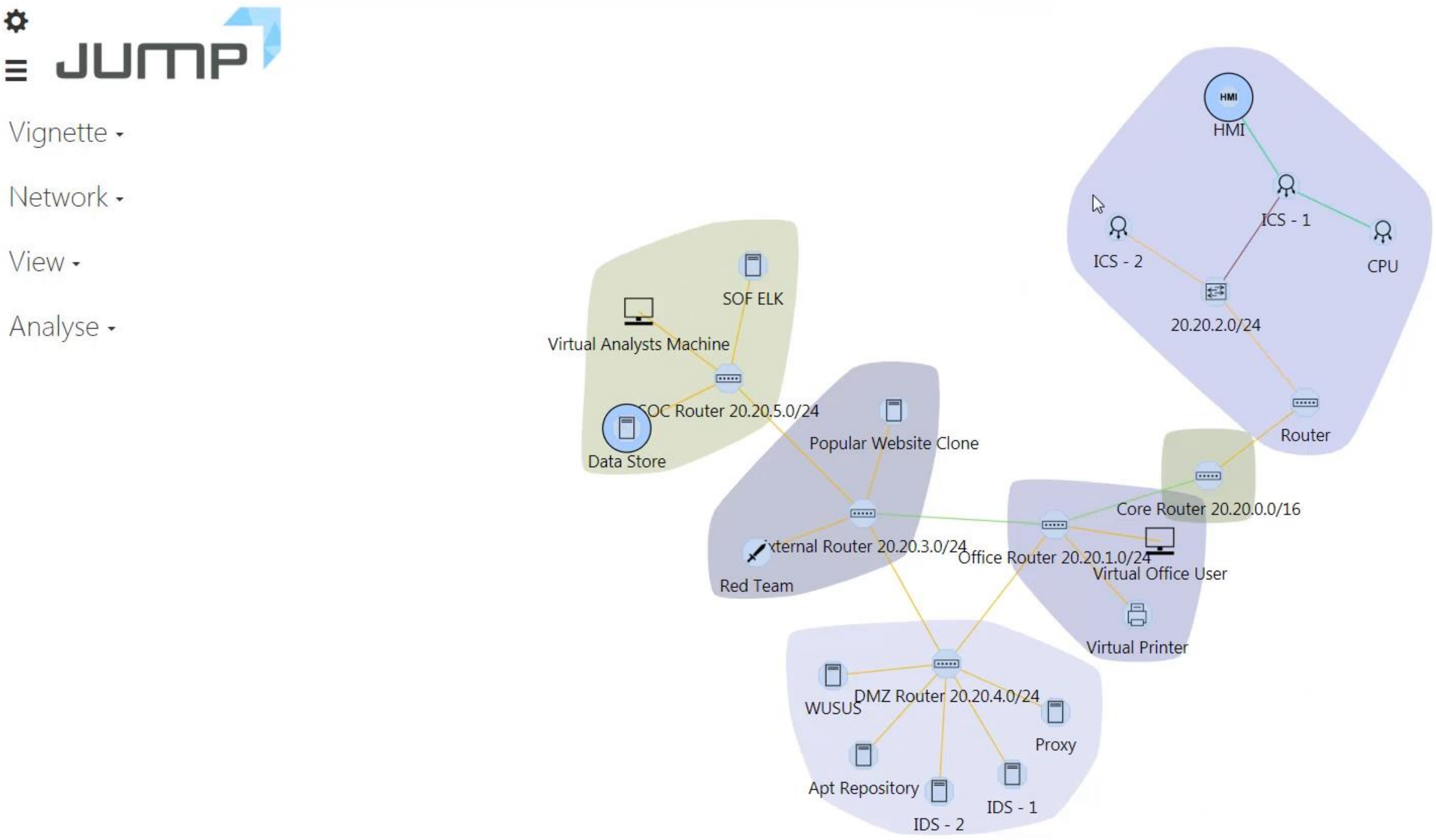
Interfaces - Cyber Analyst

- **Cyber Analyst:** model complex mission objectives, supporting processes and component hierarchies while visually interrogating the results of simulated threats, both at the network and mission level.
- Visual analytics enable the Cyber Analyst to interactively construct and analyse the mission impact of cyber-attacks on the underpinning cyber infrastructure.



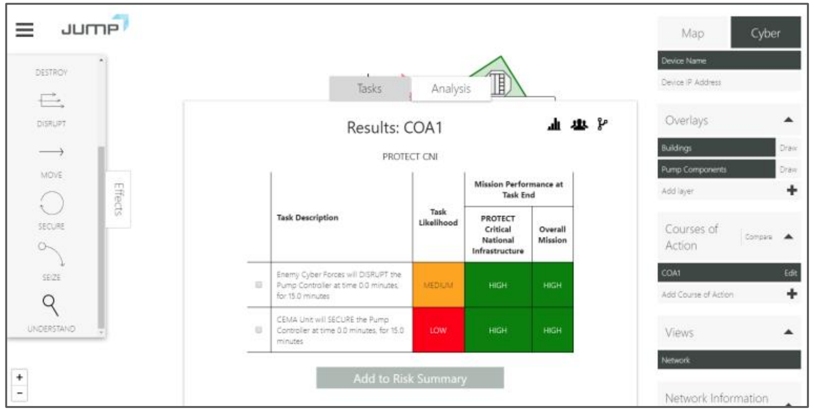
PROTECT CNI

Power Station network



Analytics - Evaluating Courses of Action

- JUMP aims at enabling a Cyber Commander to analyse and evaluate a CoA for a given mission.
- Compute and provide multiple metrics, including:
  - Performance, cost and time, risk and impact of mitigations, and the likelihood of tasks succeeding
- An extensible library of analytics computes these metrics, which factors in the physical, geographic and cyber information stored in JUMP. For example:
  - Identify critical assets for a given cyber network or mission
  - Compute the performance of a CoA by performing MIA, identifying the cost and time for given tasks
  - Cyber risk analysis based on risk level, deployed mitigations, controls and countermeasures

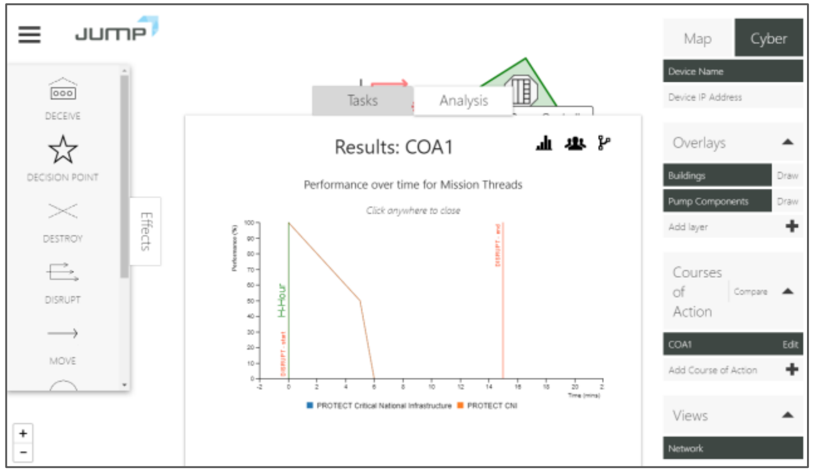


Results: COA1

PROTECT CNI

	Task Description	Task Likelihood	Mission Performance at Task End	
			PROTECT Critical National Infrastructure	Overall Mission
□	Enemy Cyber Forces will DISRUPT the Pump Controller at time 0.0 minutes, for 15.0 minutes	MEDIUM	HIGH	HIGH
□	CEMA Unit will SECURE the Pump Controller at time 0.0 minutes, for 15.0 minutes	LOW	HIGH	HIGH

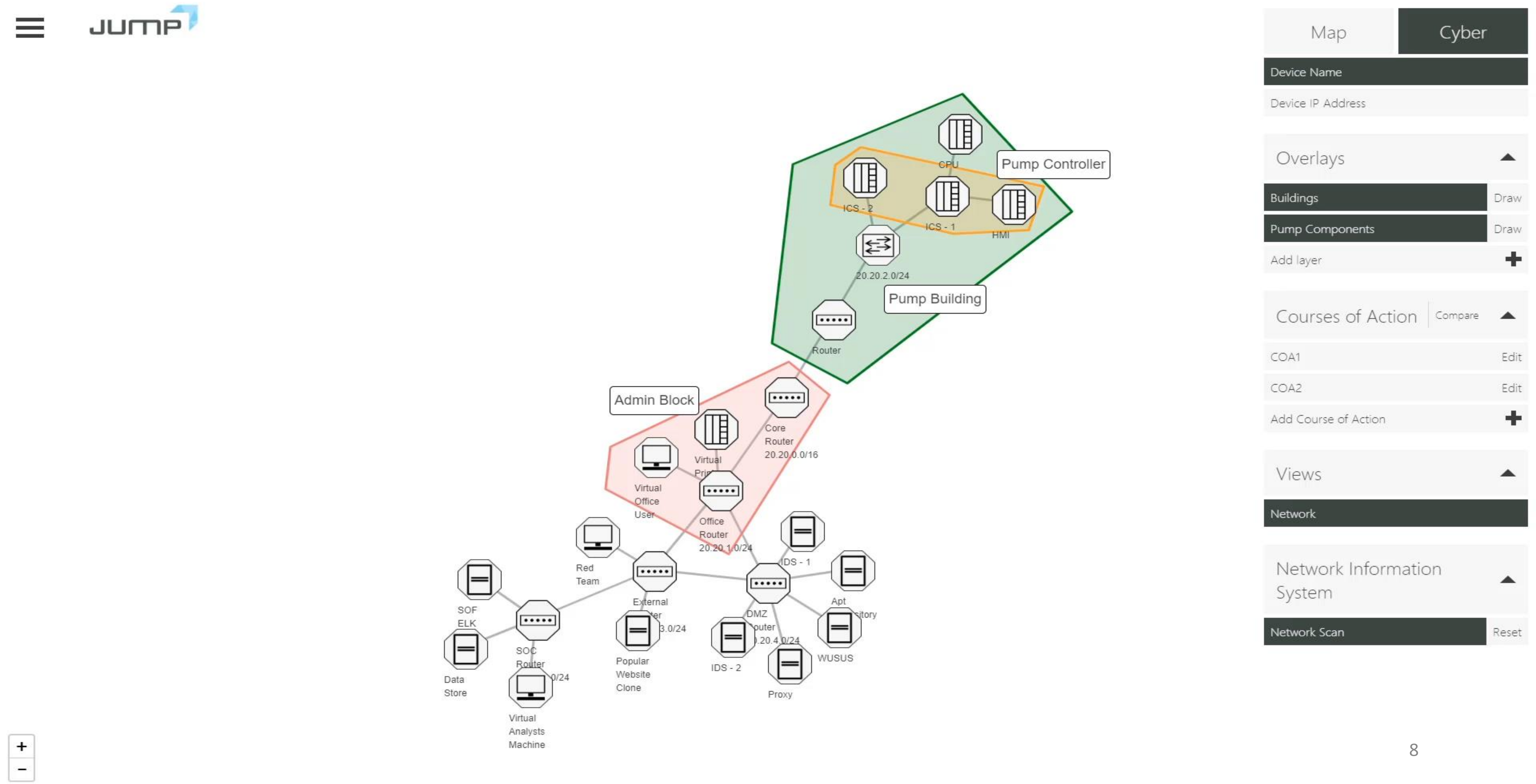
Add to Risk Summary



Results: COA1

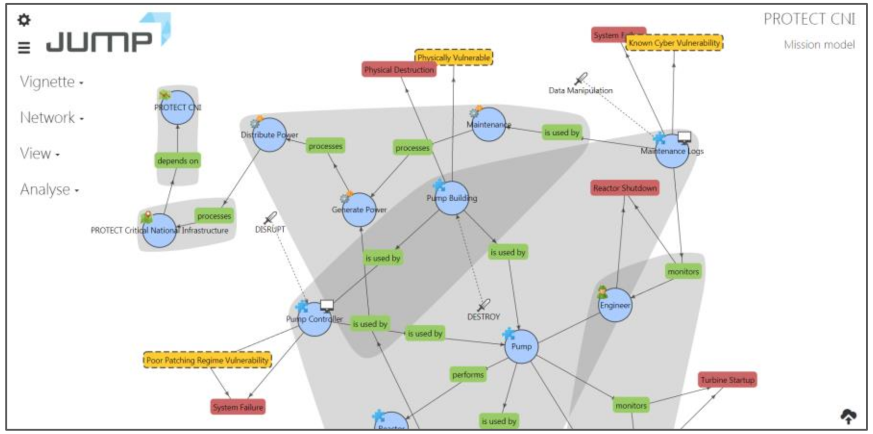
Performance over time for Mission Threads

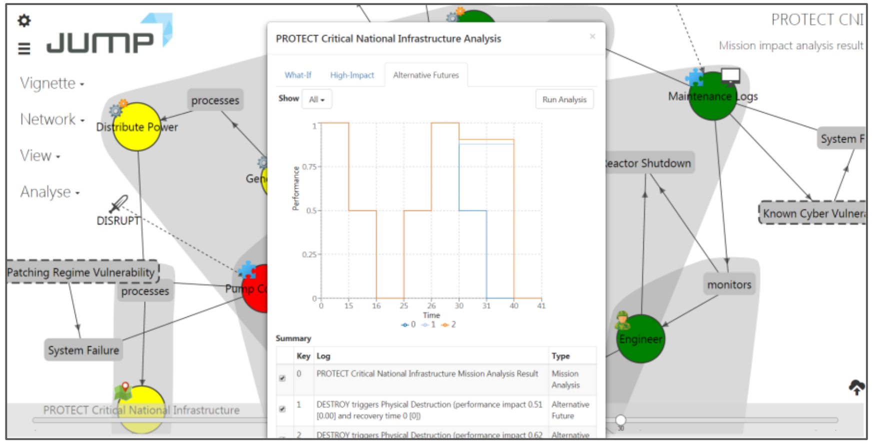
Click anywhere to close


JUMP
Pump Controller
CPU
ICS - 2
ICS - 1
HMI
20.20.2.0/24
Pump Building
Router
Admin Block
Core
Router
20.20.0.0/16
Virtual
Pri
Virtual
Office
User
Office
Router
20.20.1.0/24
Red
Team
External
ter
3.0/24
IDS - 1
Apt
itory
DMZ
outer
.20.4.0/24
SOF
ELK
SOC
Router
0/24
Data
Store
Virtual
Analysts
Machine
Popular
Website
Clone
IDS - 2
Proxy
WUSUS
Map
Cyber
Device Name
Device IP Address
Overlays
Buildings
Draw
Pump Components
Draw
Add layer
Courses of Action
Compare
COA1
Edit
COA2
Edit
Add Course of Action
Views
Network
Network Information System
Network Scan
Reset
+
−

Analytics - Mission Impact Assessment

- A unified connected-graph model-driven approach allows JUMP to represent the cyber terrain and mission in a single, coherent data.
- The mission is modelled as a topological vignette of interdependent mission components. These can represent mission threads, actors, processes and other mission-critical assets.
- Mission components can be associated with network devices, and have time-based events, vulnerabilities and impacts associated with them to allow the mission impact of both conventional and cyber events to be modelled.





PROTECT Critical National Infrastructure Analysis

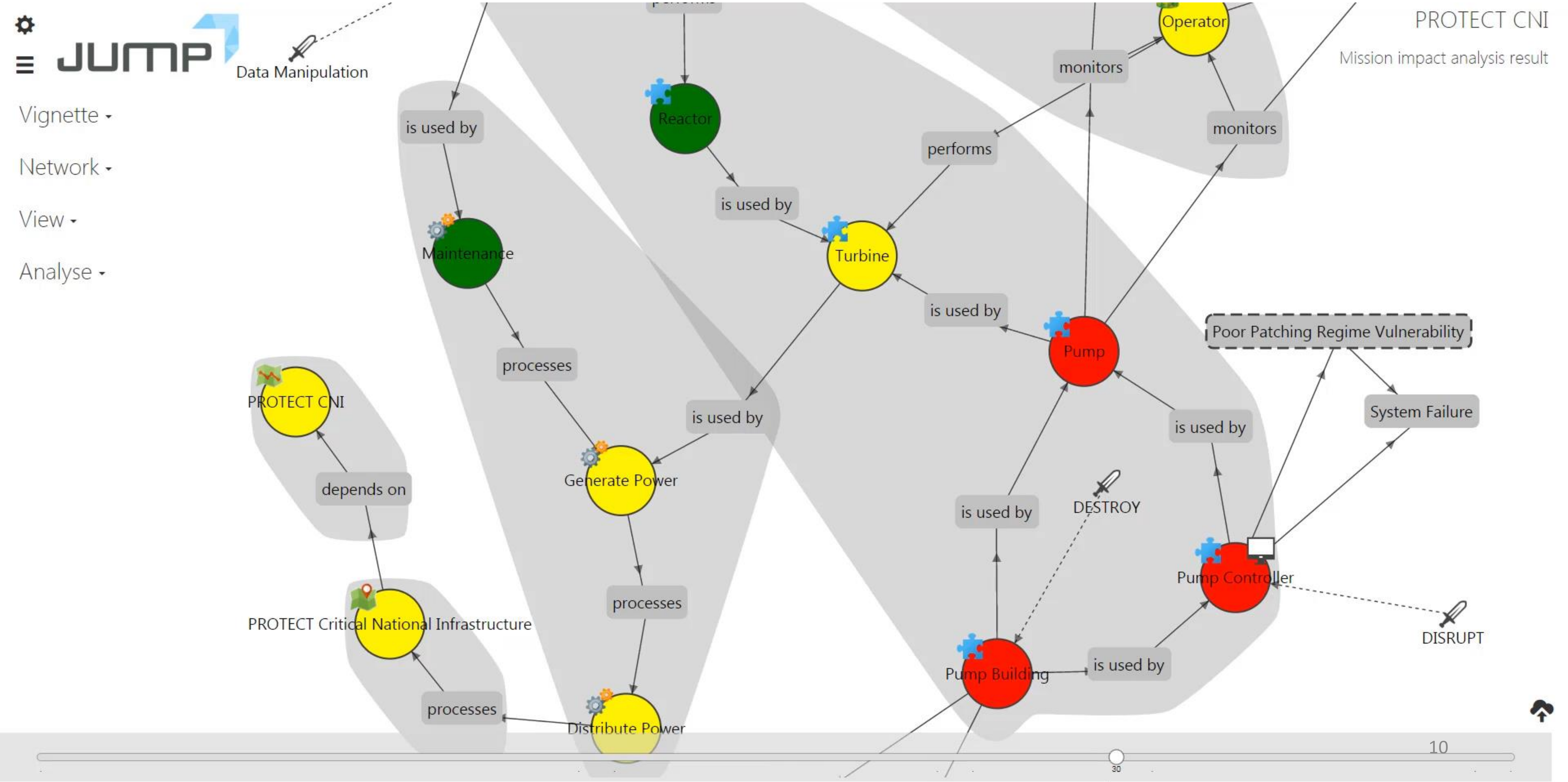
Summary

	Key	Log	Type
☑	0	PROTECT Critical National Infrastructure Mission Analysis Result	Mission Analysis
☑	1	DESTROY triggers Physical Destruction (performance impact 0.51 [0.00] and recovery time 0 [0])	Alternative Future
	2	DESTROY triggers Physical Destruction (performance impact 0.62	Alternative

BMT Defence Services
"Where will our knowledge take you?"

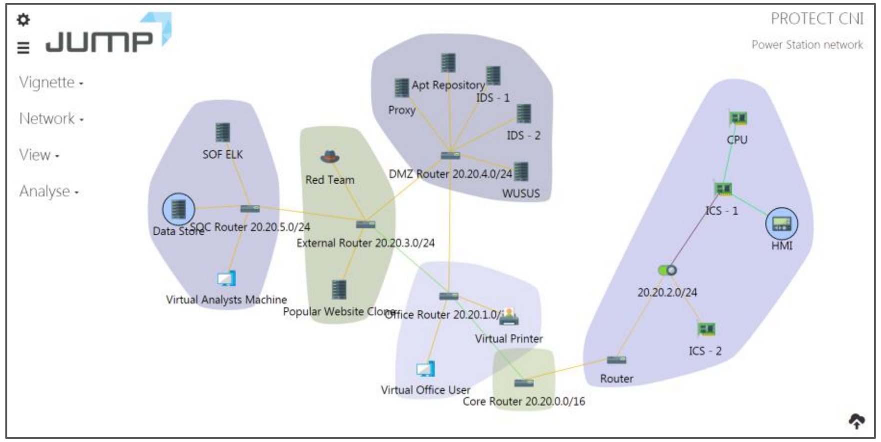
JUMP

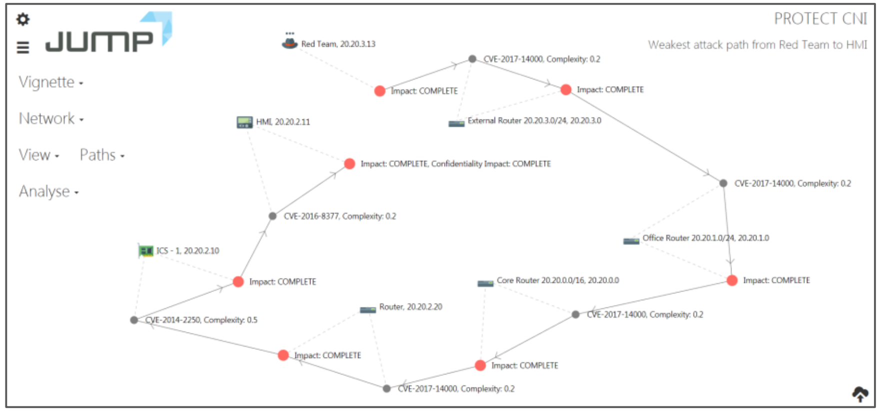
Riskaware
capability through technology

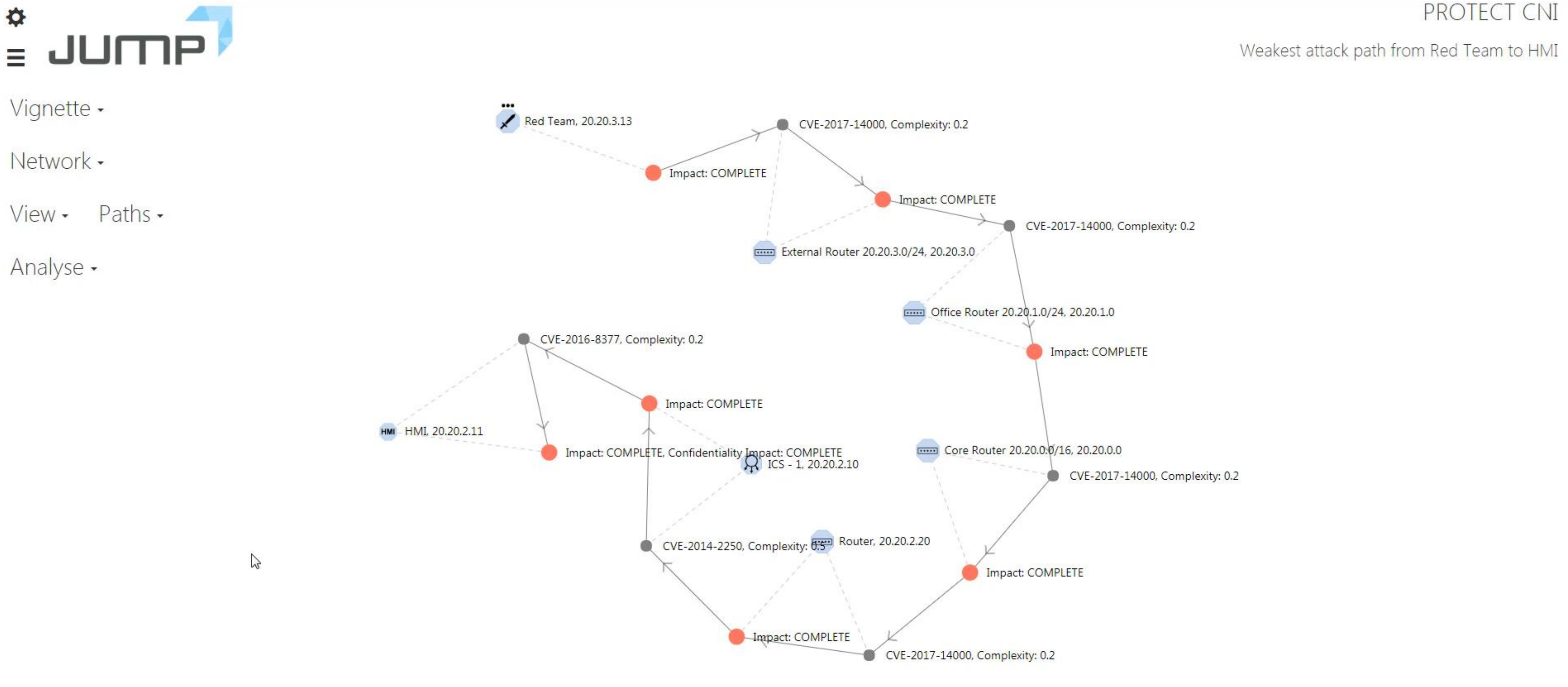

JUMP
Vignette
Network
View
Analyse
Data Manipulation
PROTECT CNI
Mission impact analysis result
performs
Operator
monitors
monitors
performs
Reactor
is used by
is used by
Maintenance
Turbine
is used by
Pump
Poor Patching Regime Vulnerability
System Failure
processes
is used by
is used by
PROTECT CNI
depends on
Generate Power
is used by
DESTROY
Pump Controller
processes
PROTECT Critical National Infrastructure
DISRUPT
Pump Building
is used by
processes
Distribute Power
30

Analytics - Cyber-Attack Analysis

- A computer network in JUMP can be analysed to display viable cyber-attack paths that could be used by a cyber threat during an attack.
- Device inter-relationships are modelled, and software vulnerabilities analysed to see how a cyber threat could traverse a network to a given mission-critical device.
- A cyber threat actor can be graded in capability and positioned topologically given operational intelligence to best simulate the logical attack origin.
- Attacks from multiple threat actors can be simulated simultaneously with varying levels of capability, and human-facilitated attack vectors can be modelled.




JUMP
Vignette ▾
Network ▾
View ▾
Paths ▾
Analyse ▾
PROTECT CNI
Weakest attack path from Red Team to HMI
Red Team, 20.20.3.13
CVE-2017-14000, Complexity: 0.2
Impact: COMPLETE
Impact: COMPLETE
HMI, 20.20.2.11
External Router 20.20.3.0/24, 20.20.3.0
Impact: COMPLETE, Confidentiality Impact: COMPLETE
CVE-2017-14000, Complexity: 0.2
CVE-2016-8377, Complexity: 0.2
Office Router 20.20.1.0/24, 20.20.1.0
ICS - 1, 20.20.2.10
Impact: COMPLETE
Core Router 20.20.0.0/16, 20.20.0.0
Impact: COMPLETE
Router, 20.20.2.20
CVE-2014-2250, Complexity: 0.5
CVE-2017-14000, Complexity: 0.2
Impact: COMPLETE
Impact: COMPLETE
CVE-2017-14000, Complexity: 0.2


JUMP
PROTECT CNI
Weakest attack path from Red Team to HMI
Vignette
Network
View
Paths
Analyse
Red Team, 20.20.3.13
CVE-2017-14000, Complexity: 0.2
Impact: COMPLETE
Impact: COMPLETE
CVE-2017-14000, Complexity: 0.2
External Router 20.20.3.0/24, 20.20.3.0
Office Router 20.20.1.0/24, 20.20.1.0
Impact: COMPLETE
CVE-2016-8377, Complexity: 0.2
Impact: COMPLETE
HMI
HMI, 20.20.2.11
Impact: COMPLETE, Confidentiality Impact: COMPLETE
ICS - 1, 20.20.2.10
Core Router 20.20.0.0/16, 20.20.0.0
CVE-2017-14000, Complexity: 0.2
CVE-2014-2250, Complexity: 0.5
Router, 20.20.2.20
Impact: COMPLETE
Impact: COMPLETE
CVE-2017-14000, Complexity: 0.2

Summary and Conclusions

- To date JUMP has been used for interactive CoA evaluation, MIA and cyber-attack analytics that provide insight into scenarios that bridge the cyber and physical domains.
- Feedback from stakeholders and users at demonstrations has indicated that it has utility at both the tactical and strategic level, especially if limitations concerned with advanced cyber-attack modelling, uncertainty and EM capabilities are addressed.
- Current research efforts for 2018/2019 are focused on addressing these limitations by enhancing:
    - Modelling of socio-technical cyber risks and controls (including threat actor goals and techniques)
    - Modelling temporal device connectivity and network uncertainty
    - Modelling EM effects (including the defence of mesh networks)
    - Optimising task cost and time calculations for CoA evaluation

JUMP