20th ICCRTS

"C2, CYBER, AND TRUST"

Theoretical Model for Cybersecurity: Using Socially-Aware Purposeful Agent and Reflexive Game Theory

Suggested Topics: Agile C2 Security; Modeling and Simulation; Concepts, Theory, and Policy

Name of Author: Kofi Nyamekye, Ph.D.

Point of Contact: Kofi Nyamekye, Ph.D.

Name of Organization: Integrated Activity-Based Simulation Research, Inc.

Complete Address: 1919 South Grand Boulevard, Suite 412, Saint Louis, MO 63104-1573

Telephone: 314-704-7964

E-mail Address: kofinsoyameye@iabsri.net

ABSTRACT

Using the socially-aware purposeful agent, the new term coined by the author to replace the previous term purposeful agent, and the Reflexive Game Theory (RGT), this paper discusses the framework for constructing a theoretical model for cybersecurity. The paper uses the RGT to initially model the socially-aware purposeful agent, as a group of one socially-aware purposeful agent or elementary socially-aware purposeful agent that resides within the endpoint's internal operating environment. Unlike the traditional agent, the socially-aware purposeful agent has cognitive capabilities which permit the socially-aware purposeful agent to create a mental image or situational awareness of a threat object in the endpoint device's internal operating environment. Within the context of the RGT, the behavior of an elementary socially-aware purposeful agent is in the state of free choice. Upon realizing the threat object to be a malware, the socially-aware purposeful agent dynamically changes its behavior to be in conflict with the cyber hacker that launched the code. In terms of the RGT, we now have an interaction between two socially-aware purposeful agents, in conflict. A graph is then constructed for the two interacting socially-aware purposeful agents, in conflict. The graph is then decomposed to create the polynomial, depicting the analytical notation of the graph. A diagonal form is then established for the polynomial. Using the influences of the cyber hacker on the subconscious and conscious domains of the socially-aware purposeful agent, the subsets of actions to deal with the malware can now be predicted. The socially-aware purposeful agent can choose any of the predicted actions and realize any non-empty realizable subsets of the chosen set of actions. Four examples are given to demonstrate the theoretical model for cybersecurity. Furthermore, the framework borrows from pi-calculus to model interaction as the basis for information sharing among DoD System-of-Systems to mitigate cybersecurity risks.

INTRODUCTION

As cyber security has become serious threats to physical security system components or endpoint devices and current cyber security measures are inadequate to mitigate such threats, a critical need exists for a formal development of modeling the behavior of new agents with cognitive capabilities, for addressing the cyber security threats. An example of such new agents is the emerging socially-aware purposeful agent that not only can make a decision to perform some cybersecurity actions, but also can interact with a cyber hacker and an instrument, e.g., a malware, which a cyber hacker uses to attack the physical security system components or endpoint devices. Because of its cognitive capabilities, the socially-aware purposeful agent can reason like a human to decide which set of the chosen cyber security actions to use for defeating a cyber threat. We define an instrument as an object which an individual or system uses to co-produce the outcome of an individual's or system's action [Ackoff 2006]. Thus, a malware is an object which a cyber hacker, who is also a socially-aware purposeful agent, uses to co-produce the outcome, e.g., malware infection of a physical security system component or an endpoint device, of a cyber

hacker's action. In this case, the cyber hacker's action is attacking a user's endpoint device. We should emphasize that the instrument does not have the reasoning capability or the cognitive capability as the socially-aware purposeful agent (cyber hacker). According to Lefebvre (through private communication with Lefebvre [Nyamekye and Lefebvre, October 17, 2013]), a socially-aware purposeful agent can be an inanimate or animate subject, with a cognitive capability. Lefebvre also emphasizes that a subject, e.g., a Warfighter, a country, can be anything to which our attention is directed [Lefebvre 2010]. In this paper, we will focus our attention on cybersecurity modeling in endpoint devices. Future publications will focus on cybersecurity modeling in network systems.

To understand what we mean by modeling the behavior of a socially-aware purposeful agent that can reason like a human to decide which set of the chosen cyber security actions to use to defeat a cyber-threat, let us use "a strategic corporal" as an example, in dealing with insurgents, in irregular warfare (IW). A direct excerpt from Wikipedia [Wikipedia] explains "strategic corporal" as follows: *the **Three Block War** is a concept described by U.S. Marine General Charles Krulak in the late 1990s to illustrate the complex spectrum of challenges likely to be faced by soldiers on the modern battlefield. In Krulak's example, soldiers may be required to conduct a full-scale military action, peacekeeping operations and humanitarian aid within the space of three contiguous city blocks. The thrust of the concept is that modern militaries must be trained to operate in all three conditions simultaneously, and that to do so, leadership training at the lowest levels needs to be high. The latter condition caused Krulak to invoke what he called "strategic corporals"; low-level unit leaders able to take independent action and make major decisions*. Here the strategic corporal is the socially-aware purposeful agent and the insurgent is the cyber hacker. We can make an analogy between the operating environment, which may include the local tribesmen, tribal leaders, the villagers, of the "strategic corporal" and the operating environment, which may include the operating system, processors, application programs, etc., within the endpoint device's security system components. The "strategic corporal" has the responsibility to make a tactical choice or decision as a commander in one instance of attacking an enemy (insurgent), which in our cyber analogy, the cyber hacker's instrument (malware), and in another instance the "strategic corporal" may play the role of a local tribal leader, e.g., resolving tribal disputes among the indigenous people. The behavior of a strategic corporal, in playing the role of a local tribal leader in resolving tribal disputes among the indigenous people, is similar in concept to the behavior of a socially-aware purposeful agent, for example, interacting with new updates of software applications on the endpoint devices, to ensure that such new updates come from trusted sources. Thus, the socially-aware purposeful agent must have the cognitive capability to distinguish between the enemy (malware) and the friendly systems (trusted software applications), just as the strategic corporal can distinguish between the enemy (insurgent) and the local friendly indigenous people in the villages. We will later discuss socially-aware purposeful agent in details, within the context of an elementary subject and non-elementary subject [Nyamekye June 8, 2015], respectively.

While much literature exists on the two most popular anti-virus technologies, namely; virus scanners and integrity checkers, for detecting and preventing damage from computer viruses, very few publications exist on the behavior blockers, for detecting and eliminating viruses in endpoint devices. A brief overview of each technology is essential before subsequent discussions.

A virus scanner examines the contents of each file that can carry executable instructions, e.g., ".exe", ".bat", ".com", ".vbs", ".scr", etc. The virus scanner searches each potential file for certain "search strings" which are present in known viruses [Auburn University]. Using a variety of search techniques, e.g., fuzzy search, a virus scanner compares the executable instructions with the known executable instructions and if a match is found, it will eliminate the virus [Auburn University]. Since scanners use a database of known viruses, unknown viruses can easily escape detection [Auburn University]. More importantly, minor variants of known viruses can be missed.

An integrity checker creates a checksum for each executable file in a directory, and stores the results in a file [Auburn University]. Each time the integrity checker is run, it recomputes the checksum for each executable file and compares this value to the previously stored checksum [Auburn University]. If the values match, then the file is assumed to be clean. If the values do not match, the executable has probably been infected by a virus [Auburn University]. Problems with integrity checking include the following [Auburn University]: a virus can modify checksum file, so when an integrity checker compares the computed checksum with checksum stored in the file, the integrity checker will ignore the file; a virus can delete the checksum file, thus with the checksum file deleted, there is no basis for determining previous checksums; a virus can encrypt checksum file, which has the same effect as deleting the checksum file; integrity checking only works for file infecting viruses, so, viruses that copy themselves to the hard disk (as many viruses do) will be ignored, since there is no checksum discrepancy.

A behavior blocker does not proactively search for known viruses [Auburn University]. Rather, it monitors the system for suspicious activity. For example, a program "virus.exe" suddenly attempts to delete "all.mp3" files stored on the hard disk [Auburn University]. If the behavior blocker observes a suspicious activity, it will consult a list of rules to determine an appropriate action. For example, it may allow the program to continue performing the desired operation or it may terminate the program before the program attempts to perform the operations. If no appropriate rule is found, the behavior blocker will consult the user/administrator. A behavior blocker has many advantages [Auburn University]. Among them are: it is more resistant to unknown threats than virus scanning and integrity checking [Auburn University]; no need exists to download new virus definitions - system does not necessarily require continual maintenance [Auburn University]. The disadvantages are namely: continuous monitoring of every aspect of system can greatly reduce system speed [Auburn University]; monitoring memory allocation, network access, file system access simultaneously is an expensive proposition [Auburn University]; many possible false positives can occur -- artificial intelligence (AI) has simply not matured enough to correctly

interpret every system action; system is not "bullet proof" -- new viruses may be able to perform actions that do not get flagged, but can still be used to execute payload [Auburn University]; new viruses may be able to emulate other programs installed on the system, fooling the system [Auburn University]. Despite these disadvantages, a behavior blocker offers great opportunities for future research in modeling anti-virus system. According to Auburn University [Auburn University], behavior blocking appears to be the future of anti-virus. In fact model construction, for the socially-aware purposeful agent [Nyamekye 2013, Lefebvre and Nyamekye 2014] -- an emerging behavior blocker with cognitive capabilities -- is an example of such a research endeavor that can potentially fulfill such a research need.

Under the request by the Department of Defense for examining the theory and practice of cyber security, JASON Program Office at MITRE Corporation [JASON], conducted a study for identifying several subfields of computer science that might be specifically relevant to the science of cyber security. More importantly, JASON's efforts included evaluating whether some underlying fundamental principles that would make it possible to adopt a more scientific approach, existed to identify what was needed in creating a science of cyber security. Furthermore, JASON should recommend specific ways in which scientific methods could be applied for modeling cyber security. Among the subfields of computer science that JASON's study covered, were, namely: model checking, cryptography, randomization, and type theory [JASON]. For simplicity, we will use JASON to represent JASON Program Office at MITRE Corporation. A direct excerpt from JASON's study, noted the following: *in model checking, one develops a specification of an algorithm and then attempts to validate various assertions about the correctness of that specification under the specific assumptions about the model. Cryptography, which examines communication in the presence of an adversary and in which the assumed power of that adversary must be clearly specified is viewed today as a rigorous field, and the approaches pursued in this area hold useful lessons for a future science of cyber-security. The use of obfuscation, in which one attempts to disguise or randomize the data paths and variables of a program, can help in constructing defenses against some common modes of attack. Type theory is any of several formal systems that can serve as alternatives to naive set theory and is also effective in reasoning about the security of programs. Game theoretic ideas will be useful in understanding how to prioritize cyber defense activities. Game theoretic approaches provide a framework for reasoning about which critical assets must be chosen for protection against cyber security risks*. The implication of JASON's study is that Game Theory provides the technical and scientific foundation for cybersecurity efforts! Though JASON's study was promising (and it is still so), it did not provide an in-depth discussion on how Game Theory could be employed to address cyber security.

Bruschi et al. [Bruschi et al. 2006] proposed a strategy for the detection of metamorphic malicious code inside a program P based on the comparison of the control flow graphs of P against the set of control flow graphs of known malware. They provided experimental data supporting the validity of their strategy. We should point out that a metamorphic malicious code exhibits a dynamic behavior instead of some static *properties* (e.g. fixed byte sequences or strangeness in the

executable header) [Bruschi et al. 2006]. Thus, malware detection, which is normally performed by pattern matching, within which malware detectors have a database of distinctive patterns (the signatures) of malicious code and they (malware detectors) look for the signatures in possibly infected systems, does not work well with metamorphic malicious codes [Bruschi et al. 2006]. In fact, virus scanners employ pattern matching techniques for detecting malicious codes.

In response to the cyber security threats to the U.S. critical infrastructure, President Obama signed an Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013 [Whitehouse]. The Executive Order was designed to increase the level of core capabilities for U.S. critical infrastructure to manage cyber risk. It did this by focusing on three key areas: (1) information sharing, (2) privacy, and (3) the adoption of cybersecurity practices. The EO tasked the National Institute for Standards and Technology (NIST) to work with the private sector to identify existing voluntary consensus standards and industry best practices and build them into a Cybersecurity Framework. The NIST closely worked with the private sector to create the Cybersecurity Framework 1.0 [NIST]. The author of this technical paper contributed to the development of the CSF, through submission of comments to NIST [Nyamekye November 13, 2013; Nyamekye November 15, 2013]. The NIST Cybersecurity Framework contains three primary components: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. A direct excerpt from the Framework will be helpful to provide an overview of the Framework.

The Framework Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

The Framework Profile represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as

the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations. The Framework not only provides an excellent common language to standardize the approach for addressing cybersecurity concerns, but also it provides the foundation on which the cybersecurity risks mitigation community must think about creating a proactive methodology -- *Framework Implementation Tier 4* -- for addressing cybersecurity threats before they even occur. A behavior blocker naturally fits into this new paradigm. Most importantly, the author's paper addresses such a critical issue on proactive methodology. We will later discuss how this paper fulfills this issue and agility as noted before. Today, many of the antivirus solutions react to cybersecurity threats after they occur. Thus, it is fitting to emphasize the importance of this paper in augmenting the NIST's Cybersecurity Framework 1.0.

Recent publication of Lefebvre and Nyamekye [Lefebvre and Nyamekye 2014] has discussed how we can use RGT to model terrorists' activity. Both authors' work provides some insightful ideas into modeling the cyber security threats in endpoint devices.

The organization of this paper is as follows. In the subsequent sections we will first discuss an overview of RGT, and purposeful individuals and socially-aware purposeful agents, followed by the mathematical model of RGT in *choice or decision making* of a socially-aware purposeful agent. Based on the recent author's work [Nyamekye June 8, 2015], we will discuss a socially-aware purposeful that can behave as an elementary subject (with new features established as an extension of RGT), and as a non-elementary subject, within the context of elementary and non-elementary subjects, respectively, as previously noted. Borrowing from the previous work of Lefebvre [Lefebvre 1977] we will provide the theoretical framework for *situational awareness*. Then four examples will be given to demonstrate how we can use RGT to model cybersecurity threats. Conclusions will then follow. Appendix A will borrow from pi-calculus to model *interaction* as the basis for information sharing among DoD System-of-Systems to mitigate cybersecurity risks.

OVERVIEW OF REFLEXIVE GAME THEORY (RGT), PURPOSEFUL INDIVIDUALS AND SOCIALLY-AWARE PURPOSEFUL AGENTS

From the viewpoint of the classical game theory, decision making involves two types of theories, namely: descriptive theory and prescriptive theory. The descriptive theory is about a choice

prediction of a player [Lefebvre 2010], and the prescriptive theory is about the choices the player must make – choice selection from the choice prediction. To minimize the losses of a player, the classical game theory employs max-min decision function for both theories. A major issue with the classical game theory is that a player is inclined to an irrational risk in making a decision – from faulty reasoning process [Lefebvre 2010]. Consequently, we cannot use the classical game theory when we want to minimize risk in choice or decision making. Particularly in cybersecurity modeling, where much uncertainty (e.g., a deceitful cyber hacker's instrument in the endpoint's internal operating environment) could lead to irrational risk in the socially-aware purposeful agent choice or decision-making, -- inadvertently deleting a software application from a trusted and known source -- the classical game theory is inappropriate for decision-making. More importantly, the classical game theory does not account for the cognitive system of the socially-aware purposeful agent – e.g. the socially-aware purposeful agent -- in decision making. The RGT addresses such deficiencies in choice or decision making. The goal of RGT is to predict the individual choice made by a socially-aware purposeful agent belonging to a group [Lefebvre 2010]. Also, the RGT can predict the influences of other socially-aware purposeful agents in a group on another socially-aware purposeful agent to make a particular choice [Lefebvre 2010]. We call such an extension of the RGT, reflexive control [Lefebvre 2010]. This paper will not address reflexive control. Please note that a socially-aware purposeful agent can represent single individuals or different types of organizations, e.g., military units, political parties, and even states [Lefebvre 2010]. Though this paper will not deal with reflexive control, the concept of reflexive control is very intriguing and deserves attention, especially for cybersecurity modeling. For example, in cybersecurity modeling if the socially-aware purposeful agent can find the Internet Protocol (IP) address of the cyber hacker's endpoint device, the socially-aware purposeful agent can send a deceptive message to the cyber hacker to purposely influence the cyber hacker to make a decision that would benefit the objectives of the socially-aware purposeful agent. The idea here is to create a mental model of the cyber hacker and thereby use it to influence the cyber hacker's future actions. The author's future publications will address reflexive control, in cybersecurity modeling. The term socially-aware purposeful agent draws from the purposeful individual or system [Ackoff et al. 2006; Lefebvre 2010]. A brief overview of a purposeful individual, system or a socially-aware purposeful agent is essential, before subsequent discussions.

A purposeful individual or system [e.g., a cyber hacker or system (e.g., a weapon system)] is one that not only can change its behavior to pursue the same goal -- as conditions in the operating environment change --, but also a purposeful individual or system is one that can choose its own goals and the means by which to pursue the goals [Ackoff et al. 2006]. *A purposeful individual or system thus displays will* [Ackoff et al. 2006.] Please note that a purposeful individual or system can also learn and adapt itself to uncertainties in its environment [Ackoff et al. 2006]. More importantly, the environment of the individual or system cannot choose the goals for the purposeful individual or system! This statement implies that a purposeful individual or system is a PROACTIVE system (as opposed to a simple "Pavlovian" system that just reacts to changes in its surrounding environment, e.g., a virus scanner). Only humans or people are purposeful individuals or systems! Thus, Nano-devices, artificial intelligent robots, etc., are not purposeful systems. They emulate purposeful systems. Ackoff et al. [Ackoff et al. 2006] call such systems, multi-goal-seeking individuals or systems. The users -- humans (e.g., the strategic corporal) -- of these systems set the goals! ***We define socially-aware purposeful agents to be agents that can set their own***

goals and they have the same cognitive capabilities closely resembling those demonstrated by humans. ***Contrary to the socially-aware purposeful agents, the traditional agents cannot set their own goals and they lack cognitive capabilities of humans*** [Nyamekye 2013; Lefebvre and Nyamekye 2014]. This is the fundamental difference between the traditional agent and the socially-aware purposeful agent. In fact North and Macal [North and Macal 2007, Page 102] clearly articulate the *traditional agent* as follows: "*The fundamental features that make something a candidate to be modeled as a traditional agent are the capabilities of the component to make independent decisions, some type of goal to focus the decisions, and the ability of other components to tag or individually identify the component." Unlike the socially-aware purposeful agent that sets its own goals, the traditional agent must use the goal set by some individual or the user of the system being modeled*. We should emphasize that the term socially-aware purposeful agent replaces the author's previous term, purposeful agent [Nyamekye 2013; Lefebvre and Nyamekye 2014].

SOCIALLY-AWARE PURPOSEFUL AGENT: AS AN ELEMENTARY SUBJECT AND NON-ELEMENTARY SUBJECT, RESPECTIVELY

A theory must be logically completed [Lefebvre 2010]. For logical completeness, RGT must include a diagonal form consisting of one letter, Equation 1. We call this form an elementary subject. The elementary subject has the *freedom of choice* [Lefebvre 2010]. A dismounted Warfighter investigating the presence of a landmine on the battlefield, while the other members of the small unit search for the enemy on the battlefield, is an example of an elementary subject. We will later discuss the *freedom of choice*. Please note that such a dismounted Warfighter may not be temporarily interacting with the small unit, as he or she focuses his or her attention on the landmine. By logical completeness, we mean that Equation 1 should not include non-defined elements [Lefebvre 2010]. Because of this, the subject's choice cannot be predicted by an external observer [Lefebvre 2010]. To predict subjects' possible choices, RGT needs at least two subjects with their *relations* [Lefebvre 2010]. We will later discuss the *relations* among non-elementary subjects. We call such subjects non-elementary subjects [Lefebvre 2010]. When the dismounted Warfighter investigating the presence of a landmine on the battlefield changes from non-interaction to interaction with the small unit, he or she becomes a non-elementary subject. Borrowing from Lefebvre's work [Lefebvre 2010], we represent the theoretical model of an elementary subject by a diagonal form of the type shown in Equation 2a.

$$a = [a] \qquad \text{Equation 1}$$

$$\Phi = P^{W} \qquad \text{Equation 2a}$$

where P is the bottom-most polynomial of the diagonal form [Lefebvre 2010]; $W = A_1 * A_2 * \ldots * A_k$; $k \geq 2$; * either "**.**", or "**+**", and A_i diagonal forms representing the subject's images of self [Lefebvre 2010]. We should emphasize that W is the non-elementary subject's *integral image of*

the self [Lefebvre 2010], which in RGT consists of a collection in cooperation or conflict with one another [Lefebvre 2010]. For details about the *integral image of the self*, please refer to the previous publication of Lefebvre and Nyamekye [Lefebvre and Nyamekye 2014]. Most importantly, W is the result of the non-elementary subject's *mental choice*, in the subject's cognitive system [Lefebvre 2010]. This statement does not imply that an elementary does not have a cognitive system or a mental system. It simply means that W is the result of the *choice* made by the *integral image of self* – in the subject's mind -- for a non-elementary subject. Equation 2a is an exponential function [Lefebvre 2010], with P, the base and W, the exponent of the function, respectively. Equation 2a can be represented as Equation 2b. Lefebvre calls it a *reflexion function*.

$$\Phi = P + \bar{W} \qquad \text{Equation 2b}$$

Because of the importance of the elementary subject in cybersecurity modeling and more importantly in many situations on the battlefield, the author has recently extended the RGT to establish new features for an elementary subject (elementary socially-aware purposeful agent). Below is the direct excerpt from the author's work [Nyamekye June 8, 2015]:

Awareness: An elementary subject (elementary socially-aware purposeful agent) is aware of "something [Ackoff and Emory]" if he or she forms a "mental picture (image) [Lefebvre 1977] of the "something". The elementary subject (elementary socially-aware purposeful agent) is said to have a situational awareness of the "something." The "something" may be an instrument [Ackoff and Emory 2006], e.g., a landmine (on the battlefield), used by another elementary subject (elementary socially-aware purposeful agent) to coproduce some outcome of that elementary subject's (elementary socially-aware purposeful agent's) action [Ackoff and Emory 2006] against the elementary subject (elementary socially-aware purposeful agent).

Understanding: An elementary subject (elementary socially-aware purposeful agent) understands the meaning of the mental picture (image) of the "something" if he or she influences [Lefebvre 1977] himself or herself that the "something" can produce a course of action [Ackoff and Emory 2006] against him or her with desirable or undesirable outcome. The elementary subject (elementary socially-aware purposeful agent) is said to have self-influence [Lefebvre 1977]. That "something" may be an instrument used by another elementary subject (elementary socially-aware purposeful agent) to coproduce the outcome of that elementary subject's (socially-aware purposeful agent's) action.

Decision: An elementary subject (elementary socially-aware purposeful agent) has the freedom of choice [Lefebvre 1977], from which he or she can choose a realizable set of actions or an alternative [Lefebvre 1977]. The elementary subject (elementary socially-aware purposeful agent) is said to make a decision. Please note that while these extra features are extensions of RGT, they do not ensue from RGT. For simplicity, we will interchangeably use the term *an elementary socially-aware purposeful agent* with *an elementary subject*.

MATHEMATICAL MODEL OF REFLEXIVE GAME THEORY (RGT) FOR CHOICE OR DECISION MAKING

Conceptual Representation of a socially-aware purposeful agent

In RGT, we assume that a socially-aware purposeful agent can perform actions $\alpha 1, \alpha 2, \ldots, \alpha s, S \geq 1$ [Nyamekye 2013; Lefebvre 2010]. Such actions are initially defined, similar in concept to the actions initially defined for an *automaton* in pi-calculus [Milner 1999]. Also, we assume that the socially-aware purposeful agent can perform these actions both technically and morally [Nyamekye 2013; Lefebvre 2010]. According to Lefebvre, *the relation of preference on the set of actions is not given.* He defines a universal set, as a non-empty set of actions which can be represented as 1. Please note that an empty set contains no elements or actions. The set ***M*** of all subsets of the universal set, including an empty set, is the set of alternatives [Nyamekye 2013; Lefebvre 2010]. That is, each alternative is a subset of the universal set of actions. The socially-aware purposeful agent's action then consists of choosing an alternative from the set ***M*** and then "realizing" the "choice" [Lefebvre 2010]. When a socially-aware purposeful agent chooses an empty set, it means that the socially-aware purposeful agent refuses to choose any non-empty alternative. To distinguish between the "realization" and "choice", consider a universal set which consists of two sets [Nyamekye 2013; Lefebvre 2010]:

$\alpha 1$- turn left
$\alpha 2$- turn right

We represent the universal set as 1= $\{\alpha 1, \alpha 2\}$, and empty set as 0 = {}. Using the Boolean algebra, we can represent all the possible alternatives (set of actions) as:

1= $\{\alpha 1, \alpha 2\}$, $\{\alpha 1\}$, $\{\alpha 2\}$, 0 = {}

Please note that if the universal set consists of elements (actions), then we can always find the corresponding Boolean algebra, consisting of all the possible set of actions, including the empty set, from the relationship 2^Z (power set) [Lefebvre 2010]. Please note that the set ***M*** as previously noted, includes not only the set of all subsets of the universal set, -- 4 in the above case --, but also the set ***M*** includes the Boolean operations "+", "**.**", "***negation***", and the relation "***greater or equal***". The choice of $\{\alpha 1\}$ means that the socially-aware purposeful agent can perform only action $\alpha 1$, and the choice of $\{\alpha 2\}$ means that the socially-aware purposeful agent can perform only action $\alpha 2$. Consider the alternative $\{\alpha 1, \alpha 2\}$. Since the socially-aware purposeful agent cannot perform actions $\alpha 1$(turn left) and (turn right) $\alpha 2$ at the same time, alternative $\{\alpha 1, \alpha 2\}$ is not realizable. However, the socially-aware purposeful agent can realize either subset $\{\alpha 1\}$ or subset $\{\alpha 2\}$ after socially-aware purposeful agent chooses alternative $\{\alpha 1, \alpha 2\}$. The socially-aware purposeful agent does nothing if the socially-aware purposeful agent chooses the empty set 0 = {}.

Choice or Decision Making Equation of a socially-aware purposeful agent

Equation 3 predicts the choices of a socially-aware purposeful agent. Equation 3 is the descriptive model we noted before.

$$X = AX + B\bar{X} \qquad \text{Equation 3}$$

where X, A, B ϵ(elements of) $\boldsymbol{M}$ and A and B do not depend on X [Lefebvre 2010]. Equation 3 has a solution if and only if Equation 4 is valid. The "+" represents the Boolean operator.

$$A \supseteq B \qquad \text{Equation 4}$$

Using Equations 3 and 4, we can find alternatives that the socially-aware purposeful agent can realize. The socially-aware purposeful agent then performs the set of actions, from the chosen alternatives. This last step is the prescriptive model. In RGT, a socially-aware purposeful agent can exhibit four states ***of behavior*** [Lefebvre 2010]: the socially-aware purposeful agent cannot make a choice or ***is in a state of frustration***; the socially-aware purposeful agent can have a freedom of choice or ***is in a state of free choice***; the socially-aware purposeful agent can ***only*** choose to do nothing or ***is in a passive state***; the socially-aware purposeful agent can choose to perform some action or ***is in an active state***.

MODELING SITUATIONAL AWARENESS

We will borrow from the pioneering work of Lefebvre [Lefebvre 1977] on the structure of awareness, to discuss *situational awareness*. Consider an elementary socially-aware purposeful agent which can be an inanimate or animate system, for example, a socially-aware purposeful agent, with a cognitive capability. As we noted before, an elementary socially-aware purposeful agent's choices of alternatives are known -- prescriptive model. Thus, the RGT does not apply for an elementary socially-aware purposeful agent. That is, RGT only applies to interaction between at least two socially-aware purposeful agents, as we previously discussed. Consider the strategic corporal in the rural area of the indigenous people in Afghanistan. At time $\boldsymbol{t0}$ the strategic corporal sees an object which resembles an improvised explosive device (IED) at a nearby place in the village. We should emphasize that the IED is an instrument which some insurgent (a socially-aware purposeful agent) has placed at the location. Let us suppose that at $\boldsymbol{t0}$ the strategic corporal has not yet formed an image within him or her. According to Lefebvre [Lefebvre 1977], we can represent the situation at $\boldsymbol{t0}$ by Equation 5.

$$\Omega 0 = T \qquad \text{Equation 5}$$

where T = represents the IED. At time $t1$, the strategic corporal forms a *mental picture (image)* of the IED. That is, he or she becomes aware that the IED could be a deadly object to him or her. According to Lefebvre, we can represent the situation at $\boldsymbol{t1}$ by Equation 6.

$$\Omega 1 = T + Tx \qquad \text{Equation 6}$$

where Tx = image of the IED within the strategic corporal. Equation 6 models the *situational awareness* of an elementary socially-aware purposeful agent -- the strategic corporal. We will

discuss awareness of a socially-aware purposeful agent in a group consisting of two socially-aware purposeful agents.

EXAMPLES

Example 1: A cyber hacker interacts with the supplier of a major retail company. The hacker sends a virtual instrument -- a malware, e.g., a Trojan -- to the supplier's desktop PC. The virtual instrument then steals the login credentials which the supplier uses to access the database of the retail company. Using another virtual instrument -- a malicious code -- and the stolen login credentials, the hacker successfully penetrates into the retail company's information system and steals massive personal data of the retailer's customers. For simplicity, we will create the cybersecurity model for the interaction between the cyber hacker and the supplier (user). The interaction, between the cyber hacker and the supplier, represents an example between a group consisting of two socially-aware purposeful agents -- the cyber hacker and the supplier or the user. Figure 1 shows the basic diagram of the interaction between the cyber hacker and user.

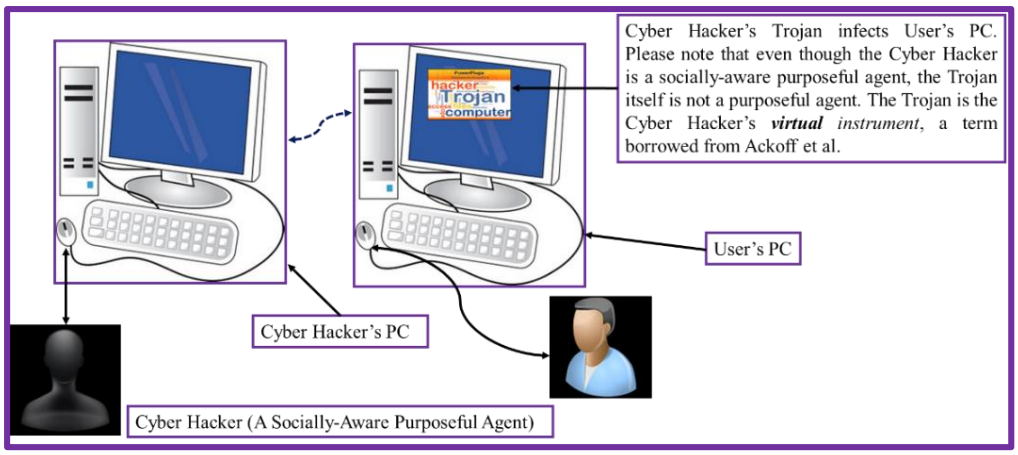


Figure 1. Interaction between a Cyber Hacker and a User (Supplier).

In RGT, constructing a model begins with the definition of the socially-aware purposeful agents, which in this example are, namely: the cyber hacker and the user, in Figure 1. Also, the socially-aware purposeful agents define their ***set of actions***. The next step is the construction of the graph, Figure 2, which represents the relationships between the socially-aware purposeful agents. For example, a dotted line represents conflict, and a solid line represents cooperation, between any two socially-aware purposeful agents. Letter "a" stands for a victim (user). Letter "b" stands for the cyber hacker; b = 1 means b's influence to "a" is to allow penetration to a's system; b=0 means the absence of this influence.

Please notice that we have modeled the relationship between the cyber hacker and the user, as a cooperation. Typically, cyber hackers usually pretend to be nice folks whenever they infiltrate into the endpoint devices of users. That is, they pretend to be acquaintances of the users and thus they

feel they are no threats to the users. We have assumed that the user has no antivirus application installed on his or her desktop PC. Even if an antivirus application exists, the cyber hacker's malicious code can conceal itself from detection -- metamorphic malware. For details about constructing the graph in RGT, please see the work of Lefebvre [Lefebvre 2010]. From the graph, Figure 2, we then construct the polynomial, Equation 7, which represents the analytical notation of the graph, where the "+", represents the Boolean operation for addition, and "**.**", represents the Boolean operation for multiplication [Lefebvre 2010]. Again, for details about the polynomial in RGT, please see the work of Lefebvre [Lefebvre 2010].

Figure 2. The Graph, Depicting Cooperation between the Cyber Hacker and the User.

$$[a].[b] \qquad \text{Equation 7}$$

The next step is to convert the polynomial into a diagonal form, Equation 8. The first part of the diagonal form represents the group's influence on the socially-aware purposeful agent, in making a choice or decision. The rest of the diagonal form represents the mental choice (from the cognitive system), W, in Equation 2, of the socially-aware purposeful agent. We can think of the diagonal form as an exponential function (Equation 2a), where the base of the exponential function is the same as the polynomial (Equation 7 or P in Equation 2a) and the exponent (same as W in Equation 2a) is the mental choice of the socially-aware purposeful agent, in decision-making. Again, for details about the diagonal form in RGT, please see the work of Lefebvre [Lefebvre 2010].

$$a = [a].[b]^{[a].[b2]} \qquad \text{Equation 8}$$

In a cybersecurity threat where the cyber hacker manages to attack the user's endpoint device, -- with or without antivirus application --, we can model the situation as follows: a is not aware of b's influence; the values of b are different on the first and second tiers: b1 is a's subconscious image of b; b2 is a's conscious image of b. Substitution of b1 and b2 into Equation 8 yields Equation 9.

$$a = [a].[b1]^{[a].[b2]} \qquad \text{Equation 9}$$

During the cyber hacker's attack, the user subconsciously feels that strange signals in the desktop's operating system do not mean the existence of outside influence, but his or her conscious analysis shows that something is threatening the operating system's normal functioning: b1 = 0, b2 = 1. That is, the user is ***unaware*** at his or her subconscious level that his or her PC is being attacked. The user only becomes ***aware*** at his or her conscious level that his or her PC has been attacked. Substitution of b1 and b2 into Equation 9 yields Equation 10.

$$a = [a].[0]^{[a].[1]}$$ Equation 10

Using the *reflexion function* [Lefebvre 2010], Equation 2b, we can then transform the diagonal form into the final analytical form, Equation 11, to obtain the generic choice equation for a.

$$a = [a].[0]^{[a].[1]} = 0 + \bar{a} = \bar{a}$$ Equation 11

Equation 11 says that "a" cannot make a choice. That is, the user is in a state of frustration -- cannot perform any action! The cyber hacker has used his or her virtual instrument -- malicious code, e.g., a Trojan -- to totally take control of the user's PC. More importantly, the hacker has already stolen the login credentials for penetrating into the retailer's information system!

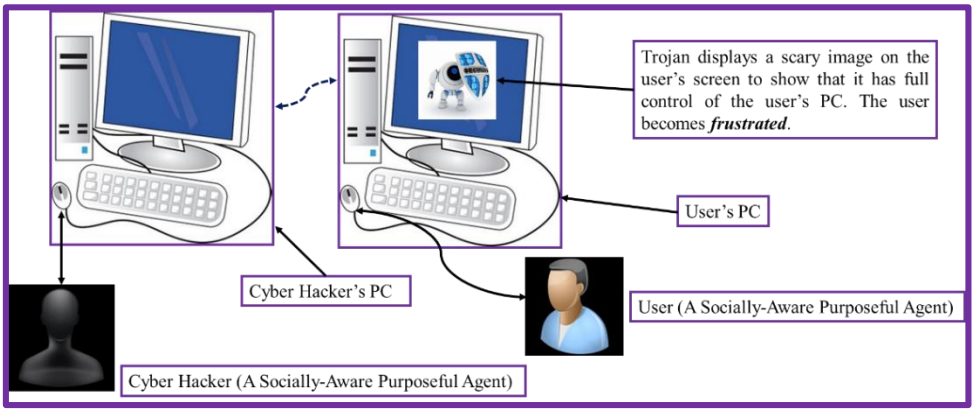


Figure 3. User's Frustration (Awareness) After Trojan Infects User's PC.

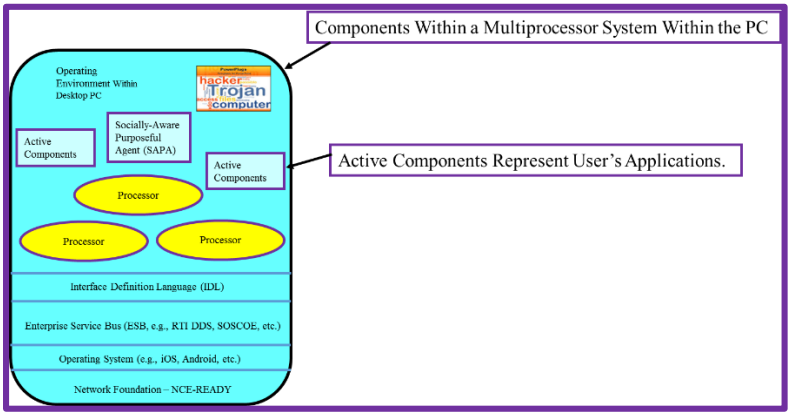


Figure 4. Multiprocessor System with Socially-Aware Purposeful Agent.

Figure 3 shows the user's frustration after the cyber hacker uses his or her virtual instrument, e.g., Trojan to infect the user's PC.

Example 2: Suppose we now explore building an emerging socially-aware purposeful agent or an emerging ***behavior blocker***, to address the cyber security threat in Example 1.

Figure 4 shows a new multiprocessor system that we have invented within the PC of the user. For simplicity, we have omitted the details of the new multiprocessor system. The active components represent the user's application programs. The multiprocessor system also contains a ***socially-aware purposeful agent***, which we have also invented to continuously monitor the system and to create ***a situational awareness*** (Equation 6) of any object it encounters. Then it takes remedial actions to destroy any malicious threat, e.g., Trojan. In this example only one socially-aware purposeful agent or an elementary subject exists. As we noted before, RGT requires at least two socially-aware purposeful agents. However, we can use Equation 1 to represent the set of actions of the socially-aware purposeful agent. In this case, the socially-aware purposeful agent is ***in a state of free choice***.

$$a = [a] \qquad \text{Equation 1}$$

The implication of the socially-aware purposeful agent is that not only can it exhibit a dynamic behavior but it can choose its goals and a set of actions to fulfill the new goals. Thus, it can deal with any emerging cybersecurity threat, similar in concept to the strategic corporal dealing with a variety of emerging warfighting situations in irregular warfare (IW).

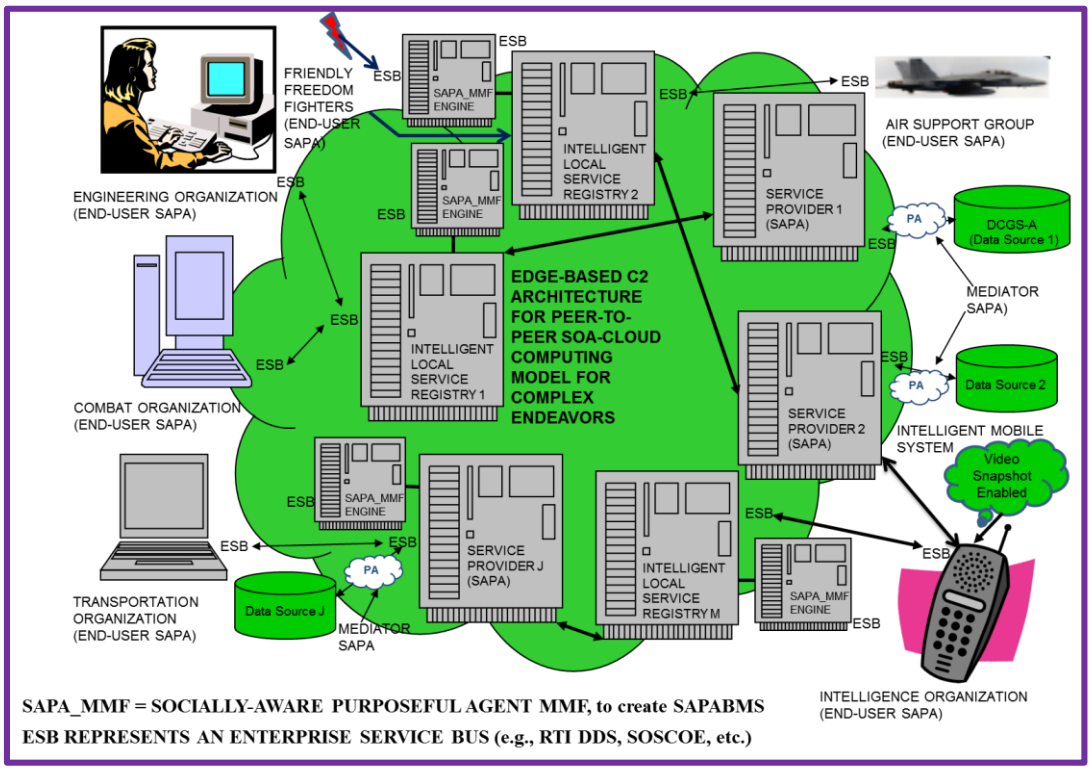


Figure 5. MTMMF SAPA-Based Modeling and Simulation (SAPABMS) C2 and Supporting System-of-Systems Architecture [Nyamekye 2010].

Example 3: To mitigate cybersecurity risks in a net-centric ecosystem for supporting the warfighters on the battlefield, we have extended our model by introducing a socially-aware purposeful agent in each endpoint device for the Multi-Threaded Missions and Means Framework (MTMMF) Socially-Aware Purposeful Agent-Based Modeling and Simulation (SAPABMS) Command and Control (C2) and the Supporting System-of-Systems Architecture. For details on the MTMMF and net-centric ecosystem for C2 and the Supporting SoS Architecture, please see the previous work of Nyamekye [Nyamekye 2010]. Figure 5 shows such architecture.

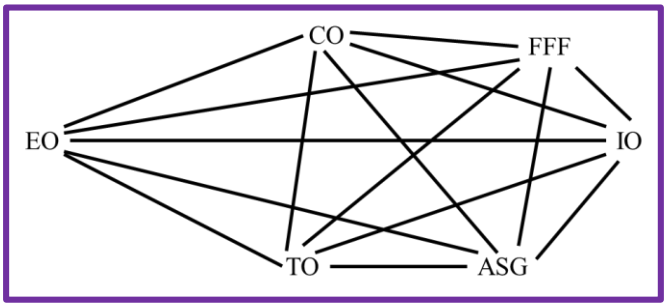


Figure 6. Graph for Interaction among the Socially-Aware Purposeful Agents in Multi-Threaded Missions and Means Framework (MTMMF) Socially Aware Purposeful Agent-Based Modeling and Simulation (SAPABMS) Command and Control (C2) and the Supporting System-of-Systems Architecture [Nyamekye 2010].

The group consists of six socially-aware purposeful agents. They are represented as follows: Engineering Organization (EO), Combat Organization (CO), Transportation Organization (TO), Intelligence Organization (IO), Air Support Group (ASG), and Friendly Freedom Fighters (FFF) -- represented as one group. Cooperation exists among them. Figure 6 depicts the graph; each node corresponds to a socially-aware purposeful agent. The set of actions for each socially-aware purposeful agent includes: monitor system for suspicious activity, terminate the program for suspicious activity, destroy program with suspicious activity. Thus, the universal set of actions is: 1 = {monitor system for suspicious activity, terminate the program for suspicious activity, destroy program with suspicious activity}. Each socially-aware purposeful agent influences each other to report any suspicious activity that each socially-aware purposeful agent encounters from any cyber security threat and the action the socially-aware purposeful agent takes to eliminate the threat to all socially-aware purposeful agents in the group. Equations 12 and 13 give the polynomial and the diagonal form, respectively.

$$[EO].[CO].[TO].[IO].[ASG].[FFF] \quad \text{Equation 12}$$

$$[EO].[CO].[TO].[IO].[ASG].FFF^{[EO].[CO].[TO].[IO].[ASG].[FFF]} \quad \text{Equation 13}$$

$$[EO].[CO].[TO].[IO].[ASG].FFF^{[EO].[CO].[TO].[IO].[ASG].[FFF]} = 1 \quad \text{Equation 14}$$

Transforming the diagonal form into a final analytical form (by applying the *reflexion function*, Equation 2b), yields Equation 14. Equation 14 says that all socially-aware purposeful agents are *superactive* agents [Lefebvre 2010]. That is, each socially-aware purposeful agent always chooses alternative 1 = {monitor system for suspicious activity, terminate the program for suspicious activity, destroy program with suspicious activity}. More importantly, each socially-aware purposeful agent cannot influence the behavior of other socially-aware purposeful agents, in the group. That is, no socially-aware purposeful agent's choice of action -- from the universal set of actions -- depends on any socially-aware purposeful agent's influence. At any state, the socially-aware purposeful agent can only choose and execute one action from the universal set. More importantly, each socially-aware purposeful agent can exhibit a dynamic behavior -- change its behavior depending on the cybersecurity threat -- at any state. Superactive behavior of a socially-aware purposeful agent is quite intriguing in cyber security threats, because such a behavior implies that no master-slave relationship, -- which usually may slow down the decision a socially-aware purposeful agent must make in critical situations --, exists among the agents. Such a behavior of a superactive socially-aware purposeful agent is the thinking behind the behavior of a "strategic corporal" when dealing with insurgents' dynamic behaviors at the tactical level in irregular warfare (IW). The strategic corporal can call for air support if needed but he or she needs not to wait for the commander to tell him or her what to do at the tactical level in attacking and defeating insurgents in IW.

Example 4: The elementary socially-aware purposeful agent dynamically changes its behavior to be in conflict with the cyber hacker after realizing from the ***situational awareness*** of the cyber hacker's instrument -- Trojan -- that the cyber hacker intends to inflict harm. The model is identical to Example 1 except that Figure 1 is slightly modified to depict the socially-aware purposeful agent, to monitor the Trojan on the PC's screen. Figure 7 shows the modified Figure 1.

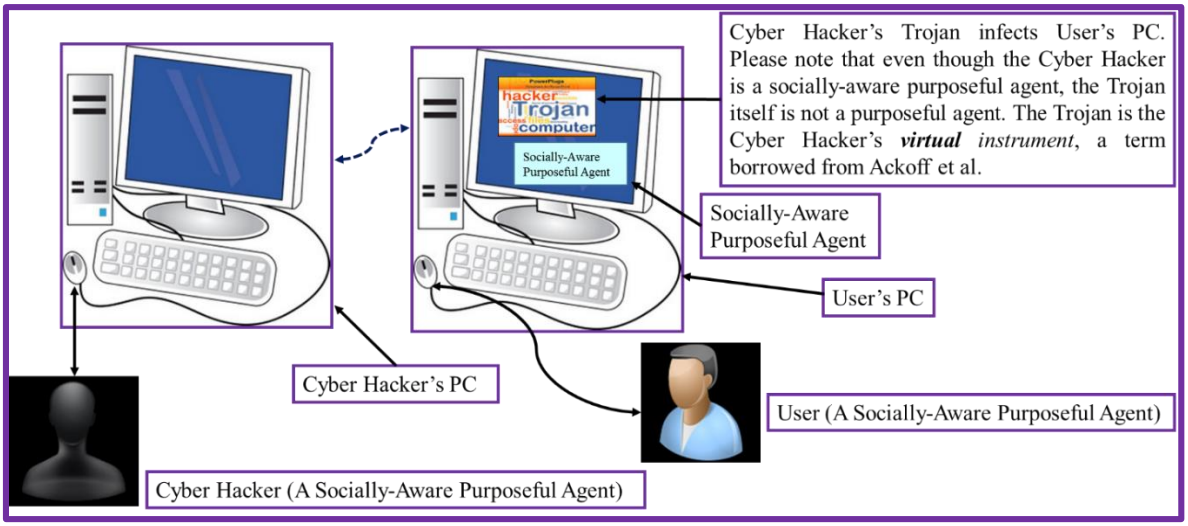


Figure 7. Interaction between a Cyber Hacker and a Socially-Aware Purposeful Agent.

Please note that Figure 7 has our newly invented multiprocessor system (in Figure 4) which contains the ***socially-aware purposeful agent***. As we noted in Figure 4 we have also invented the ***socially-aware purposeful agent*** into the system to continuously monitor the system and to create ***a situational awareness*** (Equation 6) of any object it encounters. Figure 8 depicts the graph model, which is a dotted line to indicate that the socially-aware purposeful agent is in conflict with the cyber hacker. We then construct the polynomial, Equation 15, which represents the analytical notation of the graph, where the "+", represents the Boolean operation for addition [Lefebvre 2010]. Again, for details about the polynomial in RGT, please see the work of Lefebvre [Lefebvre 2010].

Figure 8. The Graph, Depicting Conflict between the Cyber Hacker and the Social-Aware Purposeful Agent.

$$[a] + [b] \qquad \text{Equation 15}$$

Following the same concept in Example 1, we convert the polynomial into a diagonal form, Equation 16.

$$a = [a] + [b]^{[a]+[b]} \qquad \text{Equation 16}$$

Since "a" is aware of "b's" influence (the value of b is the same on the first and second tiers). Using the *reflexion function* [Lefebvre 2010] as in Example 1, we then transform the diagonal form into the final analytical form, Equation 17.

$$a = [a] + [b]^{[a]+[b]} = a + b + \overline{a + b} = 1 \qquad \text{Equation 17}$$

Now, "a" has become a superactive socially-aware purposeful agent and chooses an action to destroy the cyber hacker's instrument. Through the deceptive action that we noted before, the socially-aware purposeful agent can also take a proactive approach to getting the mental model of the cyber hacker that sent the instrument – Trojan.

Rather than using the traditional software engineering concepts such as the manifesto for agile software development to discuss agility, we have borrowed from the previous work of Alberts and Hayes [Alberts and Hayes 2003] which has much technical and scientific rigor, for our effort. A direct excerpt, from both authors' work, to describe the six key attributes of agility, will be helpful [Alberts and Hayes 2003].

Robustness: the ability to maintain effectiveness across a range of tasks, situations, and conditions;

Resilience: the ability to recover from or adjust to misfortune, damage, or a destabilizing perturbation in the environment;
Responsiveness: the ability to react to a change in the environment in a timely manner;
Flexibility: the ability to employ multiple ways to succeed and the capacity to move seamlessly between them;
Innovation: the ability to do new things and the ability to do old things in new ways; and
Adaptation: the ability to change work processes and ability to change the organization.

Our socially-aware purposeful agent can fulfill these attributes. When a socially-aware purposeful agent dynamically changes his or her behavior from elementary socially-aware purposeful agent to a non-elementary subject, he or she is indeed retaining a level of *responsiveness*. Furthermore, when a socially-aware purposeful agent employs a different set of actions to defeat a malware threat, he or she is maintaining a level of *flexibility*.

This paper has many applications. For example, we can employ the socially-aware purposeful agents to design resilient systems against cyber security threats for any organization. Most importantly, we can use socially-aware purposeful agents to create a robust system-of-systems to mitigate cyber security threats in a DoD net-centric ecosystem. In fact, Example 3 (Figures 6 and 7) demonstrates such an application of the paper. We should emphasize that Example 3 fulfills one of the tenets of President Obama's Executive Order (EO) 13636.

CONCLUSIONS

Using the *socially-aware purposeful agent* and the Reflexive Game Theory (RGT), this paper has established the framework for constructing a theoretical model for cybersecurity. Most work to date on cyber security has focused on virus scanning, with virtually no emphasis on the cyber hacker that deployed the malware on the user's endpoint devices. In fact the concept of a malicious code which the cyber hacker employs as an instrument in a user's endpoint device was even previously unheard of in the literature on cybersecurity. Thus, for the first time this paper has filled this missing gap by first introducing the concept of a virtual instrument to describe the malicious code. The paper has established the scientific model for the situational awareness. By extending the RGT, the paper has provided new features for an elementary subject or an elementary socially-aware purposeful agent. Of particular importance is the ability of the socially-aware purposeful agent to dynamically transition his or her behavior from an elementary subject to a non-elementary subject. Using the RGT we have constructed the socially-aware purposeful agent with a cognitive capability. We have invented a new multiprocessor system to contain a *socially-aware purposeful agent*, which could continuously monitor the system and create *a situational awareness* of any threat object it encounters. Four examples have been given to demonstrate the application of the model. Agility of the socially-aware purposeful agent has been discussed within the context of net-centric system-of-systems' architecture.

REFERENCES

Alberts, S. D., and Hayes, R. E. *Power to the Edge*, Command and Control Research Program, CCRP Publication Series, Washington, D.C. 2003.

Ackoff, R. L., and Emery F. E. *On Purposeful Systems: An Interdisciplinary Analysis of Individual and Social Behavior as a System of Purposeful Events*, Aldine Transaction, a Division of Transaction Publishers, New Brunswick (U.S.A.), 2006.

Auburn University, Computer Science Classes: *COMP 5370/6370*, http://www.eng.auburn.edu/cse/classes/comp6370/lessons/Lecture 7_Virus Detection & Prevention_x_6.pdf (Accessed June 11, 2015).

Bruschi, D., Martignoni, L., Monga, M. Detecting Self-Mutating Malware Using Control Flow Graph Matching, *PROCEEDINGS OF THE CONFERENCE ON DETECTION OF INTRUSIONS AND MALWARE & VULNERABILITY ASSESSMENT (DIMVA), IEEE COMPUTER SOCIETY*, 2006.

JASON, *Science of Cyber-Security*, the MITRE Corporation, McLean, Virginia, 2010.

Lefebvre, V. and Nyamekye, K. Construction of Theoretical Model for Antiterrorism: From Reflexive Game Theory Viewpoint, *Proceedings of 19th ICCRTS, Modeling and Simulation*, Paper Number 012, http://dodccrp.org/events/19th_iccrts_2014/post_conference/html/home.html (Accessed March 6, 2015), 2014.

Lefebvre, V. *The Structure of Awareness, Toward a Symbolic Language of Humans*, Sage Publications, 1977.

Lefebvre, V. A. *Lectures on Reflexive Game Theory*. Leaf & Oaks Publishers, 2010.

McBride, T., Waltermire, *D. SOFTWARE ASSET MANAGEMENT: Continuous Monitoring*, National Cybersecurity Center of Excellence, NIST, https://nccoe.nist.gov/sites/default/files/nccoe/Continuous%20Monitoring%20Building%20Block%20-%20Software%20Asset%20Management.pdf (Accessed March 9, 2015), September 16, 2013.

Milner, R. *Communicating and Mobile Systems: the Pi-Calculus*, Cambridge University Press, 1999.

NIST (National Institute of Standards and Technology). *Framework for Improving Critical Infrastructure, Version 1.0*, http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm (Accessed March 6, 2015), February 12, 2014.

North, M. J., and Macal C. H. 2007. *Managing Baines Complexity*, Oxford Univ. Press. NY, New York.

Nyamekye, K. Technical and Scientific Architecture For Testing and Evaluating Net-Centric Ecosystem, *Proceedings of 15th ICCRTS, Modeling and Simulation*, Paper Number 130, http://dodccrp.org/events/15th_iccrts_2010/html_post_conference/index_post_conference.html (Accessed March 6, 2015), 2010.

Nyamekye, K. *IABSRI's Framework Comments Submission*, IABSRI PART 1, http://csrc.nist.gov/cyberframework/framework_comments/20131125_kofi_nyamekye_iabsri_part1.pdf (Accessed March 6, 2015), November 13, 2014.

Nyamekye, K. *IABSRI's Framework Comments Submission*, IABSRI PART 2, http://csrc.nist.gov/cyberframework/framework_comments/20131125_kofi_nyamekye_iabsri_part2.pdf (Accessed March 6, 2015), November 15, 2014.

Nyamekye, K. *IABSRI's Response to NIST's Request for Information (RFI) on Cybersecurity Framework*, http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_iabsri_nyamekye.pdf (Accessed March 6, 2015), October 10, 2014.

Nyamekye, K. "Warfighter Decision Making in Complex Endeavors: Using Purposeful Agents and Reflexive Game Theory," *Proceedings of 18th ICCRTS: Modeling and Simulation*, Paper Number 074, http://www.dodccrp.org/events/18th_iccrts_2013/post_conference/papers/074.pdf (Accessed October 4, 2013), 2013.

Nyamekye, K. *Extension of the RGT For Establishing New Features For An Elementary*, June 8, 2015.

Nyamekye, K, and Lefebvre, V. *Definition of a Subject in RGT*, October 17, 2013.

Whitehouse. Foreign Policy, *Cybersecurity -- Executive Order 13636*, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/eo-13636 (Accessed March 6, 2015), February 12, 2013.

Wikipedia. Three Block War. http://en.wikipedia.org/wiki/Three_Block_War (Accessed March 6, 2015).

APPENDIX A: The Theoretical Model -- From the Viewpoint of Pi-Calculus -- for Interaction among Socially-Aware Purposeful Agents

For simplicity, we have directly borrowed an excerpt, from http://www.ebpml.org/pi-calculus.htm, for the theoretical model -- from the viewpoint of pi-calculus -- for interaction among socially-aware purposeful agents.

The ubiquity of TCP/IP and the Internet has enabled many systems to communicate with their environment with great ease. Such interactive systems are actually becoming the norm. Surprisingly, most of the work to model these categories of systems has started fairly recently when compared to the theory of sequential algorithmic processes (lambda-calculus) which is the foundation of all programming languages. Actually the first steps of lambda-calculus can be traced back to the 1600s with the work of Mathematician and Philosopher, Blaise Pascal, who designed and built the first (mechanical) calculator.

The lambda -calculus theory is about modelling systems which have no or little interactions with their environment. On the contrary, the pi-calculus theory developed by Robin Milner in the late 1980s is about modelling concurrent communicating systems. This theory also takes into account the notion of "mobility" which can either be physical or, as in the case of B2B, virtual (movement of links between systems). I think we can actually relate the mobility to the notion of "change": change of business partner, business document format, capabilities, etc – any modification of an existing relationship between two companies may be associated with mobility.

As a side note, pi-calculus is the foundation of two of the main Process Markup Languages: BPML from the BPMI consortium and XLANG (now BPEL4WS) from Microsoft, which we will study at the end of this chapter.

*At a high level, a company can be considered to be a very large automaton whose logical **state** consists of gigabytes or terabytes of data, and physical state is made of the raw materials, manufactured goods, people and money under its control. Its state is strictly bounded in the sense that it is owned and accessible in its entirety from the corporation, but hidden from any other corporation. A company can change its state by initiating an **action** (ship an order, pay a supplier, ...). When another corporation wants to change or query this state it is done via an **interaction.** Interactions usually trigger some internal actions based on business rules, which enable the corporation to ultimately be in a state which is consistent with the one of its business partners.*

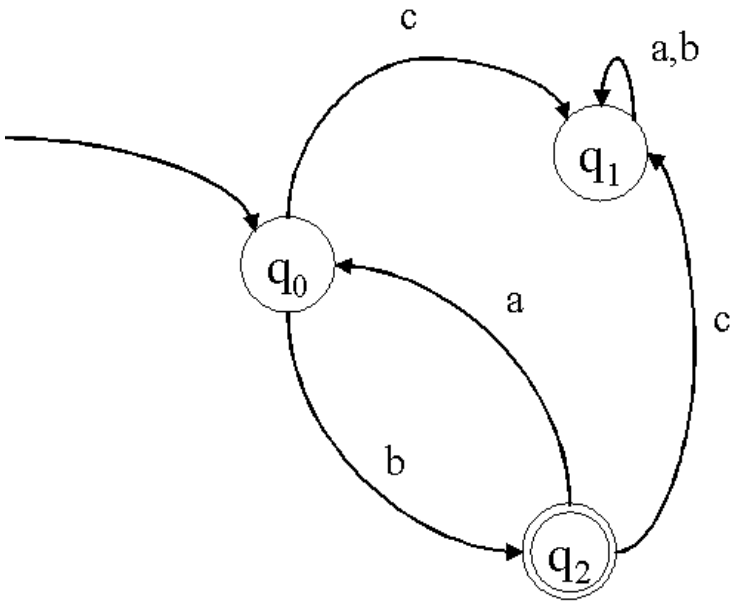
*The company's **actions**, when executed, transition from one state to another. Interactions and actions, when assembled together, form the enterprise business processes. Both the number of **actions** and **states** can be large for any given corporation. However, they are both finite.*

Let's look in more details at an automaton. The classical theory, as the starting point of Milner's theory, specifies that an automation over a set of actions ***Act*** *has four ingredients:*

- *A set of states* $\mathbf{Q} = \{q_0, q_1, \ldots\}$
- *A start state* q_0
- *A set of transitions which are triplets (q,a,q') members of* $\mathbf{Q \times Act \times Q}$
- *A subset* $\mathbf{F}$ *of* $\mathbf{Q}$ *called the accepting states*

In theory a business is deterministic, thus will obey the rule that for each pair of state and action (q,a) there is at most one transition (q,a,q').

An automaton can be represented with a directed graph as shown below. States are represented in circles ($q_0, q_{1\ldots}$*) transitions are represented as arrows (*$t = q_0$ *.c.* q_1 *) and accepting states are represented with a double circle:*



This model can be extended to introduce the notion of events and conditions, which may act as a ***guard*** *to an action. Actions may be automatic; when one reaches a state* q_i *an action "a" occurs without any other pre-conditions. In other cases, a "condition" may decide whether action "a" or "b" will happen, again automatically. Lastly, an event, sometimes combined with a condition, may trigger an action (Event Condition Action model), which in turn will transition the automaton from a state to another.*

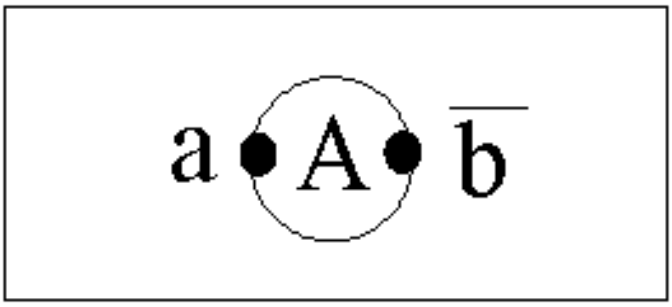
When the number of potential states is large this diagram becomes impractical and is often replaced by an activity diagram, just like the UML activity diagram. This diagram is drawn from a different perspective. It does not show the specific states the automaton may take but rather the

controlled succession of activities (that is, actions) that may occur within a corporation. State-transition or activity diagrams are often referred to as a processes or a sequential processes.

When two corporations are engaging in B2B activities, they are each running their (internal) sequential process concurrently. These two processes must interact to reflect commitments, transfer of economic resources, and many other aspects of the business activity shared between the two business partners.

This causes the actions of a given corporation to be divided into two different sets: those which are externally observable and those which are internal.

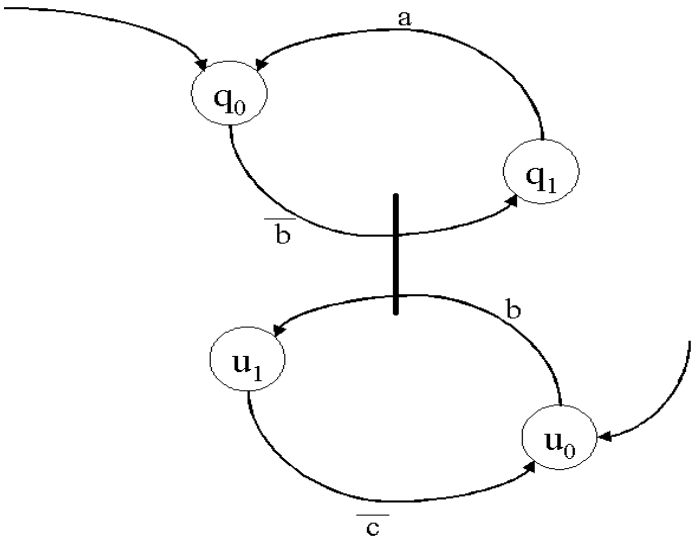
*At this point the automaton **A** (that is, the corporation) is considered as a black box and the externally observable actions can be represented with the following notation (in this case only two of them):*



a and b are called labeled ports. Each complementary pair (b, b) of ports represents a means of interaction between two automata. These are the points of synchronization between the automata.

This graph is called a flowgraph. While the transition graph depicts the dynamic properties of a system, a flowgraph depicts the structure of the system, in other words the relationships between its components. An automaton can have any number of labelled ports, and a port may bear any number of arcs directed to any number of automata.

If we look at a global picture we see that the two automata A and B are running with no particular dependence except that any action b from B must be synchronized with an action from B from A:



The synchronization is represented by a shared transition between their state-transition graphs. This notion of shared transition was first introduced by Carl-Adam Petri in his theory of Automata. The corresponding graphs have been known as Petri nets.

Let's draw some conclusions from this very short exposure to the p-calculus theory. First and foremost, there is no need to expose the details of the processes to model their interactions. It is enough to focus on the externally observable actions. Nothing prevents a corporation from exposing as much of its internal actions as it wishes (sometimes to obey regulatory requirements such as the ones in the aerospace or pharmaceutical industry, or yet to comply with standards such as ISO 9000), but it is completely separate from the specification of interactions. These internal actions do not become external once they are exposed, they remain internal since they are not part of the interaction. This is the ultimate goal: providing a shared view of the interactions regardless of the actions that lead to any particular interaction. Most companies consider their internal actions as their core assets and therefore are very reluctant to expose them.

Second, interactions are solely supported by the actions of the two concurrent automata involved. In particular, interactions do not require a third automaton which role would be to manage them, unless chosen by design (such as a broker, or a market place between buyers and suppliers in typical B2B topologies).

Last, a set of enterprise information systems can be viewed as a communicating and mobile automata. Inside a corporation, they can be aggregated to form a single logical automaton. Once we reach the boundary of a corporation, automata may no longer be composed since corporations do not share any state but rather synchronize their respective states when they communicate.

The pi-calculus theory is far more elaborate than what was presented in this section. Our goal here was to introduce a few concepts that will be helpful in building the big picture and position PMLs and ebXML together.

AUTHOR BIOGRAPHY

DR. KOFI NYAMEKYE is the president and chief executive officer of Integrated Activity-Based Simulation Research, Inc. Dr. Nyamekye has extensive prior experience as a senior research scientist in modeling and simulation of complex adaptive distributed enterprise systems for Boeing's Army Future Combat Systems (FCS). In collaboration with Dr. Vladimir Lefebvre who pioneered the Reflexive Game Theory, Dr. Nyamekye is currently using Reflexive Game Theory to model Cybersecurity risks and more importantly construct a socially-aware purposeful agent-based system (SAPABS) to mitigate Cybersecurity risks, in a Net-Centric Ecosystem (NCE). Using Experimental Laboratory for Investigating Collaboration, Information Sharing, and Trust (ELICIT) platform, he will then conduct experimental tests for information sharing and collaboration among the entities, for mitigating Cybersecurity risks, in NCE. Dr. Nyamekye has extensively published many refereed journals on the scientific design, multi-socially-aware purposeful agent-based modeling, and simulation of integrated and adaptive C4ISR SoS. He holds a Doctor of Philosophy degree in industrial and management systems engineering from Pennsylvania State University, a Master of Science degree in mechanical engineering from Pennsylvania State University, and a Bachelor of Science degree in mechanical engineering from the University of Wisconsin-Madison. Dr. Nyamekye is also an adjunct professor in Operations Management -- similar in concept to Command and Control (C2) which is organization and management of operations --, at Webster University. E-mail: kofinsoyameye@iabsri.net.

