2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)
2013 © NATO CCD COE Publications, Tallinn

Mission-Centricity in Cyber Security: Architecting Cyber Attack Resilient Missions

Gabriel Jakobson
Altusys Corporation
Princeton, NJ, U.S.A.
jakobson@altusystems.com

Abstract: Until recently the information technology (IT)-centricity was the prevailing paradigm in cyber security that was organized around confidentiality, integrity and availability of IT assets. Despite of its widespread usage, the weakness of IT-centric cyber security became increasingly obvious with the deployment of very large IT infrastructures and introduction of highly mobile tactical missions where the IT-centric cyber security was not able to take into account the dynamics of time and space bound behavior of missions and changes in their operational context. In this paper we will show that the move from IT-centricity towards to the notion of cyber attack resilient missions opens new opportunities in achieving the completion of mission goals even if the IT assets and services that are supporting the missions are under cyber attacks. The paper discusses several fundamental architectural principles of achieving cyber attack resilience of missions, including mission-centricity, survivability through adaptation, synergistic mission C2 and mission cyber security management, and the real-time temporal execution of the mission tasks. In order to achieve the overall system resilience and survivability under a cyber attack, both, the missions and the IT infrastructure are considered as two interacting adaptable multi-agent systems. While the paper is mostly concerned with the architectural principles of achieving cyber attack resilient missions, several models and algorithms that support resilience of missions are discussed in fairly detailed manner.

Keywords: *mission-centric cyber security, cyber attacks resilient missions, cyber terrain, impact dependency graphs, adaptable multi-agent systems*

1. INTRODUCTION

Traditionally, the success of cyber security has been measured by the level of cyber attack protection achieved for information technology (IT) infrastructure hardware and software components that are used as an operational resource by different time and space bound activities like military missions and enterprise business processes. Until recently the IT-centricity was the prevailing paradigm in cyber security. It was organized around achieving three main goals: confidentiality, integrity and availability of IT assets [1]. Despite of its widespread usage, the weakness of IT-centric cyber security became obvious with the deployment of large IT infrastructures, where it was economically unjustifiable to seek absolute protection for all IT components, and introduction of mobile tactical missions, where the IT-centric cyber security was not able to take into account dynamic behavior of the missions.

Initial changes in the cyber security paradigm were associated with the introduction of the notions of mission critical assets [2] and network-centricity [3, 4]. The essence of mission criticality in cyber security was in the idea of protection of some, not all assets, and protecting them not always, but within some time window. The network-centric cyber security paradigm promoted by US DoD was motivated by the acceleration of the speed and mobility of the modern battlespace, and aimed building a secure information space for connecting people and systems independent of time and location.

The concepts of mission critical assets and net-centricity were important steps in orienting IT security measures towards the real needs of mission security, however in both cases the missions were considered as static entities that at best were used for parameterization of the IT-centric security models. At the same time, protecting missions, not IT infrastructure components is the ultimate goal of cyber security. Of course, the protection of IT infrastructure components continues to play important, but still, the subordinate role in mission cyber security. In other words, the success of protecting IT infrastructure components should be measured by the success of missions that this IT infrastructure is supporting. We will call this mission-centric cyber security

In this paper we are introducing the notion of cyber attack resilient missions as an example of mission-centric cyber security systems. We will show that mission cyber attack resilience is achieved through emergent (collective and adaptive) behavior of IT infrastructure components and missions. The paper discusses several critical architectural principles of achieving cyber attack resilience of missions, including mission-centricity, resilience through adaptation, and synergistic mission C2 and mission cyber security management. In order to achieve the overall system resilience under a cyber attack, both, the command an control of missions in the phusical space, and management of IT infrastructure components in s cyber cpace are considered as two interacting adaptable multi-agent systems. As such, the quality of those physical and cyber operations cannot be any more assessed as silos of two independent processes.

The rest of the paper is organized as follows. Section 2 discusses how the notion of resiliency is understood in different disciplines, provides a definition of resilient missions, and reviews relevant work. Section 3 describes the basic conceptual elements and architecture of a mission-centric cyber security. Section 4 describes the models of cyber terrain, impact dependency graph, and the tactical space and time bound missions that are used in the proposed approach. Section 5 provides a model of mission resilience that is reached via interactive adaptation of cyber terrain and missions, it describes how the process of mission adaptations can be implemented using an adaptable multi-agent system, and presents a sample set of mission adaptation policies. Section 6 draws some conclusions and refers to the future research directions.

2. CYBER ATTACK RESILIENT MISSIONS

In this section we'll review some origins of the notion of resiliency in complex systems and define the notion of a cyber attack resilient mission.

A. UNDERSTANDING RESILIENCY

Resilience as a fundamental feature of all complex systems, being them natural or artificial systems, has been an interest or study of many scientific disciplines. Dictionary.com defines resilience as the power or ability to return to the original form, position, etc., after being bent, compressed, or stretched; or as ability to recover readily from illness, depression, adversity, or the like. In social science resiliency is the ability of individuals, but also groups, to overcome challenges, like trauma, tragedy, crises, isolation, and bounce back stronger, wiser, and more socially powerful [5]. Psychological resilience is an individual's tendency to cope with stress and adversity. This coping may result in the individual "bouncing back" to a previous state of normal functioning, or simply not showing negative effects [6]. In engineering disciplines resilient systems are designed to anticipate and avoid catastrophic accidents, and survive and recover from natural disruptions and terrorist attacks [7]. A general framework for classifying system resilience is given in [8]. In [9] the resilience of a system or organization is understood as including at least two of the following capabilities: (a) anticipation and preparation before an adverse event; (b) survival during the event; and (c) recovery after the event.

Summarizing the different understandings of system resiliency, one can define the principal goal of resilient systems is the system's desire to survive, even if not any individual component of the system is surviving. In other words, the system resiliency is achieved through emergent (collective and adaptive) behavior of all components of the system. The emergent systems [10, 11] expose new global properties not as a mechanical sum of local properties of its components but as a qualitatively new feature that emerges from the inter-component interactions and adaptations.

B. DEFINING A CYBER ATTACK RESILIENT MISSION

Inspired by the definition of resilient computer networks given in [9] we define resilient missions as missions that in a given time window are able to reach their operational goals situation under the impact adverse events, like adversary attacks, human errors, disruptions in support services, and natural disasters. The concept of mission resilience assumes structural changes in mission task flows, adaptability of mission execution processes, and a graceful degradation of mission goals.

As applied to the domain of mission cyber security we define cyber attack resilient mission as resilient missions that are capable to:

a) Predict plausible impact of cyber attack situations **before** they occur;

b) Survive through adaptation and graceful degradation **during** the attacks;

c) Recover its operational capacities **after** the attacks;

As we already mentioned in the Introduction, we will consider a mission and its supporting IT infrastructure together as one synergistic interacting system. This is an important conceptual viewpoint – by adopting it we will show that cyber attack mission resiliency can be achieved by cross-mission and IT infrastructure interactions and adaptive behavior of all components of this synergistic system containing both the IT infrastructure components and mission components.

C. RELATED WORK

Over the last three decades significant research and development results have been reached in the area of cyber attack tolerant, survivable, and resilient IT systems [12-15]. A broad overview of resilient computer networking and related fields is given in [16], where the resilience is defined as the ability of the network to provide and maintain an acceptable level of service in the face of attacks, faults, natural disasters and other challenges to normal operation. Probably, Fraga and Powell were the first who used the terms of "fault tolerance" and "intrusion tolerance" in 1985, when they described the capabilities of a fault and intrusion tolerant file system [17]. Since then the term fault tolerance is understood as a capability of the system to continue satisfactory operations in the presence of faults. Fault tolerance capabilities are built in almost every modern technological and infrastructure system, including communication networks, power grids, space systems and others. During the last three decades significant results in fault tolerance research were achieved by fault tolerant computing [18], including distributed fault-tolerant architectures, masking (hardware redundancies), models of graceful degradation, dynamic reconfiguration, fault detection by spatial and temporal event correlations, automatic recovery and response techniques, system vulnerability analysis, damage assessment and evaluation, and other methods. Since the start of research on intrusion tolerant systems almost two decades ago significant body of research and system development has been produced. A good overview of those results has been presented in [19].

A model of increasing mission survivability based on reinforcement learning was proposed in [20]. The paper defines the measure of mission survivability as a ratio between the successfully completed workflows of the mission to the total number of the workflows. The paper examines two core capabilities to increase mission survivability: redistribution of the network resources to ensure mission continuity, and learning of the attack patterns to estimate the level of vulnerability of other nodes. Both of these capabilities are concerning the resource network, while adaptation of the mission was not addressed.

In June 2011 The Defense Advanced Research Projects Agency (DARPA), the US Department of Defense's advanced research department, announced that it is working on a project called Mission oriented Resilient Clouds (MRC), which aims to build resiliency into existing cloud networks to preserve mission effectiveness during a cyber attack [21]. The MRC program will run an ensemble of interconnected hosts acting in concert. Loss of individual hosts and tasks within the ensemble is allowable as long as mission effectiveness is preserved. The MRC project will include redundant hosts and will be able to correlate attack information while switching around resources. The goal is to provide resilient support to the mission through adaptation. The MRC program looks on cyber attack resilient clouds that are adaptable towards mission needs, still adaptation of the missions themselves as in [21] is not defined in the program research topics.

3. ARCHITECTURE OF A CYBER ATTACK RESILIENT MISSION

Reference architecture of a cyber attack resilient mission is given on Figure 1. It contains two main interacting closed-loop processes: Cyber Security Situation Management (CSSM) process and the Mission Operations Situation Management (MOSM) process. The CSSM and MOSM processes interact through a common object of interest – the mission. As mission progresses in time CSSM receives IT service requests from the mission and provides the requested services back to the mission. Concurrently to this process, MOSM proceeds with the tasks of mission situation awareness, undertakes mission decision support functions, and transitions the mission into a new state. The new mission state might require renewed IT support services from CSSM. In order to achieve resiliency to withstand the impact of cyber attacks the above-described interaction between CSSM and MOSM requires of mutual adaptation of the cyber terrain and the mission, e.g. reconfiguration of dependencies among the cyber assets and services, replacing or upgrading certain assets, changing the logical or temporal order of mission tasks, or proceeding with a graceful degradation of the mission goals.

Figure 1 illustrates a tactical military mission conducted in an urban mission operational theater. The mission is conducted by two small military units against hostile agents. In addition to the cyber attacks, the mission must withstand physical impacts caused by natural forces and external mission disruptions. MOSM acts according to the mission model, and military tactical policies and rules. The MOSM includes two sub-processes, the Mission Situation Awareness (MSA) and the Mission Decision Support (MDS) processes. MSA and MDS themselves are fairly complex operations: MSA performs the tasks of (a) sensing and pre-processing of real-time data coming from sensors and human reports; (b) perception of the collected data and construction of the tactical situation model of the operational; (c) mission impact assessment caused by the actions and forces in the Physical Space; and (d) prediction of future plausible impacts on the mission caused by adverse events in the physical space. MDS performs the tasks of mission operations planning, mission adaptation and mission execution.

Like the MOSM process, the closed-loop CSSM process contains two major sub-processes, Cyber Security Situation Awareness (CSSA) and Cyber Security Decision Support (CSDS) processes. The CSSA process includes the following tasks: (a) real-time correlation of cyber attack alerts, and recognition of complex multi-stage cyber attacks; (b) cyber attack impact assessment on cyber assets that were directly hit by the attack, (c) propagation of the impact of the cyber attack through the inter-component dependencies in the Cyber Terrain, and

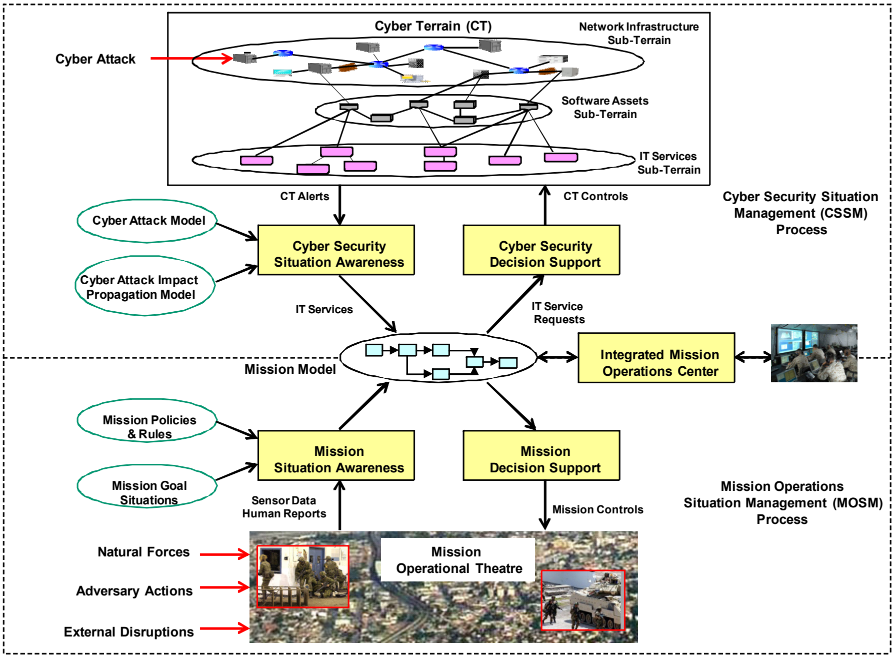
Cyber Terrain (CT)
Network Infrastructure Sub-Terrain
Cyber Attack
Software Assets Sub-Terrain
IT Services Sub-Terrain
CT Alerts
CT Controls
Cyber Security Situation Management (CSSM) Process
Cyber Attack Model
Cyber Attack Impact Propagation Model
Cyber Security Situation Awareness
Cyber Security Decision Support
IT Services
IT Service Requests
Mission Model
Integrated Mission Operations Center
Mission Policies & Rules
Mission Goal Situations
Mission Situation Awareness
Mission Decision Support
Sensor Data Human Reports
Mission Controls
Mission Operations Situation Management (MOSM) Process
Natural Forces
Adversary Actions
External Disruptions
Mission Operational Theatre

Figure 1. Synergistic mission cyber security and command & control management

(d) assessment of plausible future cyber attack impacts. The cyber attack impact propagates through the CT and reaches mission tasks that consume the cyber services provided by the CT. Through the fabric of mission task, sub-mission and mission dependencies this impact reaches the top level of a mission and might affect the success of the mission completion. The CSDS process contains the following tasks: (a) CT vulnerability scanning and preventive maintenance, (b) CT adaptation as response to the cyber attacks and as reaction to IT service requests from the missions, and (c) CT recovery actions.

For performing of the above-mentioned tasks the CSSA and CSDS processes need variety of data and knowledge sources. In this paper we will mention two of them, the Cyber Attack Model and the Cyber Attack Impact Propagation Model. The Cyber Attack Model is used for calculating the effect of the cyber attack on the operational capacity of the directly hit cyber assets, while the Cyber Attack Impact Propagation Model is used for calculating the indirect impact of the cyber attack on those assets that are tied by dependencies according to the structure of the CT.

The closed-loop CSSM and MOSM processes are conceptually built following the principles of Situation Management (SM), which is more in detail discussed in our earlier work [23].

4. MAIN CONCEPTUAL COMPONENTS OF THE APPROACH

In this section we will discuss several key elements of the proposed approach of building cyber attack resilient missions, including cyber terrain, tactical mission and impact dependency graph.

A. CYBER TERRAIN - MODELING IT INFRASTRUCTURE

Cyber terrain (CT) is a multi-level information structure that describes cyber assets and services, and their intra- and inter-dependencies [22]. As was already shown on Figure 1 it contains three sub-terrains: hardware, software, and service sub-terrains. The hardware (HW) sub-terrain is a collection of connected network infrastructure components like routers, servers, switches, firewalls, communication lines, terminal devices, sensors, cameras, printers, etc. All the dependencies between the components, like connectivity, containment, location, and other relations, represent the physical/logical topology of the HW sub-terrain. The software (SW) sub-terrain describes different software components, such as operating systems, middleware, applications, etc., and defines its own dependencies between the components. A software component in the SW sub-terrain might be characterized by different attributes like functional class of the component, vendor specification, release number, references to known vulnerabilities, etc. The service sub-terrain presents all the services and their intra-dependencies. Examples of typical services include database, file transfer, e-mail, GIS, universal time, and security services. The most common dependencies between two services include: enabling of one service by other and containment of one service within a package of multiple services.

As among the components of a sub-terrain, dependencies exist between the sub-terrains: a HW sub-terrain component may “house” SW sub-terrain components and a SW sub-terrain component may enable some services. CT is a dynamic information structure: its components and their inter-dependencies are a function of time.

While supporting the missions, the CT possesses certain “operational capacity”, i.e. the ability to provide resources and services to the missions with a certain level of quantity, quality, effectiveness, and cost to the missions. In this work we will introduce the operational capacity (OC) as a universal measure characterizing the operational quality of each of the component in the CT, being it a cyber asset or service. The operational capacity is measured in an interval [0, 1], which indicates to what level the asset or service was compromised under a cyber attack. Value 0 means that an component is totally compromised (not trustworthy, not operational) and value 1 means that the component is fully operational.

In a general attack situation, a software asset can be either directly hit by a cyber attack causing permanent damage to its operational capacity, or the operational capacity of an asset may be indirectly impacted by a remote attack via inter-asset dependencies. The operational capacity level of the directly hit asset stays unchanged as long as corrective actions are made to the asset. A sequence of direct attacks might reduce the operational capacity of an asset, or totally destroy the asset bringing its operational capacity to 0. Contrary to the effect of the direct attack, an indirect cyber attack does not cause permanent damage to the cyber asset. However, its operational capacity might be reduced because of its dependency on other assets that either suffer from direct attacks or are also indirectly impacted. To measure the impact of a permanent damage to the software assets, we will introduce the notion of permanent operational capacity (POC) that is applicable only to software assets.

B. MISSIONS

Military mission (aka military operation) is 0 coordinated order of space and time bound military actions to resolve political or military situations in the favor of the agent conducting the mission. Depending on the scope of developing situations, the size of the engaged military units, and the defined goal situations the military missions are considered at three main levels: strategic, operational and tactical levels. The strategic mission describes actions over large, often continental area of operations with national commitment to the mission. The operational level mission describes a subset of a strategic operation with specific military goals, while the tactical mission being part of an operational level mission is limited in time, space, the scope of objectives, and engaged military resources. In this paper we are focusing mostly on tactical missions.

Missions are modeled sequential or parallel flows of mission steps that in addition to the AND/OR logic, are controlled by temporal interval logic [25]. The content of the actions executed at a mission step is defined by a mission task. It is not excluded that the same tasks can be executed at several different mission steps, and a single task can be decomposed into a sequence of multiple steps, if of course, from the mission command control perspective such need arises. A mission step can be another flow, another mission, or mission task. Figure 3 illustrates a Mission X that has two parallel flows that are forked by an AND-node. The first branch contains another flow of three sequential steps (d1, d2, d3), while the second flow contains two sub-missions A and B. The Mission A represents itself two flows that are forked by an OR-node, while the second mission B represents a special case of an AND-node called “Cloud”. The AND-node requires that both branches of the flow should be executed, while the OR-node prescribes that at least one branch should be taken.

All missions and mission steps are formally described as interval events that have their start time, duration and end time. While the AND-nodes and OR-nodes specify only the logical conditions of executions of the mission flow branches, they do not identify the exact temporal order of missions/mission steps as events. For example, on Figure 2 the AND-node in Mission X specifies that both branches,

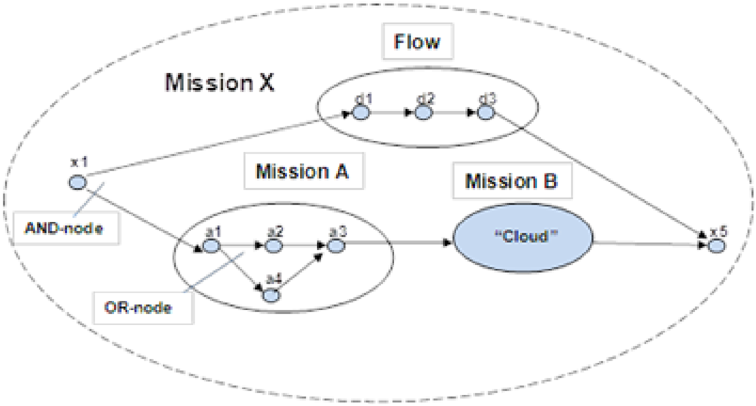

Figure 2. Mission Task Flows

Flow(d1, d2, d3) and Flow(Mission A, Mission B) should be taken, but the question in what temporal order remains open. In order to determine the order of execution of mission flows we will use temporal logical relations such as BEFORE, AFTER, STRICTLY-AFTER, etc. between the mission steps. In our earlier paper on temporal relations in event correlation [24] we used temporal interval logic proposed by John Allen [25]. In addition to those temporal relations we will introduce in this paper a temporal relation UNDEFINED that do not require any specific temporal relation to be identified between the events. The above-mentioned sub-mission B called "Cloud" is exactly described by the temporal relation UNDEFINED, namely we require that all steps from the "Cloud" should be taken, but in any arbitrary order.

The existence of temporal order between missions and mission steps, and the options to change the order, e.g. advance or delay the order of execution of mission flows, opens an opportunity to adapt mission so that to minimize the cyber attack impact on missions. Such method of mission adaptation will be discussed in the Section IV. As the embedded structure of missions unfolds during the mission execution process all mission steps will be ultimately turned into executable mission tasks.

C. IMPACT DEPENDENCY GRAPH

Formally, the cyber terrain and the missions and propagation of the impact through cyber terrain and the mission-submission structure is described by the impact dependency graph. Impact dependency graph (IDG) [22] is a mathematical abstraction of the domain semantics of assets, services, mission steps and missions and all of their dependencies. We consider assets, services, mission steps and missions as nodes of an IDG and their inter-dependencies as dependencies among the nodes of the IDG. In addition to the nodes of assets, services, mission steps and missions, IDG has two special nodes: AND-nodes and OR-nodes that represent logical dependencies among nodes in IDG. The AND-node defines that the parent node depends on all of its children nodes, while the OR dependency defines the required presence of at least one child node. The OR dependency is introduced to capture system redundancy or for alternative functionality, performance, cost, reliability or for some other reason. Figure 3 shows a sample impact dependency graph, which comparing with an IDG introduced in [22] has been extended with an Agent Pool.

As a result of a cyber attack against the cyber terrain, the cyber attack impact propagates through the IDG, and when the impact reaches an agent pool, the operational capacities (OC) will be calculated for all agents in the pool. The agent with the highest OC in the agent pool will be assigned to the corresponding mission task, and then the impact propagation process continues up to the top level mission node in the IDG.

During real-time mission monitoring, the impact of a cyber attack on a mission depends on two major factors: (1) what impact the attack has on steps of the mission, and (2) in what state - planned, ongoing, or completed state the mission steps are. For example, if the cyber attack can impact assets and services that support steps a, …, m, but those steps have been already completed (see Figure 4), then the impact of the attack should be irrelevant as far as these steps are concerned. Contrary, the ongoing steps during the cyber attack, like step x will be directly affected by the attack. The case for the steps that are planned for execution (steps p to s) at the moment when a cyber attack happens needs a special analysis.

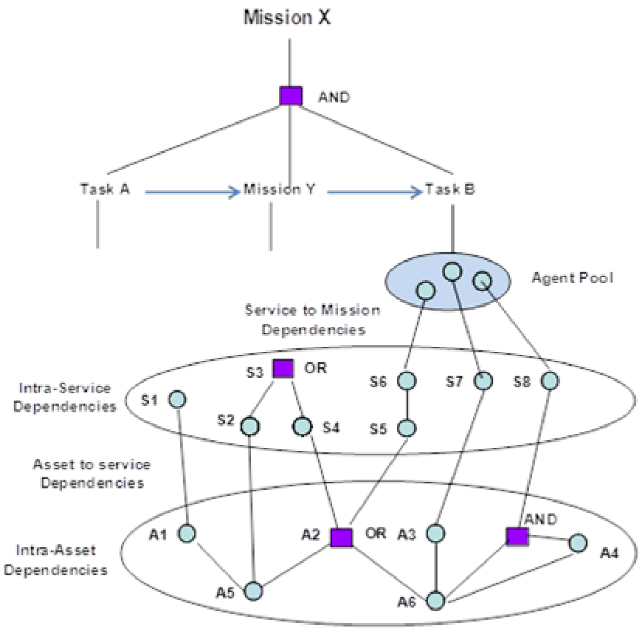

Figure 3. Impact Propagation Graph

First, since those steps have not yet been undertaken, their operational situation will not be accounted in the calculation of the operational situation of the overall mission. However, we are able to calculate a potential impact on those steps, which could happen. One practical action could be to reconfigure the cyber terrain or give a warning to the mission C2 commander.

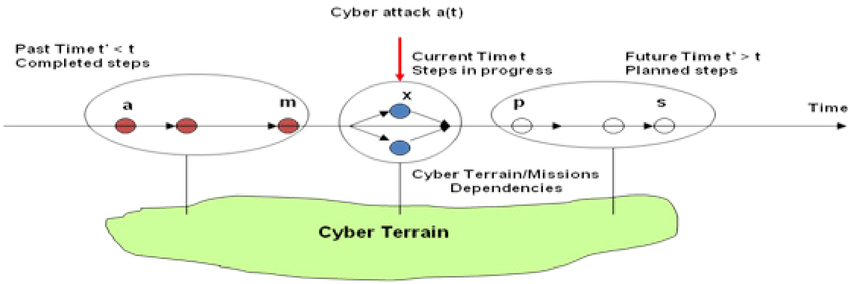

Figure 4. Time-dependent impact of cyber attacks on missions

5. MISSION RESILIENCE THROUGH ADAPTATION

A. ADAPTATION IN MULTI-AGENT SYSTEMS

In order to achieve mission resilience under a cyber attack, both, the missions and the CT are considered as two interacting adaptable multi-agent systems (MAS). In this section we outline some principles of CT and mission adaptation.

In many applications, including mission command and control, and mission cyber security management, operational components of the systems need to be flexible and adaptable to deal with dynamic environments. To address this need, there are several general requirements of the system architecture, including openness, self-awareness and the use of meta-knowledge to adjust the structural organization and behavior of the system according to the adopted policies. It is assumed that an adaptable system is capable of exhibiting autonomous run-time behavior without outside intervention. Often the following types of adaptation are considered:

- Structural adaptation – adaptation to internal structural changes, e.g. loss of inter-node connectivity, or loss of nodes
- Functional adaptation - detection of changes in the functions of nodes of the system,
- Resource adaptation - adaptation in the system internal resources, i.e. loss or corruption of physical memory, or loss of battery power

All these three types of adaptations are useful in adaptation of CT and missions to achieve mission survivability and they will be used through the framework of adaptable multi-agent systems. The paradigm of multi-agent systems has its roots in distributed artificial intelligence, object oriented systems and human team cognition. MAS is currently one of the most powerful approaches used in building distributed computing systems [26]. MAS have several important features which correspond to our specific interests, particularly:

- Adaptation: the ability to reorganize and improve behavior with experience
- Autonomy: goal-directedness, proactive and self-starting behavior
- Collaboration: the ability to work with other agents to achieve a common goal
- Inference: the ability to act on abstract task specifications
- Mobility: migration in physical or cyber space

A typical MAS solution to situation awareness, and consequently to the whole process of command and control, is based on dividing situation awareness, command and control into several dedicated agents either across functional tasks, e.g. data detection, classification, visualization, etc., or across levels of abstraction of information, e.g. signal, data and semantic information levels. In this paper we will use BDI (Belief, Desire and Intension) agent model that was originally proposed in [27-29] and later advanced with adaptation capabilities [30, 31] as a main building block for MAS.

B. MISSION ADAPTATION POLICIES

Mission adaptation policies are rules that are used by an agent to modify the missions, its components and inter-dependencies between the mission components. From a mission execution viewpoint each task is implemented by an agent that is assigned to the task. As we talk about missions as objects of adaptations, two types of mission adaptation methods are considered, entity-level adaptation, relation-level adaptation. On entity-level adaptation each entity, a mission, task or an agent can be a subject for modification. For example, one can change the criticality index of a mission or a task, or operational capacity of a task or an agent. An important adaptation function is the election of an agent from a pool of pre-defined agents to implement a particular mission task. All these individual adaptation functions are undertaken within the constraints identified for each entity. The relation-level adaptation covers the functions of changing or modifying the structural, temporal, logical, or domain-specific relations between the entities. For example, adding or deleting a task, changing the AND-nodes and OR-nodes in a mission flow, changing the temporal order of tasks in a mission flow, delaying or moving up the start or the end time of a mission or its components. Below we will present a sample list of mission adaptation policies for ongoing mission tasks that are under execution at the time of the cyber attack:

1. For every currently active mission task select an agent from a corresponding agent pool that has the highest operational capacity that is equal or greater than the required operational capacity specified in the mission task. If no agent is found, use Policy #2.
2. Reduce incrementally the value of the task's required operational capacity from the current value to the lowest permitted level. For each incremental required operational capacity value perform the Policy #1. If no agent is found that matches the Policy #1, use Policy # 3.
3. Modify the mission task flow so that the tasks with no matching agents are moved for a later time of execution. Issue a CT reconfiguration order to replace/or repair the CT node with a low operational capacity.

4. Stop execution of those mission tasks, where (a) the stop execution permission is granted, and (b) no agent could be found with operational capacity that is at least equal to the required operational capacity of the task.
5. Select from the alternative mission flows (mission flows that are in OR condition among themselves) a flow where all tasks have the matching agents, whose operational capacities are greater than the required operational capacities in the corresponding tasks.
6. Select first those tasks from the "Cloud" in the mission flow that satisfy the required operational capacity condition. For the rest of the tasks issue CT reconfiguration order.

Our approach to mission cyber attack impact assessment, both to the current real-time impact when the cyber attack occurred during the execution of the mission, and assessment of the impact of plausible future cyber attacks is discussed elsewhere [22, 32].

6. CONCLUSIONS

In this paper we stressed the importance of a cyber security paradigm shift by moving towards mission-centricity in cyber security. We motivated this paradigm shift with several arguments, namely the fast increase in the scale of IT infrastructures and the practical inability to protect every component of the IT infrastructure, as well the high mobility and dynamics of modern battlefield and business processes. In this paper we proposed the notion of cyber attack resilient missions and how they should act before, during and after the cyber attacks. As proposing the architecture for building those missions, we presented several innovative solutions, including (a) synergistic adaptation of the cyber terrain and tactical missions implemented as two situation-aware adaptable BDI multi-agent systems, (b) the overall model of a cyber situation management system, (c) the model of cyber attack impact propagation through the impact dependency graph (IDG), and (d) modeling the dynamic behavior of missions by graphical flowcharts augmented with logical and temporal constraints.

We argued that only integrated approach that combines synergistic management of mission command and control, and mission cyber security can lead to resilient and survivable missions. Future work will include extending of the proposed principles to resilient and survivable missions that are oriented towards faults, human errors, and natural and technological disasters.

REFERENCES

[1] Aceituno, V., 2005, On Information Security Paradigms, *ISSA Journal,* September, 2005.

[2] US GAO, 2011, Critical Infrastructure Protection. Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use", *USA GAO Report to Conressional Requesters GAO-12-92*.

[3] US DoD, 2012, "Department of Defense Net-Centric Data Strategy", http://dodcio.defense.gov/docs/net-centric-data-strategy-2003-05-092.pdf.

[4] Kerner, J., Shokri, E., 2012, Cybersecurity Challenges in a Net-Centric *World, Aerospace Crosslink Magazine*, Spring 2012.

[5] Cacioppo, J. T., Reis, H. T., Zautra, A. J., 2011, Social Resilience: The Value of Social Fitness with an Application to Military, *American Psychologist*, Vol. 66, No. 1, pp. 43-51.

[6] Reivich, K., Shatte, A., 2003, The Resilience Factor: 7 Keys to Discovering Your Inner Strength and Overcoming Life's Hurdles, *Random House*,.

[7] Jackson, S., 2007, A Multidisciplinary Framework for Resilience to Disasters and Disruptions, *Journal of Design and Process Science*, June 2007.

[8] Mostashari, A., 2010, Resilient Critical Infrastructure Systems and Enterprises, *Imperial College Press.*

[9] Westrum, R., 2006, A Typology of Resilience Situations, in (Eds. E. Hollnagel, D. Woods, D. Lelvenson) *Resilience Engineering Concepts and Precepts. Aldershot, UK: Ashgate*.

[10] De Wolf, T., Holvoet, T, 2004, Emergence and Self-Organization: a statement of similarities and differences, In: *Proceedings of the Second International Workshop on Engineering Self-Organizing Applications,* New York, USA , pp.96–110.

[11] Edmonds, B, 2004, Using the Experimental Method to Produce Reliable Self-Organized Systems, In Brueckner, S., Serugendo, G.D.M., Karageorgos, A., Nagpal, R., eds. *Engineering Self Organizing Systems: Methodologies and Application*s. Volume 3464 of Lecture Notes in Artificial Intelligence. Springer, 2004.

[12] Siewiorek, D., ed., 1995, *Fault-Tolerant Computing Highlights from 25 Years*, Special Volume of the 25th International Symposium on Fault-Tolerant Computing FTCS-25, Pasadena ,CA.

[13] Ellison, R. J., Fisher, D. A., Linger,R. C., Lipson, H. F., Longstaff, T. A., and Mead, N. R. 1999, An Approach to Survivable Systems, *Technical Report, CERT Coordination Center, Software Engineering Institute*, Carnegie Mellon Institute.

[14] Lipson, H.F., Fisher, D.A, 2000, Survivability—a New Technical and Business Perspective on Security, In: NSPW 1999: *Proceedings of the 1999 Workshop on New Security Paradigms*, pp. 33–39. ACM, New York.

[15] P. Smith, P., Hutchinson, D., Sterbenz, J. P. G, Scholler, M., Fessi, A., Karaliopoulos, M., Lac, C., Plattner, B., 2011, Network Resilience: A Systematic Approach, *IEEE Communications Magazine,* July, 2011, pp. 88-97.

[16] Sterbenz J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer J. P., Schöller, M., Smith, P., 2010, Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Elsevier Computer Networks 54, pp. 1245-1265.

[17] .Fraga, J.S., Powell, D., 1985, A fault- and intrusion-tolerant file system, In *Proceedings of the 3rd International Conference on Computer Security*. 203–218.

[18] Rennels, D. A., 1999, Fault-Tolerant Computing, *Encyclopedia of Computer Science*, ed., Anthony Ralston, Edwin Reilly, and David Hemmendinger.

[19] Verıssimo, P., Neves, N., Correia, M., 2003, Intrusion-Tolerant Architectures: Concepts and Design. In Architecting Dependable Systems, R. Lemos, C. Gacek, A. Romanovsky (eds.), *LNCS 2677, Springer Verlag*.

[20] Carvalho, M. 2009, A Distributed Reinforcement Learning Approach to Mission Survivability in Tactical MANETs, *ACM Conference CSIIRW 2009*, Oak Ridge TN.

[21] Mission-Oriented Resilient Clouds, 2011, DARPA, Information Innovation Office, http://www.darpa.mil/Our_Work/I2O/Programs/Mission-oriented_Resilient_Clouds_(MRC).aspx.

[22] Jakobson, G., 2011, Mission Cyber Security Situation Assessment Using Impact Dependency Graphs, *Proceedings of the 14th International Conference on Information Fusion*, Chicago, IL.

[23] Jakobson, G., Buford, J., Lewis. L. 2007, Situation Management: Basic Concepts and Approaches, *Proceedings of the 3rd International Workshop on Information Fusion and Geographic Information Systems*, St. Petersburg, *Lecture Notes in Geoinformation and Cartography, Springer-Verlag Berlin Heidelberg*.

[24] Jakobson G., and Weissman, M., 1995, Real-Time Telecommunication Network Management: Extending Event Correlation with Temporal Constraints, the *4th IFIP/IEEE International Symposium on Integrated Network Management*, Santa Barbara, CA, pp. 290-301.

[25] Allen, J. F, 1983, Maintaining Knowledge About Temporal Intervals, *Communications of the ACM* 26 (11), pp. 832-843.

[26] Wooldridge, M., 2002, An Introduction to Multi-Agent Systems, John Wiley and Sons.

[27] Bradshaw. J. M. 1997, An Introduction to Software Agent, In: *Software Agents*, Menlo Park, Calif., AAAI Press.

[28] Norling, E., 2004. “Folk Psychology for Human Modeling: Extending the BDI Paradigm,” *In International Conference on Autonomous Agents and Multi-Agent Systems*.

[29] Rao, A., and Georgeff, M., 1995, BDI Agents: From Theory to Practice, In *Proceedings of the First International Conference on Multi-Agent Systems*.

[30] Jakobson, G., Buford, J., and Lewis, L., 2008, Models of feedback and adaptation in multi-agent systems for disaster situation management, *SPIE 2008 Defense and Security Conference, Orlando, FL*.

[31] Maes, P., 1993, Modeling Adaptive Autonomous Agents, *Artificial Life*, vol.1, No 1-2, pp. 119-128.

[32] G. Jakobson. G., 2011, Extending Situation Modeling with Inference of Plausible Future Cyber Situations, *CogSIMA 2011*, Miami, FL.