An Overview of MITRE Cyber Situational Awareness Solutions

The 18 May 2015 NATO Communications and Information Agency (NCIA) Request for Information (RFI) (CO-14068-MNCD2) [1] seeks a multi-nation cyber defense situational awareness (CDSA) capability. While MITRE is not a commercial tool vendor, our research has led to the development of a range of technical solutions that would benefit any CDSA toolkit.

This document describes the MITRE technical solutions that can be leveraged to enable or support an overall NATO CDSA solution. In some cases, the technical solutions are standardization efforts that enable information sharing for key aspects of CDSA. In other cases, the solutions are prototype tools that could be transitioned to government entities or to commercial vendors. The specific NCIA RFI CDSA use cases are used to orient the MITRE capabilities with the overarching CDSA requirements.

It is important to note that most of MITRE's efforts have focused on solutions described in the primary RFI scenario "Oranjeland APT." For the more technical scenarios and use cases, MITRE has had success in leveraging commercial off-the-shelf (COTS) tools. These tools are evaluated and procured based on well-defined needs and requirements. They are integrated to higher-level CDSA views using aggregation tools, such as security information and event management (SIEM) and log management products or custom-developed data-processing pipelines.

MITRE CDSA Solutions

The NCIA RFI defines CDSA solutions in terms of their ability to meet 35 use cases across three scenarios. These scenarios provide insight into the operational and business requirements sought by the RFI.

It is also important to take higher-level (strategic and tactical) views of CDSA requirements. Considering technical solutions in terms of their transformative benefits helps keep the "big picture" firmly in focus. The operational use cases and scenarios then address specific concerns for instantiations of higher-level strategic/tactical directions. In our discussion of MITRE technical solutions for CDSA (oriented to strategic and tactical benefits), we point out how each solution addresses the operational use cases.

A comprehensive suite of CDSA capabilities includes four core areas:

1. **Threat Analysis** – Understand and track threat landscapes and actors, along with the tactics, techniques, and procedures (TTPs) that they employ.
2. **Dependency & Impact Analysis** – Understand the mission and asset interdependencies to identify resiliency weaknesses and extrapolate mission impact.
3. **Analysis of Alternatives (AoA)** – Identify potential Courses of Action (CoAs) and other threat mitigations, explore efficient reconstitution methodologies, and evaluation architecture modernization impacts.
4. **Emerging Solutions** – Continue to advance the state of practice with new solutions that fill key gaps.

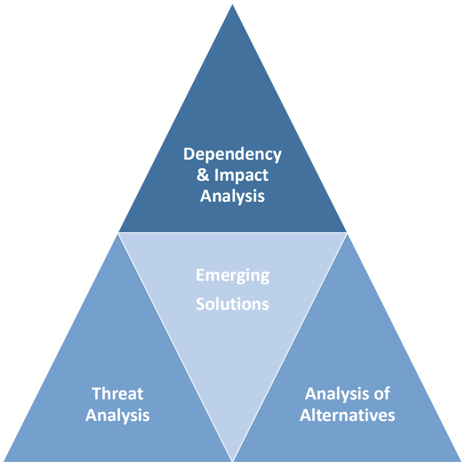


Figure 1: Core CDSA Capabilities

Within MITRE, we believe in leveraging the current COTS tools for cyber defense situational awareness. Many great products have the flexibility and scale to handle most enterprise workloads. The challenge is tailoring each product for maximum utility with the specific deployment environment.

While there are many successes and examples of leveraging COTS products for cyber SA for ourselves (protecting MITRE) and our sponsors, a majority of MITRE's research and development in this cyber security focuses on the remaining three CDSA capabilities: threat analysis, dependency & impact analysis, and analysis of alternatives. Overall, there are ten MITRE efforts that could provide immediate benefit to NATO/NCIA CDSA. Seven efforts directly support one of the three CDSA capabilities, and three are experimental CDSA efforts that take different approaches to the CDSA problem.

Table 1 and Figure 2 provide an overview of these ten MITRE efforts. The remainder of this document focuses on describing each effort and the effort's benefits to the NATO CDSA. Descriptions include an overview of the effort along with any relevant screenshots or diagrams.

Table 1: MITRE Efforts by CDSA Capability

Threat Analysis	CRITs ATT&CK™ STIX™, TAXII™
Dependency & Impact Analysis	CyCS CJA
Analysis of Alternatives (AoA)	TARA
Emerging Solutions	FACT CyGraph AMICA

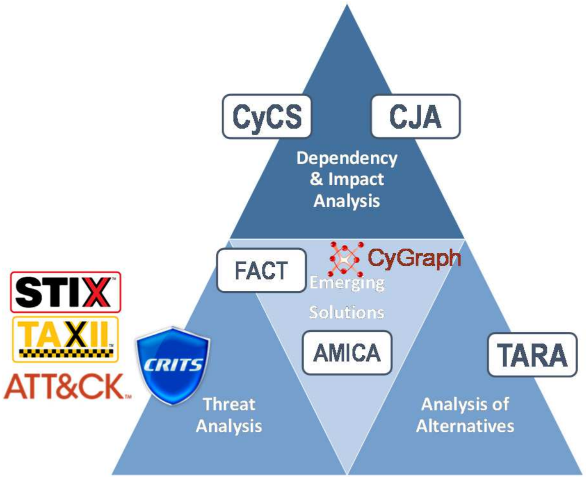


Figure 2: MITRE Efforts by CDSA Capability Area

Motivating Example

The following example is based on the primary scenario defined in the NATO CDSA RFI [1]:

> *Country Appelestan is being supported by the NATO-led RATM coalition whilst they rebuild a stable government following the fall of a dictator. Hostile Nation Oranjeland is interested in understanding the technologies and intelligence capabilities used by the RATM coalition. The aim of Oranjeland is to infiltrate the network and exfiltrate information using covert techniques to try to avoid detection.*

In order to provide a context for usage, we provide a motivating example that ties together the MITRE capabilities as used within the primary CDSA RFI use case (specific capabilities and additions have been *highlighted in italics*):

> A network administrator in the RATM Network Operations Centre (NOC) uses *newly received CRITs indicators regarding new adversary campaign TTP*. These CRITs threat indicators were received from the NOCs of several NATO member nations using *STIX & TAXII threat sharing standards*. Cross-referencing those indicators *indicating ATT&CK Custom application layer protocol Command and Control techniques*, he notices unusual network activity, which has not

been detected by the antivirus, on a server at Regional Command North (RC-N), indicating the presence of that Advanced Persistent Threat (APT).

He contacts the NATO Cyber Security Operations (CSOps), who create an incident ticket. CSOps does a series of initial investigations using *CyGraph*, and identifies this to be an Integrated Command and Control system (ICC) server. *CJA indicates that this is critical asset as it is required by many regional missions.* They collate all relevant information and options into a report and then they contact the Comprehensive Crisis and Operations Management Centre (CCOMC) Cybercell (CCC). Using *TARA to perform AoA and FACT to situate the recommendations within the overall mission context*, they recommend the course of action to disconnect the ICC server to disrupt the APT. CCC uses *CyCS* to identify that a planned mission will be effected by this mitigation. CCC then uses *AMICA* to assess the wider implications of disconnecting the server, e.g., planned downtime with respect to mission need, available cyber defender resources, and potential mission impacts of the APT (e.g. exfiltration of data).

Figure 3 illustrates the flow of information and relevant MITRE solutions for this example.

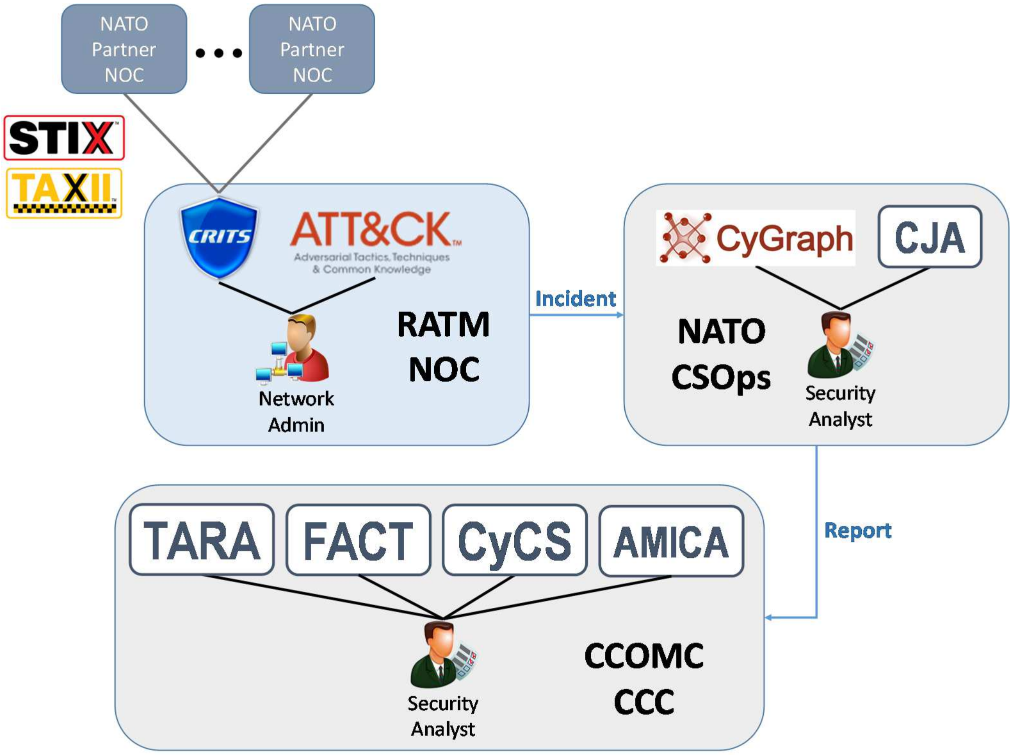


Figure 3: MITRE solutions for motivating example

Structured Threat Information eXpression (STIX) & Trusted Automated eXchange of Indicator Information (TAXII)

STIX™ (Structured Threat Information eXpression) is a standardized language for cyber threat information. STIX [2] provides “structured representations of cyber threat information that is expressive, flexible, extensible, automatable, and readable. STIX enables the sharing of comprehensive, rich, ‘high-fidelity’ cyber threat information across organizational, community, and product/service boundaries.

STIX extends simple indicator sharing to enable the management and exchange of significantly more expressive sets of indicators as well as other full-spectrum cyber threat information."

While having a standardized threat language is beneficial, the real value is achieved through threat sharing. TAXII™ (Trusted Automated eXchange of Indicator Information) defines such an automated information exchange service for sharing STIX threat indicators. TAXII [3] enables "sharing of actionable cyber threat information across organization and product/service boundaries. TAXII defines services, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats… TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose all while using a single, common set of tools."

Accurate and up-to-date threat intelligence information is critical for identifying threats as well as analyzing the system architecture for potential weaknesses. A CDSA solution should correlate the gathered real-time situational awareness, system and mission models, and threat analyses. STIX is the de facto standardized representation to exchange threat indicators, enabling CDSA complementary tool use (CDSA RFI Use Case UC09). TAXII enables easy, cross-domain sharing and aggregation of the STIX indicators, allowing the CDSA to support RFI Use Case UC35 by pulling threat data from all accessible TAXII end points. STIX has been implemented in several commercial products and is being used by many United States Department of Defense (DoD) customers along with many of MITRE's situational awareness and cyber defense efforts. TAXII is being leveraged to interconnect U.S. government cyber operations centers under a February 2015 Executive Order from U.S. President Barack Obama promoting cybersecurity information sharing [4]. A partial listing of STIX and TAXII adopters can be found at http://stixproject.github.io/supporters/#products-and-services.

MITRE and STIX/TAXII played a key role in recent cyber training exercises, called Cyber Yankee (http://www.thenationsfirst.org/cyber-training-unites-new-england.html). This event brought together U.S. Army National Guard Cyber Network Defense Teams from across the New England Region (6 states), with support from numerous federal government agencies, including the Department of Homeland Security, the Federal Emergency Management Agency, the Federal Bureau of Investigation and the U.S. Secret Service. In these exercises, MITRE helped plan scenarios and trained teams in leveraging STIX/TAXII for threat information. This structured language provided a common framework for intelligence analysts to organize and coordinate their understanding of evolving threats. A member of the MITRE team was awarded a commemorative coin for his role in these exercises, especially in STIX/TAXII training.

"I have been involved in cyber exercises for many years at the national and regional levels," said Lt. Col. Woody Groton, New Hampshire Army National Guard, who served as director of Cyber Yankee and sits on the national exercise planning team for the US DoD. "Never have I seen intelligence better integrated within an exercise. This is a model for all others to follow and build upon."

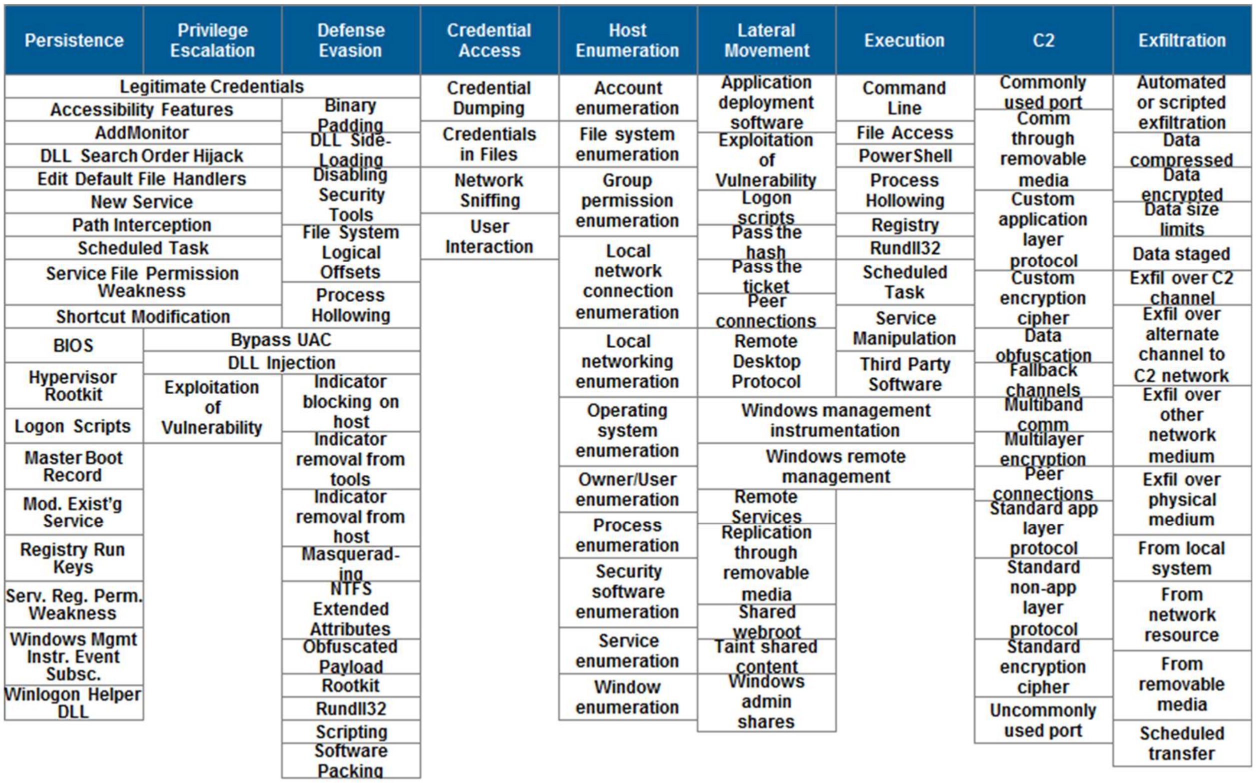
As of July 2015, MITRE has transitioned oversight of the STIX and TAXII effort to the Organization for the Advancement of Structured Information Standards (OASIS) for adoption under the Cyber Threat Intelligence (CTI) Technical Committee [5]. OASIS is an internationally recognized standardization group that will allow broader access to STIX and TAXII.

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) [6] is a MITRE-developed framework for modeling and categorizing the post-exploit actions of an advanced persistent threat (APT). The ATT&CK "model can be used to better characterize and describe post-access adversary behavior. It both expands the knowledge of network defenders and assists in prioritizing network defense by detailing the post-initial access (post exploit and implant) tactics, techniques, and procedures (TTP) advanced persistent threats (APT) use to execute their objectives while operating inside a network."

The most recent version of ATT&CK divides post-exploit APT TTPs into nine categories. ATT&CK identifies 95 different APT techniques, which are associated with one or more of the nine categories. Figure 4 provides an overview of these mappings.

The latest ATT&CK releases can be found at https://attack.mitre.org.



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials Accessibility Features AddMonitor DLL Search Order Hijack Edit Default File Handlers New Service Path Interception Scheduled Task Service File Permission Weakness Shortcut Modification BIOS Hypervisor Rootkit Logon Scripts Master Boot Record Mod. Exist'g Service Registry Run Keys Serv. Reg. Perm. Weakness Windows Mgmt Instr. Event Subsc. Winlogon Helper DLL	Legitimate Credentials Accessibility Features AddMonitor DLL Search Order Hijack Edit Default File Handlers New Service Path Interception Scheduled Task Service File Permission Weakness Shortcut Modification Bypass UAC DLL Injection Exploitation of Vulnerability	Legitimate Credentials Binary Padding DLL Side-Loading Disabling Security Tools File System Logical Offsets Process Hollowing Bypass UAC DLL Injection Indicator blocking on host Indicator removal from tools Indicator removal from host Masquerad-ing NTFS Extended Attributes Obfuscated Payload Rootkit Rundll32 Scripting Software Packing	Credential Dumping Credentials in Files Network Sniffing User Interaction	Account enumeration File system enumeration Group permission enumeration Local network connection enumeration Local networking enumeration Operating system enumeration Owner/User enumeration Process enumeration Security software enumeration Service enumeration Window enumeration	Application deployment software Exploitation of Vulnerability Logon scripts Pass the hash Pass the ticket Peer connections Remote Desktop Protocol Windows management instrumentation Windows remote management Remote Services Replication through removable media Shared webroot Taint shared content Windows admin shares	Command Line File Access PowerShell Process Hollowing Registry Rundll32 Scheduled Task Service Manipulation Third Party Software Windows management instrumentation Windows remote management	Commonly used port Comm through removable media Custom application layer protocol Custom encryption cipher Data obfuscation Fallback channels Multiband comm Multilayer encryption Peer connections Standard app layer protocol Standard non-app layer protocol Standard encryption cipher Uncommonly used port	Automated or scripted exfiltration Data compressed Data encrypted Data size limits Data staged Exfil over C2 channel Exfil over alternate channel to C2 network Exfil over other network medium Exfil over physical medium From local system From network resource From removable media Scheduled transfer

Figure 4: ATT&CK Technique-Category Mappings

ATT&CK provides a meta-standard that aligns with NATO CDSA RFI Use Case UC25, enabling operators to categorize and track threat indicators as well as map them against potential Courses of Action (CoAs). The most obvious way is to supplement the STIX indicator information with proper ATT&CK technique and category identification. By storing the associated ATT&CK information in the CDSA, a cyber defender can perform more broad analysis across the real-time information. For example, instead of trying to query for all `at.exe` and `psexec`[1], they can instead search for all instances of ATT&CK Lateral

[1] Microsoft Sysinternals PsExec: https://technet.microsoft.com/en-us/sysinternals/bb897553

Movement techniques <https://attack.mitre.org/wiki/Lateral_Movement>. This is useful for not only monitoring and detecting sequences APT post-exploit activities, but also for supporting AoA and identifying defenses to counter entire categories of APT behavior.

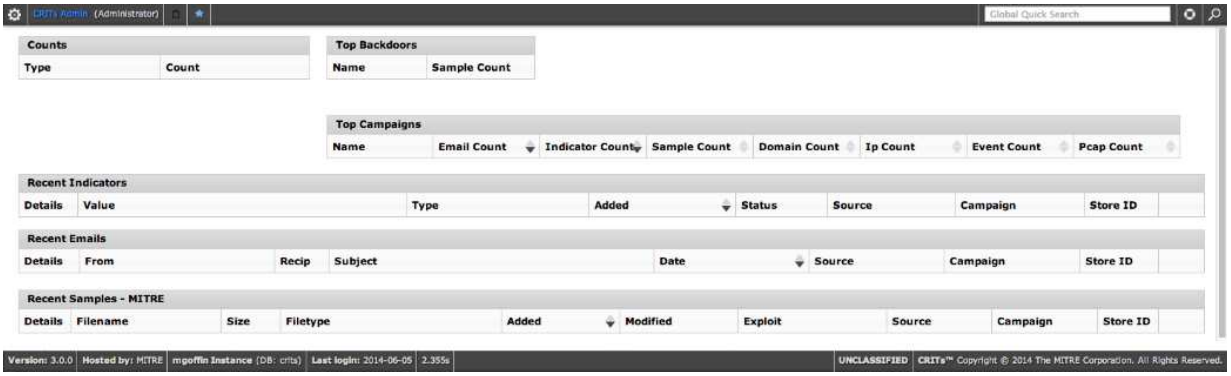
ATT&CK has been refined over the past couple of years in support of internal MITRE research and various US DoD sponsor projects. While not complete, it has proved an invaluable threat categorization framework for identifying sensor and detection gaps as well as developing AoA resiliency approaches and countermeasures.

Collaborative Research Into Threats (CRITs)

Collaborative Research Into Threats (CRITs) [7] is an extensible and collaborative defense platform for malware and threat data. CRITs combines multiple free-and-open source software (FOSS) solutions "to create a unified tool for analysts and security experts engaged in threat defense. It has been in development since 2010 with one goal in mind: give the security community a flexible and open platform for analyzing and collaborating on threat data. In making CRITs free and open source, [CRITs] can provide organizations around the world with the capability to quickly adapt to an ever-changing threat landscape."

The CRITs framework is an open-source effort and is available at: http://crits.github.io/

Once CRITs has been installed and configured, it can be populated manually or connected with other threat-sharing partners. The preferred input and collaboration format is through using the CRITs TAXII service to share STIX formatted threat indicators. These indicators can be further classified and categorized based upon the associated ATT&CK technique(s). Figure 5 shows an unpopulated CRITs dashboard that allows an operator to quickly identify the most recent and popular malware and backdoors, indicators, and APT campaigns.



Counts

Type	Count

Top Backdoors

Name	Sample Count

Top Campaigns

Name	Email Count	Indicator Count	Sample Count	Domain Count	Ip Count	Event Count	Pcap Count

Recent Indicators

Details	Value	Type	Added	Status	Source	Campaign	Store ID

Recent Emails

Details	From	Recip	Subject	Date	Source	Campaign	Store ID

Recent Samples - MITRE

Details	Filename	Size	Filetype	Added	Modified	Exploit	Source	Campaign	Store ID

Version: 3.0.0 | Hosted by: MITRE | mgoffin Instance (DB: crits) | Last login: 2014-06-05 | 2.355s

UNCLASSIFIED | CRITs™ Copyright © 2014 The MITRE Corporation. All Rights Reserved.

Figure 5: CRITs Dashboard

CRITs supports NATO CDSA RFI Use Cases UC25 (Monitor Specific Threat) and UC29 (View historical incidents by asset) by providing a single interface through which the CDSA can obtain a warehouse of threat intelligence. Such data includes threat actor, campaign indicator, APT tools, malware, and other APT TTP intelligence that can be used by a CDSA to supplement traditional vulnerability analyses and influence analysis of alternatives (AoA) prioritization. CRITs supports STIX and TAXII out of the box, and can easily be extended for tagging threat information with ATT&CK technique and category attribution.

CRITs was developed by MITRE's internal information security team to address a need for threat intelligence tracking. Since then, it has been transitioned to multiple US sponsors for use by their cyber operations teams. The core CRITs platform is offered as FOSS to the greater cyber intelligence community and is being evaluated and used by multiple researchers and organizations.

Crown Jewels Analysis (CJA)

MITRE's *Crown Jewels Analysis* (CJA) [8] is a process and corresponding toolset for "identifying those cyber assets that are most critical to the accomplishment of an organization's mission."

CJA creates a dependency map (Figure 6) to help understand what is most critical – beginning during system development and continuing through system deployment. The dependency map starts with identifying missions and assigning relative prioritization. From there, dependencies flow down through operational tasks and system function to cyber assets. These dependencies are expressed qualitatively in terms of impact on a parent node resulting from a failed or degraded child node, with provisions to minimize subjectivity. With a complete model, CJA can predicts the impact of a cyber asset failure/degradation as the realization of each parent/child logical statement, tracing the potential impact upward to high-level mission tasks and objectives.

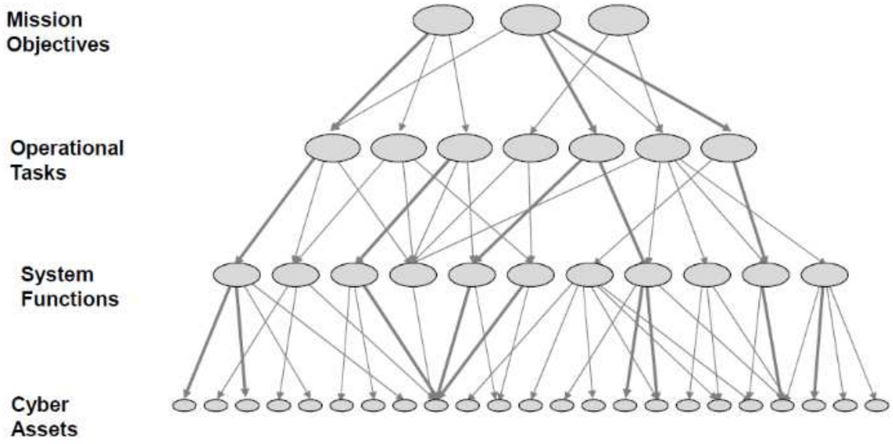


Figure 6: CJA Dependency Map

CJA supports NATO CDSA RFI Use Cases UC01, UC03, UC06, and UC19 regarding identification, navigation, and aggregation of cyber assets. A CDSA requires some sort of dependency map to associate missions, data flows, and cyber assets. CJA provides such a model along with the methodology to "roll up" cyber asset criticality based on higher-order associations, such as mission or operational priorities. The CJA model can also be inverted (Figure 7), allowing a CDSA to identify potential mission impacts of an incident to prioritize analyses. Additional information, such as that provided by TARA, can be used to supplement this information to include threat priorities and mitigation availability.

Both CyCS and TARA leverage the CJA methodology. CJA is being used by the U.S. DoD for acquisition programs, to meet requirements for mission-critical functions when protecting warfighting abilities. It has also been applied to fielded weapons systems, as well as a tabletop (hypothetical) system, demonstrating how the flexible methodology applies to various system lifecycle stages. CJA is also used for infrastructure and SCADA system analysis, like its predecessor RiskMAP [9]. Overall, CJA has been applied to 10 different systems, including for a foreign (non-U.S.) military customer.

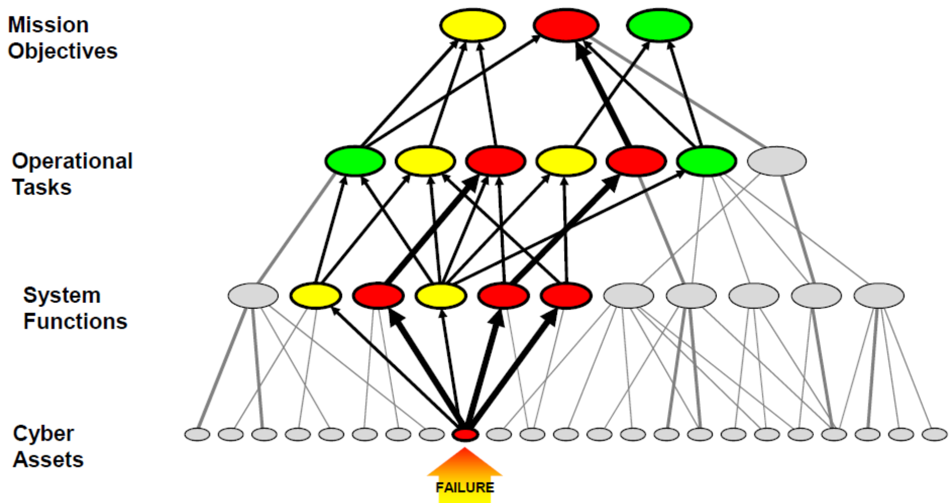
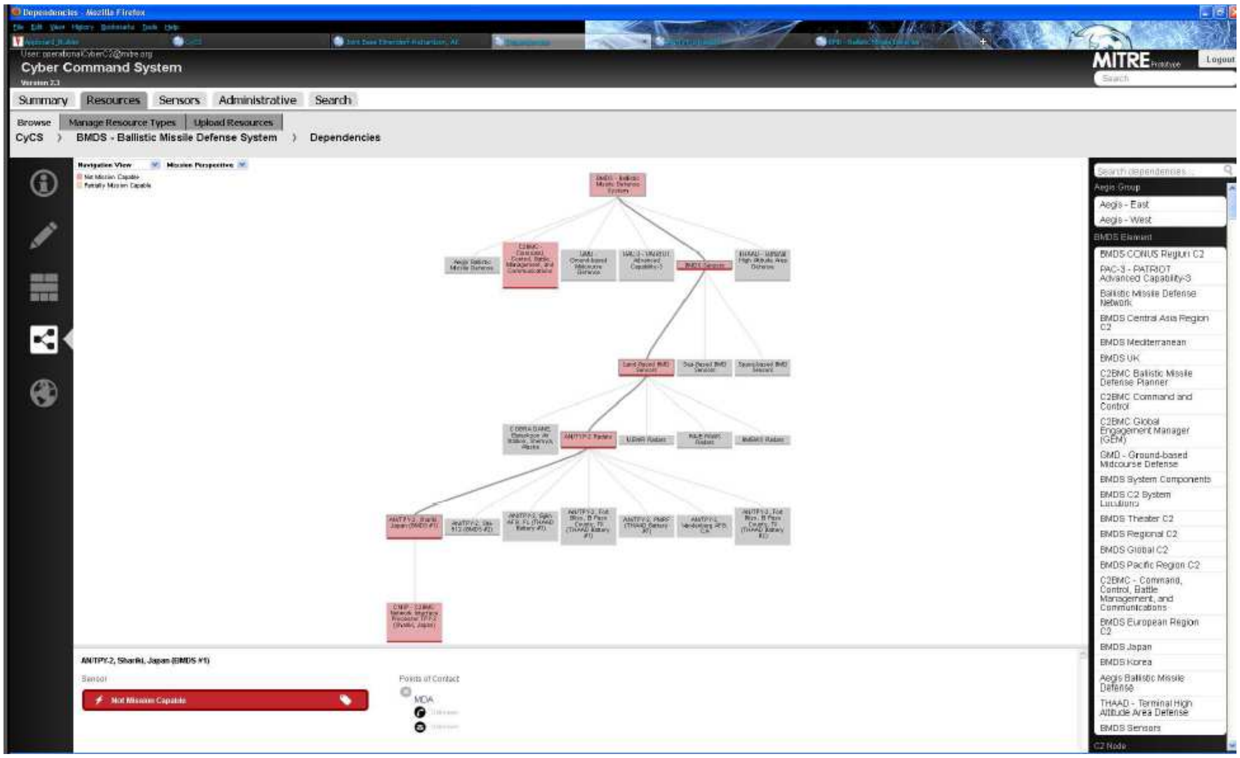


Figure 7: Assessing Failure Impact

Cyber Command System (CyCS)

Cyber Command System (CyCS) [10] is MITRE's proof-of-concept cyber situational awareness tool. CyCS "addresses the objective of improved mission assurance in cyberspace by enabling the mapping of mission operations to the network operations that support those missions. This tool provides mission-impact assessment through situational awareness and impact analysis. CyCS addresses mission-assurance challenges for highly distributed enterprise systems of systems through vulnerability, threat, and consequence management."


Dependencies - Mozilla Firefox
File Edit View History Bookmarks Tools Help
CyCS
Cyber Command System
Version 2.3
MITRE Prototype
Logout
Search
Summary
Resources
Sensors
Administrative
Search
Browse
Manage Resource Types
Upload Resources
Navigation View
Mission Perspective
Not Mission Capable
Partially Mission Capable
BMDS - Ballistic Missile Defense System
Aegis Ballistic Missile Defense
C2BMC - Command, Control, Battle Management, and Communications
GMD - Ground-based Midcourse Defense
PAC-3 - PATRIOT Advanced Capability-3
BMDS Sensors
THAAD - Terminal High Altitude Area Defense
Land-Based BMD Sensors
Sea-Based BMD Sensors
Space-based BMD Sensors
COBRA DANE
AN/TPY-2 Radars
UEWR Radars
Radars
Radars
AN/TPY-2, Shariki, Japan (BMDS #1)
C2BMC Network Interface Processor
Search dependencies...
Aegis Group
Aegis - East
Aegis - West
BMDS Element
BMDS CONUS Region C2
PAC-3 - PATRIOT Advanced Capability-3
Ballistic Missile Defense Network
BMDS Central Asia Region C2
BMDS Mediterranean
BMDS UK
C2BMC Ballistic Missile Defense Planner
C2BMC Command and Control
C2BMC Global Engagement Manager (GEM)
GMD - Ground-based Midcourse Defense
BMDS System Components
BMDS C2 System Locations
BMDS Theater C2
BMDS Regional C2
BMDS Global C2
BMDS Pacific Region C2
C2BMC - Command, Control, Battle Management, and Communications
BMDS European Region C2
BMDS Japan
BMDS Korea
Aegis Ballistic Missile Defense
THAAD - Terminal High Altitude Area Defense
BMDS Sensors
C2 Node

User: operationalCyberC2@mitre.org

CyCS 〉 BMDS - Ballistic Missile Defense System 〉 Dependencies

AN/TPY-2, Shariki, Japan (BMDS #1)

Sensor

Not Mission Capable

Points of Contact

MDA

Figure 8: CyCS Mission Dependency View [11]

CyCS follows the well-known observe-orient-decide-act (OODA) loop in its design. Its *monitoring* subsystem observes the cyber environment, with modules for information sources, collections management, information product storage/retrieval, graphical displays, and reporting. The *analysis* subsystem orients warfighters through modules for alerting, automated and ad hoc analyses, and situation "case" management. The *decision support* subsystem helps warfighters make informed decisions, with modules for guidance, authorization, planning, and orders management. The *tasking* subsystem helps operators take action through modules for resource readiness and assignment, task queue management and routing, and execution monitoring.

While the CyCS proof of concept is not a full CDSA solution, it does meet a majority of the high level NATO CDSA RFI Use Cases including UC01, UC03-UC07, UC09-UC12, UC23, UC24, UC26, and UC27. CyCS provides the major overall views for asset and mission dependencies. Assuming assets are geo-located, CyCS can interoperate with geospatial tools such as Google Earth to view incidents and assets based on their geographic locations. Since CyCS was primarily developed as a modular knowledge management solution, it can act as a single authoritative data source (UC10), easily importing new data sources, interacting with complementary tools (UC09), or creating new visualizations (UC26). Additional use cases can be met by integrating CyCS with TARA to provide AoA (UC08) with CRITs for analyses within the context of specific threats (UC25) as seen in CyGraph.

MITRE has multiple ongoing activities in demonstrating advanced cyber SA capabilities through CyCS. This includes engagements with warfighters at every level, e.g., national-level command, US combatant commands, individual agencies, and within various armed services.

Threat Assessment and Remediation Analysis (TARA)

The *Threat Assessment and Remediation Analysis (TARA)* solution defines a methodology for assessing a cyber architecture to identify cyber vulnerabilities and evaluate countermeasure effectiveness. The TARA assessment approach [12] is described as "conjoined trade studies, where the first trade identifies and ranks attack vectors based on assessed risk, and the second identifies and selects countermeasures based on assessed utility and cost. Unique aspects of the [TARA] methodology include use of catalog-stored mitigation mappings that preselect plausible countermeasures for a given range of attack vectors, and use of countermeasure selection strategies that prescribe the application of countermeasures based on level of risk tolerance."

TARA uses the three-step assessment methodology shown in Figure 9. The first step is the knowledge management (KM). KM provides and up-to-date catalog of external threat vectors and countermeasure information that is used to evaluate each system architecture. The next step is to perform the cyber threat susceptibility analysis (CTSA) on the target architecture. The CTSA leverages CJA along with CRITs and STIX definitions to identify vulnerabilities within the system architecture. CTSA produces a vulnerability matrix that is used during the final step – cyber risk remediation assessment (CRRA). The CRRA uses this matrix in conjunction with the KM countermeasure knowledge to develop a playbook. The TARA playbook provides a prioritized list of countermeasures and alternative CoAs for the evaluated architecture and can be adjusted to reflect risk, cost, or schedule constraints.

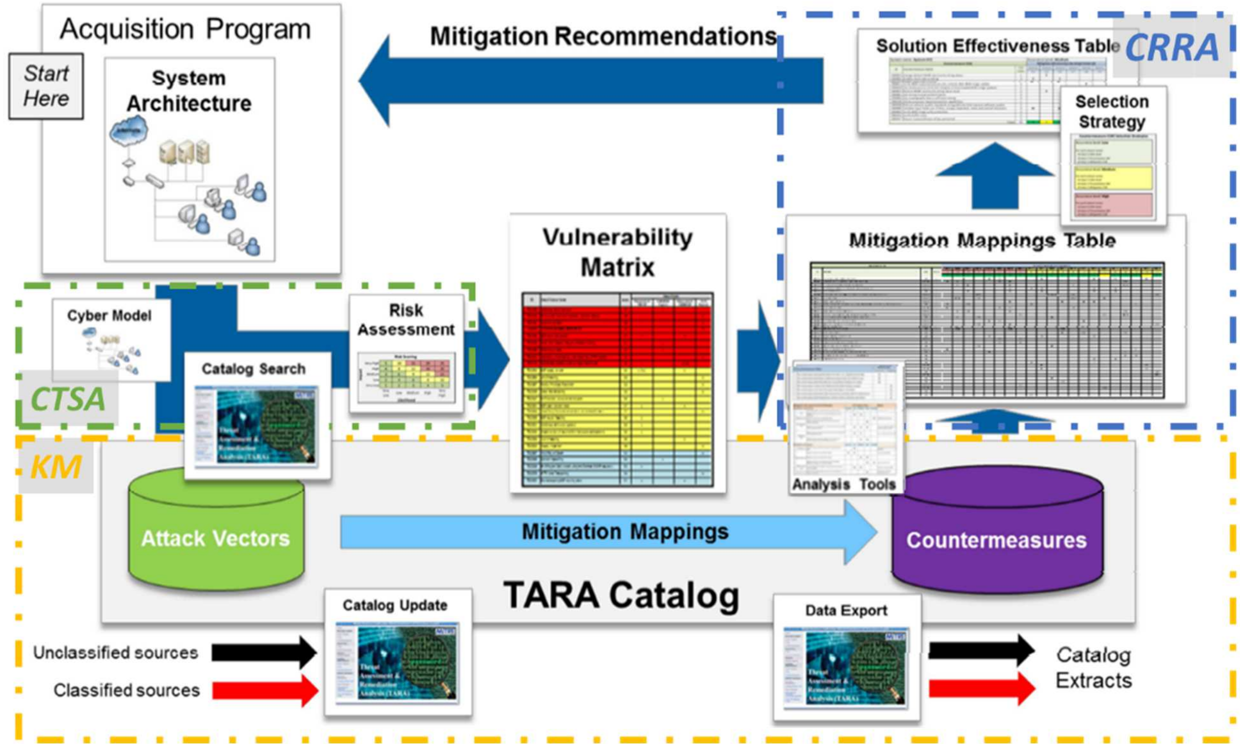


Figure 9: TARA Assessment Workflow

TARA meets NATO CDSA RFI Use Cases UC08 and UC27, providing a CDSA with analysis-of-alternatives (AoA) by generating and selecting prioritized CoA options. This provides the CDSA operators with improved decision support by factoring in details such as threat vectors and known countermeasures or CoAs. The generated TARA playbook of alternatives provides additional flexibility by allowing the user to tune the alternatives based upon external criteria such as the available resources or schedule constraints for time-sensitive operations or logistical complexities. However, the TARA AoA results are only as good as the knowledge it's supplied. Due to this limitation, TARA makes it easy to populate attack vector information using STIX or CRITs, and can leverage CJA and CyCS for the system and mission dependency models.

MITRE has used TARA to evaluate dozens of US DoD programs. While the supporting TARA tools and catalog are not publicly available, the underlying methodology described in [12] can still be implemented as part of the NATO CDSA.

Emerging CDSA Solutions

Federated Analysis of Cyber Threats (FACT)

Federated Analysis of Cyber Threats (FACT) [15] is one MITRE-funded research effort to build a CDSA targeted towards architecture assessment and incident responses platform. While traditional CDSA capabilities, including those specified for the NATO CDSA RFI [1], focus on real-time or near real-time situational awareness for cyber defenders, FACT is designed to be used to support the system engineering, recovery, and re-architecting processes required for incident response or acquisition.

FACT combines the functionality of other MITRE efforts including CRITs, TARA, and CyCS into a post hoc analysis and incident response platform (Figure 10). Cyber threat intelligence sources including threat indicators, threat actors, and campaign intrusion sets are exported from CRITs using STIX. This information is combined with the system and mission models from CyCS to develop a TARA Playbook. This Playbook contains a selection of alternative Courses of Action (CoAs) of potential incident responses.

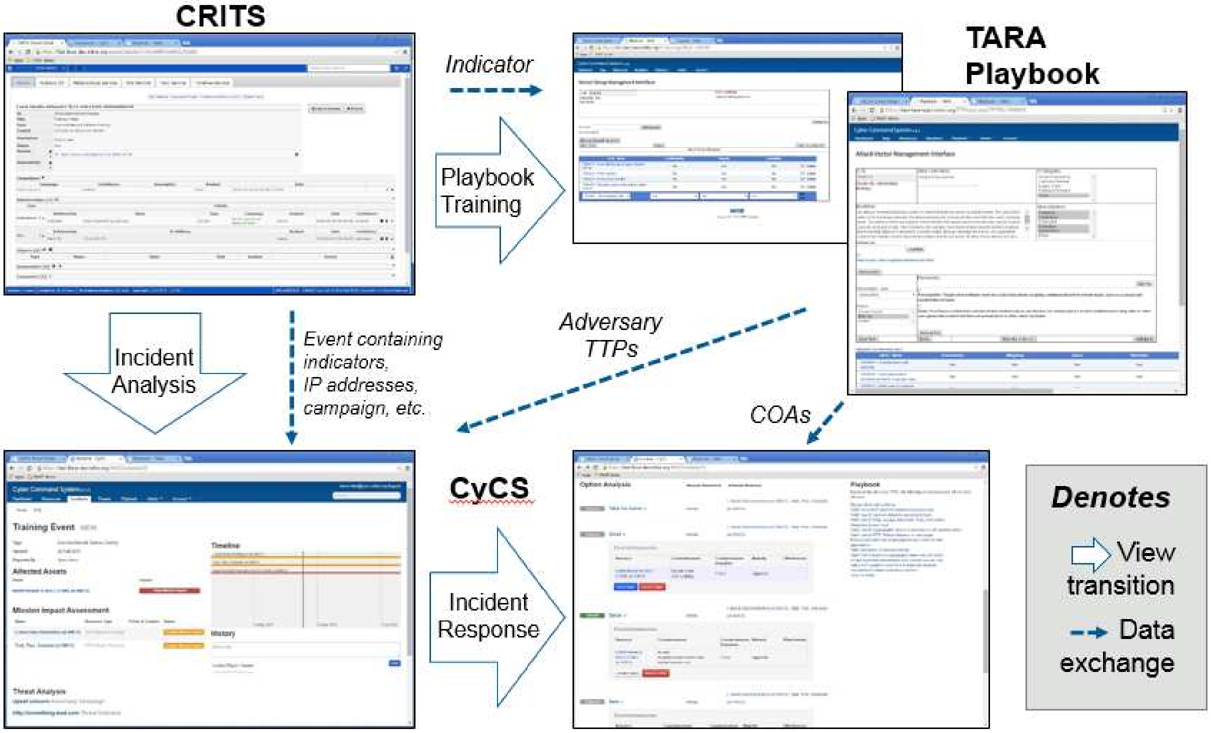


Figure 10: FACT Integration of MITRE CDSA Efforts

While FACT is targeting a different set of use cases than the NATO RFI CDSA, NATO can still leverage FACT and its concepts to support CDSA RFI Use Cases UC08 and UC27. FACT could be integrated directly as an incident response manager or the concepts can be used to build a real-time AoA capability and countermeasure evaluation platform. Additionally, FACT proves that the data required to support a CDSA is also useful to support the engineering, recovery, and re-architecting processes required for incident response or acquisition.

CyGraph: Big-Data Analytics for Network Attack Mapping

CyGraph is an emerging MITRE effort focused on real-time cyber situational awareness, bringing together isolated data and events into an ongoing overall picture for decision support and situational awareness. CyGraph [13] is a tool for “cyber warfare analytics, visualization, and knowledge management… It helps prioritize exposed vulnerabilities, alone and in combination, in the context of mission-critical assets. In the face of actual attacks, CyGraph provides context for correlating intrusion alerts and matching them to known vulnerability paths, and for suggesting best courses of action for responding to attacks. For post-attack forensics, [CyGraph] suggests vulnerable paths that may warrant deeper inspection.”

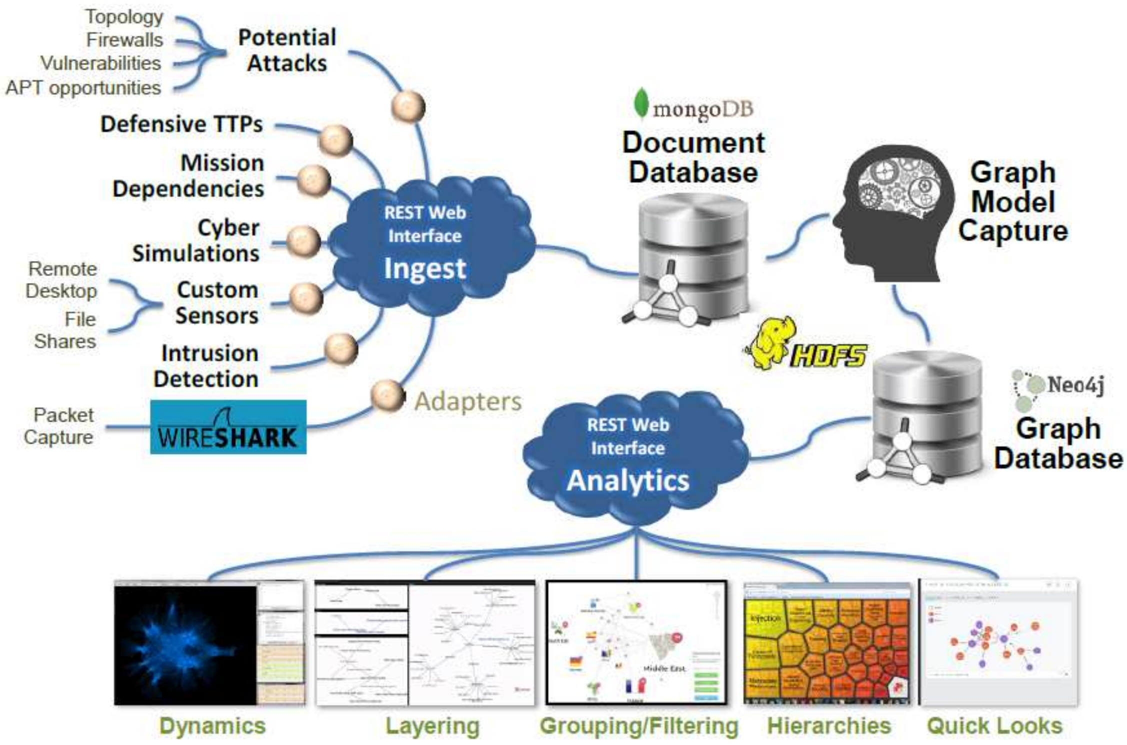


Figure 11: CyGraph Architecture

CyGraph builds an attack-graph model that maps the potential attack paths through a network. This includes any network attributes that potentially contribute to attack success, such as network topology, firewall rules, host configurations, and vulnerabilities. The dynamically evolving attack graph provides context for reacting appropriately to attacks and protecting mission-critical assets. CyGraph then ingests network events such as intrusion detection alerts and other sensor outputs, including packet capture. It also incorporates mission dependencies, showing how mission objectives, tasks, and information depend on cyber assets.

Overall, CyGraph is the MITRE capability most similar to the NATO CDSA RFI. Since it builds on other efforts, including CyCS and CJA, CyGraph is able to supplement their mission dependency capabilities with real-time sensor and attack path analysis, providing support for the CDSA RFI Use Cases UC13 (Monitor network) and UC15 (Fuse data). CyGraph also provides a number of visualizations and view options requested for UC04, UC11, UC12, and UC26.

Analyzing Mission Impacts of Cyber Actions (AMICA)

Analyzing Mission Impacts of Cyber Actions (AMICA) provides an emerging, lightweight CDSA capability for understanding mission impacts of cyber attacks. AMICA combines process modeling, discrete-event simulation, graph-based dependency modeling, and dynamic visualizations. This is a novel convergence of two lines of research: process modeling/simulation and automated attack graph generation.

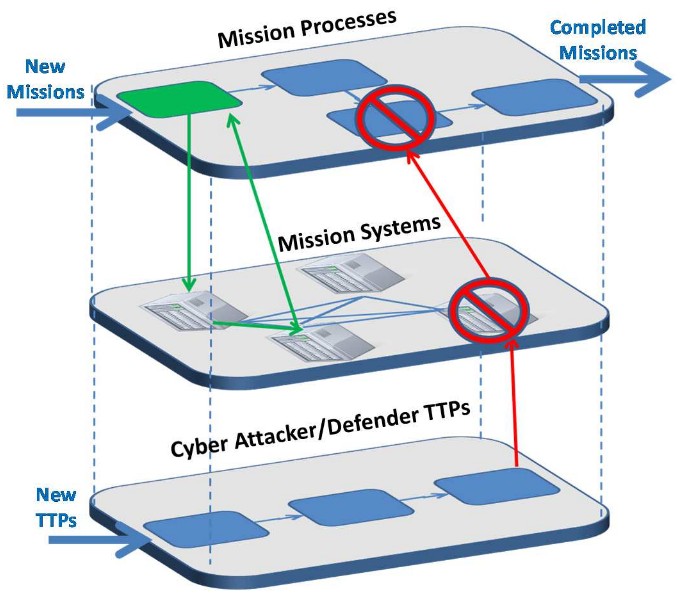


Figure 12: AMICA Model

AMICA captures process flows for modeling mission tasks as well as cyber attacker and defender TTPs. Vulnerability dependency graphs map network attack paths, and mission-dependency graphs define the hierarchy of high-to-low-level mission requirements mapped to cyber assets. Through simulation of the resulting integrated model, AMICA quantifies impacts in terms of mission-based measures, for various mission and threat scenarios. Dynamic visualization of simulations (via CyGraph) provides deeper understanding of cyber warfare dynamics, for situational awareness in the context of simulated conflicts.

Understanding mission resilience to cyber warfare requires bringing together layers of information from numerous sources. At the lower layers, network topology, firewall policies, intrusion detection systems, system configurations, vulnerabilities, etc., all play a part. AMICA combines these into a higher-level attack graph model that shows transitive paths of vulnerability. It also maps cyber assets to mission requirements (via CyCS), and captures dependencies from low-level requirements to higher-level ones appropriate for decision making. Because mission requirements are highly dynamic, AMICA captures time-dependent models of mission flow. Cyber attacks and defenses are similarly dynamic – and are also captured in AMICA process models for simulating mission impact of cyber activities.

In the context of the NATO CDSA RFI Use Cases, AMICA inherits all of CyGraph's capabilities and additionally fulfills the UC21 requirement for training and simulation. The AMICA process models can be used to exercise the architecture to simulate threat scenarios, allowing operators to evaluate potential mission impact and AoA effectiveness. Operators can simulate the effects of various CoA countermeasures, tweaking variables such as time and success rates, to choose the more appropriate for the given environment or scenario.

While an emerging capability, AMICA has been demonstrated through a case study working with DoD operators on a real-world kinetic mission. AMICA was used to model, simulate, and quantify the impact of cyber attacks on the target mission using various attack scenarios against different phases of the target-development process.

Summary

MITRE has a depth of system engineering experience and range of technical solutions that would benefit any toolkit for advanced cyber situation awareness. At tactical and strategic levels, these solutions include *threat intelligence* to understand and track threat landscapes and threat actor TTPs; analysis to understand *dependencies among mission components and cyber assets and potential mission impacts* of cyber threats; and *analysis of alternatives* for threat mitigations, response/reconstitution methodologies, and architecture modernization. There is also a wide range of ongoing research at

MITRE, as showcased by our *emerging solutions* to key problems in CDSA. For more operational use cases, MITRE has had much success in *leveraging COTS tools* and combining them with our tactical/strategic solutions.

Figure 13 summarizes how MITRE solutions span all these aspects of CDSA.

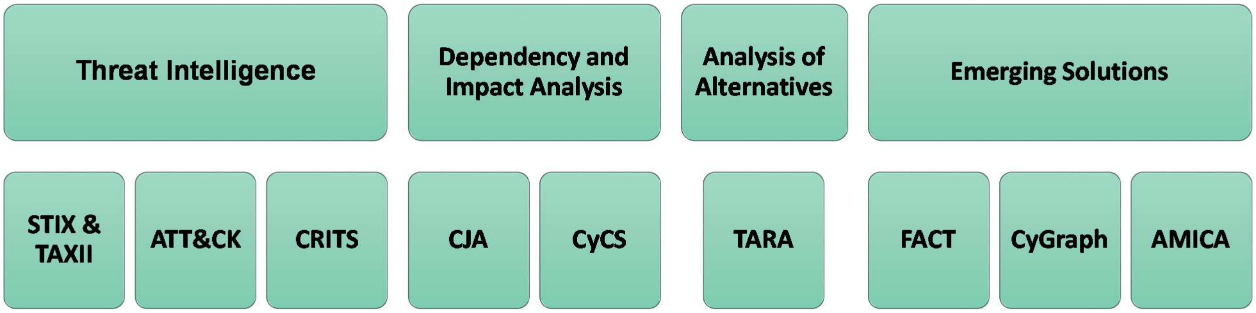


Figure 13: MITRE Solutions for CDSA

References

[1] G. Hindle, "Cyber Defence Situational Awareness Demonstration/Request for Information (RFI) from Industry and Government (CO-14068-MNCD2)," NCI Agency Acquisition, 2015.

[2] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)," 20 February 2014. [Online]. Available: http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf.

[3] J. Connolly, M. Davidson and C. Schmidt, "The Trusted Automated eXchange of Indicator Information (TAXII™)," 2 May 2014. [Online]. Available: http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_May_2014.pdf.

[4] T. Pager, "Private sector remains wary of government efforts to increase cybersecurity collaboration," 19 March 2015. [Online]. Available: http://nationalsecurityzone.org/site/private-sector-remains-wary-of-government-efforts-to-increase-cybersecurity-collaboration/.

[5] A. M. Freed, "DHS Transitions STIX , TAXII and CybOX Standards to OASIS," 29 July 2015. [Online]. Available: http://darkmatters.norsecorp.com/2015/07/29/dhs-transitions-stix-taxii-and-cybox-standards-to-oasis/.

[6] The MITRE Corporation, "ATT&CK," The MITRE Corporation, 20 May 2015. [Online]. Available: https://attack.mitre.org/wiki/Main_Page.

[7] M. Goffin, "CRITs: Collaborative Research Into Threats," The MITRE Corporation, 2014. [Online]. Available: https://crits.github.io/.

[8] The MITRE Corporation, "Crown Jewels Analysis," September 2013. [Online]. Available: http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

[9] Institute for Information Infrastructure Protection (I3P), "RiskMAP: Finding your corporate risks," February 2009. [Online]. Available: http://www.thei3p.org/docs/publications/riskmap-2009-02-09.pdf.

[10] The MITRE Corporation, "Cyber Command System (CyCS)," [Online]. Available: http://www.mitre.org/research/technology-transfer/technology-licensing/cyber-command-system-cycs.

[11] S. Foote, "Cyber Operations: Capability Research & Development," 2012.

[12] J. Wynn, "Threat Assessment and Remediation Analysis (TARA)," 1 October 2014. [Online]. Available: http://www.mitre.org/publications/technical-papers/threat-assessment-and-remediation-analysis-tara.

[13] S. Noel, E. Harley, K. H. Tam, G. Gyor, B. King, S. Kim and R. Grullon, "CyGraph: Flexible and Dynamic Cyber Graph Analysis and Visualization," [Online].

[14] J. Wynn, J. Whitmore, G. Upton, L. Spriggs, D. McKinnon, R. McInnes, R. Graubart and L. Clausen, "Threat Assessment & Remediation Analysis (TARA)," September 2012. [Online]. Available: http://www.mitre.org/publications/technical-papers/threat-assessment--remediation-analysis-tara.

[15] J. Wynn, "Federated Analysis of Cyber Threats (FACT): Capstone Overview," The MITRE Corporation, 2015.

[16] S. Noel, J. Ludwig, P. Jain, D. Johnson, R. K. Thomas, J. McFarland, B. King, S. Webster and B. Tello, "Analyzing Mission Impacts of Cyber Actions (AMICA)," 2015.

Appendix: RFI Use Case Capability Mapping

RFI Use Case	MITRE Solution
UC01 **View current risks list, ordered by impact, showing geographic location**	• Crown Jewels Analysis (CJA) • Cyber Command System (CyCS)
UC03 **Drill down / Roll up**	• Crown Jewels Analysis (CJA) • Cyber Command System (CyCS)
UC04 **Hierarchical view (tailored)**	• Cyber Command System (CyCS) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC05 **Unit and location based data security**	• Cyber Command System (CyCS)
UC06 **View asset dependencies**	• Crown Jewels Analysis (CJA) • Cyber Command System (CyCS)
UC07 **View incidents aggregated by geographic region, with linked views**	• Cyber Command System (CyCS)
UC08 **Generate and select from Course of Action options**	• Threat Assessment and Remediation Analysis (TARA) • Federated Analysis of Cyber Threats (FACT)
UC09 **Use complementary tool**	• Structured Threat Information eXpression(STIX™) & Trusted Automated eXchange of Indicator Information (TAXII™) • Cyber Command System (CyCS)
UC10 **Single authoritative data source**	• Cyber Command System (CyCS)
UC11 **View interconnectivity**	• Cyber Command System (CyCS) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC12 **View connections of asset**	• Cyber Command System (CyCS) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC13 **Monitor network (network oversight)**	• CyGraph: Big-Data Analytics for Network Attack Mapping
UC15 **Fuse data**	• Federated Analysis of Cyber Threats (FACT) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC19 **Collect asset dependencies [*manual*]**	• Crown Jewels Analysis (CJA) • Cyber Command System (CyCS)
UC21 **Training and simulation**	• Analyzing Mission Impacts of Cyber Actions (AMICA)
UC23 **View asset information**	• Cyber Command System (CyCS)
UC24 **Filter views (linked views)**	• Cyber Command System (CyCS)
UC25 **Monitor Specific Threat**	• Collaborative Research Into Threats (CRITs) • Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

RFI Use Case	MITRE Solution
UC26 **Visualizations**	• Cyber Command System (CyCS) • CyGraph: Big-Data Analytics for Network Attack Mapping
UC27 **Prioritize Incident**	• Threat Assessment and Remediation Analysis (TARA) • Cyber Command System (CyCS) • Federated Analysis of Cyber Threats (FACT)
UC29 **View historical incidents by asset**	• Collaborative Research Into Threats (CRITs)
UC34 **Capture options and decisions**	• Threat Assessment and Remediation Analysis (TARA) • Cyber Command System (CyCS) • Federated Analysis of Cyber Threats (FACT)
UC35 **View public data sources**	• Structured Threat Information eXpression(STIX™) & Trusted Automated eXchange of Indicator Information (TAXII™) • Cyber Command System (CyCS) • Federated Analysis of Cyber Threats (FACT)