

12-2013

A Social Dimensional Cyber Threat Model with Formal Concept Analysis and Fact-Proposition Inference

Anup Sharma

University of Nebraska at Omaha, asharma@unomaha.edu

Robin Gandhi

University of Nebraska at Omaha, rgandhi@unomaha.edu

Qiuming Zhu

University of Nebraska at Omaha, qzhu@unomaha.edu


William Mahoney

University of Nebraska at Omaha, wmahoney@unomaha.edu

William Sousan

University of Nebraska at Omaha, wsousan@gmav.unomaha.edu

Follow this and additional works at: <https://digitalcommons.unomaha.edu/compscifacpub>

 Part of the [Communication Technology and New Media Commons](#), and the [Computer Sciences Commons](#)

Recommended Citation

Sharma, Anup; Gandhi, Robin; Zhu, Qiuming; Mahoney, William; and Sousan, William, "A Social Dimensional Cyber Threat Model with Formal Concept Analysis and Fact-Proposition Inference" (2013). *Computer Science Faculty Publications*. 24.

<https://digitalcommons.unomaha.edu/compscifacpub/24>

This Article is brought to you for free and open access by the Department of Computer Science at DigitalCommons@UNO. It has been accepted for inclusion in Computer Science Faculty Publications by an authorized administrator of DigitalCommons@UNO. For more information, please contact unodigitalcommons@unomaha.edu.



A Social Dimensional Cyber Threat Model with Formal Concept Analysis and Fact-Proposition Inference

Anup Sharma, Robin Gandhi, Qiuming Zhu, William Mahoney, and William Sousan
College of Information Science and Technology
University of Nebraska at Omaha
{asharma, rgandhi, qzhu, wmahoney, wsousan}@unomaha.edu

Abstract - Cyberspace has increasingly become a medium to express outrage, conduct protests, take revenge, spread opinions, and stir up issues. Many cyber attacks can be linked to current and historic events in the social, political, economic, and cultural (SPEC) dimensions of human conflicts in the physical world. These SPEC factors are often the root cause of many cyber attacks. Understanding the relationships between past and current SPEC events and cyber attacks can help understand and better prepare people for impending cyber attacks. The focus of this paper is to analyze these attacks in social dimensions and build a threat model based on past and current social events. A reasoning technique based on a novel combination of Formal Concept Analysis (FCA) and hierarchical fact-proposition space (FPS) inference is applied to build the model.

Keywords — Cyber Threats; Attacks Models; Social Factors; Formal Concept Analysis; Fact-Proposition Space Inferences

1. INTRODUCTION

Cyber attacks have become a widespread global problem causing massive damage to Internet users, organizations, and information infrastructures. Current anomaly detection models focus primarily on analyzing network traffic to prevent malicious activities (Kuhl & Kistner, 2007, Liu et.al, 2008, Peng & Hong, 2007). Such approaches are proven to be inadequate since they fail to account for deviant human behaviors behind the anomalies. Meanwhile, evidence is growing that more cyber attacks are associated with current and historic events and factors in the social, political, economic, and cultural (SPEC) dimensions of the human world (Myers & Tan, 2003, Slay, 2003, Strategypage, 2008).

Social conflicts in human world have often arisen by groups or individuals over incompatible goals, scarce resources, or the sources of power needed to acquire them (Avruch, 2004). Cyberspace has become a new arena for “citizen warfare” in which individuals can express their personal or nationalistic sentiments and attack their “enemy” (Zubir, 2005). Similarly, the Internet has become a powerful instrument for making social and political statements through cyber activities, including hostile attacks (Stakhanova et.al, 2008). It is also known that the socio-technological status of the cyber attackers, their backgrounds and their motivations are essential factors in predicting, preventing and tracing cyber attacks in these dimensions (Markoff, 2008, Rasche et.al, 2007). Security experts and researchers have been trying to predict and preempt these attacks in order to reduce the damage. It’s difficult to come up with effective attack prevention and detection techniques without a full understanding of the adversaries’ behavior, their motives, goals, and the technological levels that influence their decisions to carry out an attack (Kshetri, 2006).

Continuous and timely assessment of cyber attack factors is critical in making plans and taking measures to help reduce the risk. Effective protection against attacks requires the knowledge and understanding of the attack characteristics, such as the attack agents, motives, means, and possible system vulnerabilities that maybe used by the attacker. Identifying such attack factors involved in the past cyber attack events helps in uncovering details of attack techniques, and allows for the development of defensive measures that could prevent similar attacks both now and in the future (Sharma, 2010). With a proper knowledge representation (Brachman, 1992) and reasoning techniques, it will be feasible to grasp the attack characteristics, for example, knowing how certain categories of attacks lead to specific consequences, and thus be able to select proper preventive strategies.

One of the goals of the research presented in this paper is to identify cyber attack patterns from a collection of events that have occurred in the past (Sharma 2010). The paper focuses on building a threat model by analyzing human intentions and means to carry out cyber attacks. The real world entities such as the attacker's motives, social events that triggered these attackers, attack targets etc., are all considered as components of the knowledge base for analyzing the potential correlations between historic and current SPEC events and cyber attacks. A Formal Concept Analysis (FCA) approach together with a Fact Proposition Space (FPS) inference mechanism is implemented in this research in an attempt to build a comprehensive threat model and provide a valuable insight toward the future attack characteristics.

There are several ongoing research efforts in academia, national labs, and industry involving security requirements, threats, attacks, and vulnerabilities. While most of the existing techniques to deter such attacks draw conclusions by analyzing network traffic and malicious activities, this paper focuses on building a threat model by analyzing human intentions and relevant factors to carry out cyber attacks. However, only social related cyber attacks were analyzed primarily in this paper (Sharma, 2010).

The rest of this paper is organized as follows: Section two reviews related work in cyber attack analysis. Section three discusses the methodology and the process used in this research, and illustrates our results. Finally, section four contains the conclusion and directions for future work.

2. BACKGROUND AND RELATED WORK

2.1 Cyber attacks resulting from physical world conflicts

Stakhanova et al. developed a conceptual model for explaining the evolution of ideologically motivated cyber attacks (Stakhanova et.al, 2008). Their work focused on understanding the nature of those attacks, their evolutions and factors influencing their emergence, aimed toward developing effective defense strategies against these types of threats. They adopted a sociological perspective for a conceptual model by analyzing the ideologically motivated attacks, and created methods to facilitate predictions and responses to the threats leading to such kind of attacks. The theoretical foundation behind their approach lays an explanation of collective behavior that occurs between people or a group of people sharing similar beliefs and attitudes in regard to a specific issue. Their conceptual model follows through three phrases: tension build up (the building up of emotional or physical tension among a large number of people), triggering factors (attack triggering mechanisms such as an event that suggests/justifies the release of the tension), and the attack (the actual collective behavior – a cyber attack).

A technical report (Cyber Attacks, 2001) published by the Institute for Security Technology Study at Dartmouth College examined several case studies of political conflicts that have led to attacks on cyber systems. Based on factual analysis, the report illustrated the cases of cyber attacks immediately accompanying physical attacks, revealed a close connection between conflict in the physical and cyber worlds, analyzed the vulnerability of critical infrastructure systems to cyber attacks and the increasing willingness of groups to target sensitive systems during political conflicts, and concluded that political conflicts between countries could be followed by an online campaign of mutual cyber attacks and web defacements.

2.2 Threat Assessment

Steinberg (2005) proposed an approach to threat assessment by characterizing, predicting, and recognizing threat situations. The attack hypotheses were adaptively generated, evaluated, and refined as the understanding of the situations evolved. The proposed approach was built upon the advances in situation, ontology, and estimation theory. Relationships that were inferred and exploited in situation assessment include the logical/semantic relationships (such as taxonomic), physical relationships (such as spatiotemporal), functional relationship (such as organizational role), etc. These relationships were inferred from observed attributes of entities and their context threats were then modeled in terms of potential and actualized relationship between threatening entities (such as people) and threatened entities or targets. Indicators of threat situations relate to capability, opportunity, and intent of agents to carry out attack against various targets. The threat assessment process would then generate, evaluate and select hypotheses concerning threat situation, i.e., threat situations in which threat events (attacks) were likely in terms of entities' capability, opportunity and intent to carry out various attacks. By evaluating and selecting

hypotheses, a Threat Assessment System would provide indications, warnings, and characterizations of possible, imminent or occurring attacks.

2.3 Conceptual learning with Formal Concept Analysis

Cimiano et al. (2005) proposed a model to learn concept hierarchy from text corpora. In order to derive attributes from certain text corpus, verb/prepositional phrase, verb/object, and verb/subject dependencies were parsed and extracted first. Then for each noun appearing as head of these argument positions, the corresponding verbs were used as attributes for building the formal context. A formal concept lattice was calculated on this basis. The learned concept hierarchy was compared in terms of similarity with handcrafted reference taxonomies. Further, the impact of using different information measures to weight the significance of a given object/attribute pair was examined.

Zhao and Halang proposed a method based on rough set and concept lattice to conduct ontology mapping (2006). In their approach, a reference concept lattice is first constructed with the use of a combination of two normalized contexts. Rough set theory is then employed to calculate the similarity measure of the two ontology nodes. The approach combines rough set theory and concept lattice theory to measure the concept nodes from two ontologies based on Tversky's similarity model. The use of an overlap coefficient to obtain similarity measure has also been used in the works of Liakata and Pulman (2008) and Bhagat et al. (2007).

2.4 Inference generation with Fact Proposition Space

Hospodka (2008) used Fact Proposition Space Inference to provide a valuable information fusion and belief integration engine. In his original work, a through prototype implementation of the system is made to demonstrate the capabilities and advantages of the hierarchical fact-proposition space model in risk assessment, consumer purchasing assistance, medical diagnostics, and other similar tasks. The approach used in this paper extends on this Fact Proposition Space Inference technique in a way that the belief value needed to make inference is generated from factual analysis with formal concept analysis and overlap coefficients computation.

A Fact Proposition Space (FPS) is an inference mechanism based on probability theory (Zhu, 1994). The mathematical foundations of the FPS model are Bayes' theorem and propositional logics. According to Bayes' rule, the conditional probability of some event A occurring, given the occurrence of some other event B, is defined as $P(A|B)$, and is read as "the Probability of event A given event B." In FPS model, there are two sets of information that are essential to the reasoning process, the fact set and the proposition set. Let $F = \{f_i \mid i = 1..n\}$, $n \geq 1$, be used to represent the fact set. Each element of F is a component of the evidence provided. It contains two parts: a semantic part denoted by $S(f_i)$ and a value part denoted by $V(f_i)$. The semantic part is natural language meaning of the fact and the value part can be a real number in the range from 0 to 1 to represent the belief value of the fact. Let $P = \{p^j \mid j = 1..m\}$, $m \geq 1$, be used to represent the proposition set. Each element of P contains two parts: a semantic part denoted by $S(p^j)$, and a value part denoted by $V(p^j)$. The semantic part is a natural language meaning of the proposition and the value part can be a real number in the range from 0 to 1 to represent the belief value of proposition. The FPS is a Cartesian product of the F and P sets in two-dimensional space $E^{N \times M}$, where N and M are the cardinalities of the sets F and P. Each element E_i^j represent a node of the space $E^{N \times M}$, where each node has a functional form that describes the evaluation mechanism to be performed in this field.

An FPS representation can be regarded as a matrix where facts and evidence are influencing propositions to a question. Each column of the matrix represents some facts. Each row represents some proposition or a proposed answer to a question. A node E_i^j represents how much belief that if the fact or evidence is true towards how much do we believe the proposed answer to be true. In probabilistic reasoning, the reasoning process will generate a continual belief value that quantifies the truth attached to the propositions P_j in the range of 0..1. In the FPS, the functional form E_i^j is denoted by $E_i^j(F)$. In Bayesian reasoning, the E_i^j represents the conditional probability. The value is used to denote an association between the fact and the expected evidence.

A hierarchical structure of FPS can be easily realized, and is beneficial in the way that it sub-divides a multi-level, multi-variant decision problem into a number of hierarchically organized FPS. In a hierarchical FPS, there are multiple fact sets and proposition sets. Some subset of facts could be related to one subset of propositions while another subset of facts could be related to another subset of propositions. The FPS handles the hierarchical structure by using a computation formula to get the highest belief among the proposed answers to the question, level by level.

The selected/proposed answer at a lower level is used as evidence, or a factual statement, for the next level within the hierarchy that the node influences. With the same computational steps happening at each element and each level of the hierarchy, this hierarchical FPS model is simple and regulated for its easy adaptation in reasoning process applications.

3. METHODOLOGY AND PROCESS

The methodology followed in this research is based on a predictive knowledge representation and integrated reasoning approach. The cyber threat model is built by analyzing, evaluating, and processing historic and current cases of cyber attacks. We focus only on those that are triggered by social events. These events are collected from various sources, mostly open-source intelligence, in order to construct a comprehensive knowledge base for reasoning. The knowledge base is in turn used for an assessment of the cyber attack threat through the Formal Concept Analysis and the Fact Proposition Space inference mechanism (Sharma, 2010). We consider three important aspects of knowledge representation and reasoning in our approach, and divide the research into three phases:

1. Knowledge acquisition in Cyber attack domain from news and public domain text corpus.
2. Knowledge representation using Formal Concept Analysis (FCA).
3. Knowledge Inference and belief value generation using Fact Proposition Space (FPS).

3.1 Knowledge Acquisition in Cyber Attack domain

In this phase, past and current cases of news articles and descriptive accounts of cyber attacks that are fueled by social disturbances or conflicts are collected from various resources. These cases and news reports are extracted by continuously monitoring open-source resources such as online news and articles, books, scholarly journals, and technical papers. Once a news report or article is acquired, the content of the articles is annotated with various factors that are part of an elaborative cyber attack domain model, as shown in Fig. 1 below.

The cyber attack domain model consists of following factors:

- **Social Motive:** the motivation of the attacker or attack agents to commit a cyber attack with respect to the occurrence of social events.
- **Attack Agents:** human or group of humans with a motivation to carry out a cyber attack.
- **Means:** methods and techniques used by attacker or attack agents to attack.
- **Technological Aspects:** how certain means are carried out or what technologies are used to carry out certain cyber attack.
- **Victims:** human, organizations or governments that are affected by cyber attacks.
- **Consequences:** the final outcome and damage as a result of a cyber attack.

The cyber attack domain model is a semantic network used to represent the relationships between different factors and to link attributes to these factors. The categories identified under each factor in the above domain model are based on our current corpus of articles that describe cyber attack events (CyCast, 2011).

Understanding and listing all possible social motives is a challenge. To elaborate on social motives, a social event must be defined. For this purpose, a two-pronged approach is taken. First, multiple open source information and dictionary definitions of the word “social” are consulted. This effort resulted in a thorough coverage of interpretations for the word “social” as shown in Fig. 2a. This effort allowed identifying distinct categories of social events relevant to an understanding of cyber attacks. Fig. 2b. shows a partial view of the current taxonomy of social events. This taxonomy is by no means complete, and is subject to continuous refinement and adjustment based on community input. However, the taxonomy does cover the cyber attack cases currently in our corpus, which are listed in the appendix of this paper, where words and phrases that relate to the factors mentioned in Fig. 1 are tagged and shown in red color. The characteristics of a few selected examples of these cases are represented in a tabular format (Table 1) to show how various factors are identified.

Based on the selected example, we identified a set of elements representing the social motives, attack agents, means, technological aspects, and consequences in these social relevant cyber attacks. The elements include:

(1) Social Motives:

- Protest controversial events
- Protest unpopular commemorative days/events or anniversaries
- Protest human rights abuse
- Protest information censorship/web filtering
- Protest events and policies on Environment degradation

(2) Attack Agents:

- Vandals/Hackers
- Cyber Mercenary
- Nation/States
- “Hacktivists”

(3) Means:

- Web Defacement
- Stealing information
- Sabotage/Subversion
- Malware (Malicious code)
- Penetration attempt

(4) Technological Aspects:

- SQL and code injection
- Intrusion into secure system
- Time bombs
- Trojans
- Botnets
- Exhaustion of computer resource leading to denial of service

(5) Victims:

- Government
- Social Community
- Individuals/Civilians
- Businesses/Commercial Organizations
- Critical Infrastructure

(6) Consequences:

- Damage of computational resources
- Disruption of Service
- Unauthorized modification and fabrication of information
- Information/Data Loss

Note that these elements are extracted from the use cases of our collected corpus only.

3.2 *Knowledge Representation with Formal Concept Analysis (FCA)*

The knowledge representation with the use of Formal Concept Analysis provides us the ability to see various hierarchical structures as well as the clusters of related concepts (Puerta et.al, 1994).

Formal Concept Analysis (FCA) is a method for formal representation of conceptual knowledge. It is often used for analysis of implicit relationships between objects described through a set of attributes (Ganter, 1999). There are three levels of analysis in terms of which methods of formal representation. The first level is a basic data context that consists of a binary relation between objects and attributes. The second level explains conceptual relationships for data matrices, and the third level allows a study of the representation, inference, and communication of conceptual knowledge mathematically (Wille, 1997).

Data in a FCA is represented in a basic data type, called a Formal Context, expressed as a triple $K = (G, M, I)$, where G is a set of objects, M is a set of attributes, and $I \subset (G \times M)$ is a binary relation between the sets of objects and the sets of attributes (Wille, 1997). The formal context is usually represented by a cross table. The elements on the left side are formal objects; the elements at the top are formal attributes; and the relation between them is represented by the crosses (Table 2). Within a formal context, a formal concept c is defined as an ordered pair (A, B) such that:

$$A = \{g \in G \mid \forall m \in B: (g, m) \in I\}$$

$$B = \{m \in M \mid \forall g \in A: (g, m) \in I\}$$

where A is called the *extent* ($Ext(c)$) of the concept c and B is said to be its *intent* ($Int(c)$). A formal concept (A, B) is a *subconcept* of a formal concept (C, D) , if the extent A is a subset of the extent of C or if the intent of B is a superset of the intent of D . Their relation is shown as $(A, B) \leq (C, D)$. A partially ordered set of all formal concepts is always a complete lattice structure and is called a *concept lattice*.

From the formal context, a concept lattice can be drawn. This concept lattice consists of the set of concepts and the relationships between them. Each node in the lattice, as shown in Fig. 3, is a formal concept. The bottom-half of a node is colored blue if the node owns an object; similarly the top-half of the node is colored blue if it owns an attribute. The default color is white. Formal objects are shown slightly below the formal concept whereas formal attributes are shown slightly above the formal concept. Each concept in the lattice represents a maximal sub-grouping of objects (concept extent) with shared attributes (concept intent). The lattice captures the partial order among all such concepts. Such representations support both automatic inference and user-guided discovery and exploration of hypotheses.

The lattice in Fig. 3 is annotated in a concise way to determine the intent and the extent of the formal concepts as follows: (1) all attributes encountered by navigating upward from a given formal concept are associated with that formal concept; and (2) the objects encountered navigating downward from a given formal concept are all associated with that formal concept. For example, in Fig. 3, the formal concept annotated with “Object5” includes “Attribute1,” “Attribute2,” “Attribute3,” as well as “Attribute5” in its intent. Similarly, by navigating downwards from “Object 5”, we determine that it includes only “Object 5” in its extent. The path obtained by navigating upward from a concept is called the “filter” and the path navigating downward is called the “ideal”.

Table 3 shows the Formal context table of the example use cases studied in this paper, with cyber attack news articles as objects and cyber attack factors as attributes. In the next step, all the objects (i.e. cyber attack news articles) that have the same attribute (social motive) are grouped together. The result of this grouping allows building a new formal context representation. As an illustrative example, the cause-and-effect relations from the “motives” to its corresponding “attributes” are shown in Table 4.

3.3 Knowledge Inference

The concept lattice is very useful in deriving inferences from knowledge represented in formal contexts (Sowa, 2000). Both qualitative and quantitative inferences can be performed on the lattice. In this section, two important inference mechanisms, mainly qualitative and quantitative inferences are performed from an interpretation of the lattice. With qualitative inference, characteristics and relationships among objects and attributes are discovered. Quantitative inference from the concept lattice provides approximate belief values to be used in a Fact Proposition Space model for socially motivated cyber attack threat assessment.

3.3.1 Qualitative Inference

In the concept lattice diagram of Fig. 4 each node is a formal concept. An object can only fall under the concept if it has all the attributes of that concept. For example, looking at the formal concept labeled with the object (“M1: Protest Controversial Events”), the attributes (“Hacktivists, Business and Commercial organizations, Disruption of service, Exhaustion of computer resources, and Penetration attempt”) identified by navigating above are all those associated with that object. It can be inferred from the selected formal concept that the (object) social motive of “Protest controversial events” is relevant to the following attributes: attack agents are “Hacktivists”, attack means is “Penetration attempt”, technological aspect in carrying out the means is “exhaustion of computer resource leading to denial of service”, victims are “business and commercial organizations”, and finally the consequence of the attack is “disruption of service”. This inference is predictive of the recent cyber attacks related to Wikileaks (Mackey, 2011).

Similarly, in Fig. 5, if we select the formal concept labeled with the attribute “Hacktivists”, the objects (M1, M2, M3, and M4) identified by navigating below all share the attribute. The inference that is derived from the selected formal concept in Fig. 5 is: one of the possible attack agents is “Hacktivists” when social motives are either “Protest controversial events,” “Protest human rights abuse,” “Protest information censorship and web filtering,” or “Protest policies having negative impact on environment.” FCA allows us to make systematic inferences and to derive coherent explanations for cyber attacks in terms of their social dimensional factors.

3.3.2 Quantitative Inference

The concept lattice can be investigated with algebraic methods to unravel its structure (Ganter, 1999). For our work, quantitative inference derives an approximate belief value in the range from 0 to 1, calculated using overlap coefficient. To obtain an approximate belief value, first the overlap coefficients for all the objects/attributes relationships are calculated. These overlapping coefficients are then used as probabilities for a formal object occurring with a formal attribute.

An overlapping coefficient is a similarity measure that computes the overlaps between two binary vectors (Manning & Schütze, 1999). The overlap coefficient between set A and B is defined as:

$$\text{Overlap Coefficient } (A, B) = \frac{|A \cap B|}{\min(|A|, |B|)}$$

To calculate the overlap coefficient, objects and attributes are mapped with respect to the cyber attack domain model shown in Fig. 1. From the cyber attack domain model, it is clear that “Attack Agents” are triggered by “Social Motive.” A corresponding formal context table for “Social Motive” as objects and “Attack Agents” as attributes is represented in Table 5.

In calculating the overlap coefficient, we consider objects and attributes as two individual sets. For example, the set “Social Motive” contains elements of “Protest controversial events,” “Protest unpopular commemorative events or anniversary,” “Protest human rights abuse,” etc. Similarly, the set of “Attack Agents” contains the elements of “Vandals/Hackers,” “Nation/States,” and “Hacktivists.” The overlap coefficients between the object set “Social Motive” and the attribute set “Attack Agents” are obtained by a two-step process. First, a formal concept node representing the object is selected, for example, the “Social Motive” M1: Protest controversial events, as shown in Fig. 6a. Second, a formal concept representing an attribute is selected, for example, the “Attack Agents” A1: Vandals/Hackers, as shown in Fig. 6b. All the nodes below the selected node are the element of the object “Social Motives”. From the Figure, it is clear that there is no overlap between the object “M1” and the attribute “A1”, so the overlap coefficient is 0. This means that in the past we have not observed any event where “M1” and “A1” co-occur. Similarly, the formal concept node representing the object (“Social Motive” “M3: Protest human rights abuse”) has two nodes as its elements (Fig. 7a.). The formal concept node representing the attribute “A3: Hacktivists” (Fig. 7b) has two nodes as its elements. In this case, the overlap coefficient is 1. This means that “M1” and “A1” have co-occurred in all the past events. In the same manner, overlap coefficients for all the object and attribute combinations of these specific cases are calculated, and the results are shown in Tables 6, 7, 8, and Fig. 8, respectively. Table 9, Fig. 9, and Table 10 show the formal context, concept lattice and overlap coefficient for the “Means” as objects and “Victims” and “Technological Aspects” as attributes, respectively.

After the calculation of overlap coefficients for each of objects/attributes relationships, our next step is to generate corresponding belief values. This is done by taking the average of the calculated overlap coefficients and representing them in the range from 0 to 1 based on their numerical value. The belief value represents the strength of relationships between objects and attributes.

3.3.3 Inference with Fact Proposition Space (FPS) model

To generate inference using the Fact Proposition Space model (Zhu, 1994), a decision tree/graph is constructed, as shown in Fig. 10, based on the cyber attack domain model of Fig.1. The root node in the graph is called focal point; from this point the rest of the graph is started. In Fig. 10, all arrows point in a direction leading to the parent. This shows the direction of influence that one node has on another node. Each node in the tree represents a topic that is seeking an answer to its questions, or a belief in what is true about the topic. Every child node represents the topic

that needs to be resolved before their parent node can be resolved. Since the child node is a topic that influences its parent node, so the proposition of the child node topic influences the parent's node propositions.

In Fig. 10, the focal point is the "Consequences" of cyber attacks given that there is a social conflict or disruption in social dimensions. The propositions for the "Consequences" of cyber attacks are:

- Damage of computational resources
- Disruption of Service
- Unauthorized modification and fabrication of information
- Information/Data Loss

From the focal point, input is broken down into three major influencing subtopics:

- Victims,
- Means, and
- Technological Aspects

These three are the sources of information, which would influence the consequences of cyber attacks. Since the decision tree is a graph and is based on cyber attack domain model, subtopics reappear as a source of information for multiple parent topics. The leaf node for each subtopic is "Social Motives" which are derived from the use cases as listed in the appendix:

- Protest controversial events
- Protest unpopular commemorative days, events, or anniversary
- Protest human rights abuse
- Protest information censorship/ web filtering
- Protest Policies having negative impact on environment

The next step is to create a scenario of a "Cyber Attack Threat" in the Fact Proposition Web Application (Hospodka, 2008) based on the decision tree. This scenario provides a means to find out the consequences of cyber attacks, given occurrences of specific social events. A cyber attack threat hierarchy is created adding nodes/topics based on the decision tree. Fig. 11 illustrates, as an example, the probability propagations (through a table of calculation) at an intermediate step of the inference hierarchy for the "Threat Model" in the FPS application. Note that the page has different layout designs and settings at different levels and stages of the inference process. In the figure, each leaf node is a fact (i.e. "Social Motives"). P1, P2, P3 are propositions of "Attack Agents".

- P1: Vandals/Hackers
- P2: Nations / States
- P3: Hacktivists

Level 1, Level 2, and Level 3 represent how much effect a particular fact has on proposition (i.e. how likely the fact affects the propositions). In the figure,

- Level 1: Low
- Level 2: Medium
- Level 3: High

For example, given the condition that a fact of "Social Motives" (as an "object") appears at a level 3 ("High"), which translates to a high probability value, say at 0.75, and the conditional probabilities that the "Attack Agents" being "Vandals/Hackers," "Nations/States," and "Hacktivists" is at 0.025, 0.025, and 0.9 under the given condition, as shown in Fig. 11, the probability that an attack could take place by the corresponding "Attack Agents" will be 0.019, 0.019, and 0.68 respectively. This means that under the given situation, a cyber attack is more likely to be launched by the hecktivists. An overall risk/threat factor of an information system or a web service potentially to be under attack by the "Vandals/Hackers" or "Nations/States" or "Hacktivists" with respect to an occurring event can be calculated by accumulating these components with respect to the factors such as the "means" and "Technological Aspect" all together.

Values in the matrix are calculated in a way as described in section 3.3.2 on Quantitative Inference. A level up from “Social Motives” in the hierarchy tree is the node “Attack Agents”. A level up from the node “Attack Agents” in the hierarchy tree is the node “Means”. The highest-level node is “Consequences.” After all the leaf node propositions have been filled, a factor is selected as shown in Fig. 12. The factor selector interface helps selecting propositions that is true for each and every leaf node.

When the application is executed, it is possible to see the belief values at each level and each node in the hierarchy. The inference process determines which proposition to select at each node, and propagates belief values up the tree to get the final result at the focal point. An example is shown in Fig.13 for the probabilistic computation of the “consequences” which is at the top level of the inference. Note that the web page contents and layout design is different from the one shown in Fig. 11 which shows a screen layout for an intermediate step of the inference process. Here a user can navigate through the hierarchy to see which proposition was selected, as well as where and at which belief value it was chosen.

What makes the Fact Proposition Space (FPS) model and the FPS web application efficient is its ability to predict the consequences of cyber attacks for real world cases of social events and conflicts. During the final draft of this paper (December of 2010), recent news included “The Publication of Government’s Secret Information by WikiLeaks”. In the following paragraph, the FPS model simulates the consequences given this news about “WikiLeaks”. The result below shows the inferences derived from the cyber event “WikiLeaks” and generalizes the attack characteristics, where the news about “WikiLeaks” relates to social motive “Protesting of Controversial and Unpopular Events”. As a result, in the web application the factors for “Protest Controversial Events” and “Protest Unpopular Events” are selected as “Level 3” (high) and other factors as Level 1 (low), as shown in the Fig. 14.

After the factors have been selected, the application is executed. The final result is shown in the Fig. 15. The figure shows that a different result is obtained in comparison to the one shown in Fig. 11. The example illustrates that the inference engine reacts properly and sensitively corresponding to different event inputs with different characteristic settings of the initial states. The result shows that the belief value is highest (0.504) for proposition description “Information and Data Loss” in the node “Consequences”. Similarly, we can find that the highest belief value for the “Victims” is the proposition description for “Individuals/Civilians,” which is at 0.483. The highest belief value for the “Means” is 0.276, which is “Penetration Attempt” This indicates that the means of attack used by supporters of “WikiLeaks” is predicted to primarily consist of “Penetration Attempt.” Similarly, the highest value for “Technological Aspects” is 0.398 for “SQL and Code Injection.” In this way, the FPS model generalizes and makes inferences about cyber attacks for real world events that may lead to cyber attacks. Though the accuracy of these predictions remains to be seen on a larger set of real world events, operation payback (Horn, 2010) launched by “WikiLeaks” supporters on companies such as PayPal, Mastercard and Visa for restricting donations to the site provides a strong alignment with our findings.

4 CONCLUSION

The use cases of physical world SPEC event triggered cyber attacks are on the rise. While most of the existing techniques to deter such attacks draw conclusions by analyzing network traffic and malicious activities, the research described in this paper focuses on building a threat model by analyzing previous and current cyber attacks. The threat model proposed in this paper is based on a formal knowledge representation and reasoning method. A Formal Concept Analysis (FCA) approach and a Fact Proposition Space (FPS) inference technique are implemented in multiple steps towards building a comprehensive threat model. The two approaches make the core of the formal knowledge representation and reasoning system. The following paragraph summarizes the entire process.

A knowledge base is created by continuously collecting news, articles, technical reports, and scholarly papers on real cases of cyber attacks fueled by social disputes. A semantic model in cyber attack domain is built in order to identify different factors that are associated with the attacks. Content of the news articles are annotated with various factors. Such annotation allows parameterization of the rich information expressed in news articles. Formal Concept Analysis (FCA) is used to conceptually represent the information. While FCA has been used in the past to analyze

data, and for investigating and processing given information, it hasn't been used for the analysis of cyber attacks. The use of FCA for analyzing cyber attacks in terms of objects/attributes relationships makes this research unique.

Two important aspects of FCA – the formal context and the concept lattice are used to make systematic inferences and derive coherent explanations for cyber attacks in terms of their social motivations and factors such as attack agents, attack means, technological aspects, attack victims, and attack consequences. Further, approximate belief values are generated by deriving overlap coefficients from objects/attributes relationships. This belief value acts as an input in the Fact Proposition Space inference. To generate inference using the Fact Proposition Space model, a decision tree/graph is built in the Fact Proposition Space – a Web Application - using the cyber attack domain model. Executing the FPS application allows model cyber attack threat assessment. Thus deriving systematic inferences of cyber attacks threat relationships with FCA and processing output from FCA with fact proposition inference engine allows building a comprehensive cyber attack threat model.

Our current research is only exploratory. Most of the cyber attack factors and attributes identified and represented in this paper are related to social dimension only. There are a number of limitations of the approach implemented in this research.

1. First, the categories identified under each factor in cyber attack domain are based on the current corpus only. As the corpus grows, new categories can be derived.
2. Similarly, the taxonomy of social motives is subject to continuous refinement and adjustment based on community input.
3. The overlap coefficient and the belief values are derived on the basis of formal context and concept lattice. As more cases of cyber attack cases news articles are analyzed, these values may change to reflect the nature of cyber attack threats.
4. The unreliability, incompleteness and richness of expression in vast amounts of unstructured text make prediction of cyber attacks a difficult problem.
5. Finally, the scalability of FCA to large contexts is a problem. However, by producing a bounded context that includes only the most closely associated news articles (from a large knowledge base) to a given article under investigation, the computational performance can be managed for most practical tasks.

Though major concepts addressed in this paper focus on cyber attacks threat triggered by social motives, similar concepts can be applied to build a threat model related to the political, cultural, or economic dimensions (Sharma, 2010). Implementation of the methodology used in this paper to build a threat model for other motivations would make the research more significant.

ACKNOWLEDGMENT

This research is partially funded by Department of Defense (DoD)/Air Force Office of Scientific Research (AFOSR), NSF Award Number FA9550-07-1-0499, under the title "High Assurance Software,"

To build concept lattice and compute associations, we have used the "Concept Explorer"(ConExp1.3) tool that implements the basic functionality needed for the study and research of Formal Concept Analysis (FCA). Concept explorer uses Duquenne-Guigues base and Luxenburger base rules to compute association.

REFERENCES

- Avruch, K., "Cross-Cultural Conflict," *Conflict Resolution, Encyclopedia of Life Support Systems (EOLSS)*, Eolss Publishers, Oxford ,UK, 2004.
- Bhagat, R., Pantel, P., and Hovy, E., "LEDIR: An Unsupervised Algorithm for Learning Directionality of Inference Rules," *Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning*, 2007, pp161-170.
- Brachman, R. J., and Levesque, H. J., *Knowledge representation and reasoning*, MIT Press, 1992.
- Cimiano, P., Hotho, A., and Staab, S., "Learning Concept Hierarchies from Text Corpora using Formal Concept Analysis," *Journal of Artificial Intelligence Research*, 24, 2005, pp. 305-339.

- Cyber Attacks, "Cyber Attacks during War on Terrorism: A Predictive Analysis," *Institute for Security Technology Studies*, Dartmouth College, 2001.
- CyCast, URL: <http://kewi.unomaha.edu/cycast/cybereventsdb.html#page1>, Last Accessed: 3/7/2011.
- Ganter, B., "Attribute exploration with background knowledge," *Theoretical Computer Science*, Volume 217, Issue 2, 1999, pp215-233
- Horn, L., "WikiLeaks Supporter 'Operation Payback'", URL: <http://www.pcmag.com/article2/0,2817,2374090,00.asp>, Last Accessed: 4/10/2011.
- Hospodka, P., "Bayesian Reasoning in a Fact Proposition Space," *Masters Thesis*, University of Nebraska at Omaha, 2008.
- Kshetri, N., "The simple economics of cybercrimes," *IEEE Security and Privacy*, 2006, pp. 33-39.
- Kuhl, M. E., and Kistner, J. et al., "Cyber attack modeling and simulation for network security analysis," *Winter Simulation Conference*, 2007, pp1180–1188.
- Liakata, M., and Pulman, S., "Automatic Fine-Grained Semantic Classification for Domain Adaptation," *Proceedings of the 2008 Conference on Semantics in Text Processing*, 2008.
- Liu, Z., Wang, C., and Chen, S., "Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern Modeling," *International Conference on Information Security and Assurance*, 2008, pp214–219.
- Mackey, R. "'Operation Payback' Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks," URL: <http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks>, Last Accessed: 1/31/ 2011,.
- Manning, C. D. and Schütze, H., *Foundations of Statistical Natural Language Processing*, The MIT Press, Cambridge, MA. 1999.
- Markoff, J., "Internet attacks seen as more potent and complex," URL: <http://www.iht.com/articles/2008/11/10/technology/10attacks.php>, Last Accessed: 3/7/2011.
- Myers, M., and Tan, F., "Beyond Models of National Culture in Information Systems Research," *Advanced Topics in Global Information Management*, Chapter 1, pp14-29, 2003.
- Peng, X., and Hong Z., "A Framework of Attacker Centric Cyber Attack Behavior Analysis," *IEEE International Conference on Communications*, 2007, pp. 1449–1454.
- Puerta, A. R., Neches, R., Eriksson H., Szekely, P., Luo, P., Mark A. Musen, M.A., "Toward Ontology-Based Frameworks for Knowledge-Acquisition Tools," *Knowledge Systems Laboratory*, Stanford University, USC/Information Sciences Institute, 1994.
- Rasche, G., Allwein, E., Moore, M., and Abbott, B., "Model-Based Cyber Security," *14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems*, 2007, pp 405–412.
- Sharma, A., Gandhi, R., Mahoney, W., Sousan, W., Zhu, Q., "Building a Social Dimensional Threat Model from Current and Historic Events of Cyber Attacks," *Proceedings of the International Symposium on Secure Computing (SecureCom-10) In conjunction with The Second IEEE International Conference on Privacy, Security, Risk and Trust*, Session B22, Minneapolis, MN, August 2010.
- Sharma, A., "Building a Social Dimensional Cyber Attack Threat Model with Formal Concept Analysis and Fact Proposition Space Inference," *Masters Thesis*, University of Nebraska at Omaha, 2010.
- Slay, J., "IS security, trust and culture: a theoretical framework for managing IS security in multicultural settings," *Journal Campus-Wide Information Systems*, Volume 20, Number 3, 2003, pp. 98-104.
- Sowa, J. F., *Knowledge Representation: Logical, Philosophical, and Computational Foundations*, Brooks Cole Publishing Co., Pacific Grove, CA, 2000.
- Stakhanova, N., and Ghorbani, A., "A Behavioral Model of Ideologically-motivated 'Snowball' Attacks," *Third International Conference on Availability, Reliability and Security*, 2008, pp. 88-95.
- Steinberg, A. N., "An Approach to Threat Assessment," *7th International Conference on Information Fusion (FUSION)*, 2005, pp. 1256-1263.
- Strategypage.com, "Information Warfare Article Index: Cyber War as the Ultimate Weapon," URL: <http://www.strategypage.com/htm/w/htiw/articles/20080105.aspx>, Last Accessed: 3/7/2011,.
- Wille, R., "Conceptual graphs and formal concept analysis, Conceptual Structures: Fulfilling Peirce's dream," *Fifth International Conference on Conceptual Structures*, 1997, pp. 293-303.

- Zhao, Y., and Halang, W., "Rough Concept Lattice based Ontology Similarity Measure," *Proceedings of the First International Conference on Scalable Information Systems*, 2006
- Zhu, Q., "Probabilistic reasoning in an augmented fact-proposition space and its applications," *Engineering Applications of Artificial Intelligence*, Volume 7, Issue 6, 1994, pp. 627-637.
- Zubir, M. "Exchange of 'cyber-fire' during the Malaysia-Indonesia Ambalat Dispute: a lesson for the future," *Centre for Maritime Security and Diplomacy*, MIMA, 2005.

Figure Captions

- Fig. 1. Cyber Attack domain model
- Fig. 2a. Dictionary Interpretations of the Word “Social”
- Fig. 2b. A Partial Taxonomy of Social Events
- Fig. 3. Concept Lattice of the Formal Context
- Fig. 4. Concept lattice with social motive “M1: Protest Controversial events” as a selected formal concept, with concepts in its intent highlighted
- Fig. 5. Concept lattice with attack agents “A3: Hacktivists” as a selected formal concept, with concepts in its intent highlighted
- Fig. 6a. A formal concept node representing the object selected
- Fig. 6b. A formal concept node representing an attribute selected
- Fig. 7a. A formal concept node representing the object selected
- Fig. 7b. A formal concept node representing the attribute selected
- Fig. 8. Concept lattice with “Attack Agents” as objects and “Means, Victims, and Technological Aspects” as attributes
- Fig. 9. Concept lattice with “Means” as objects and “Victims, and Technological Aspects” as attributes
- Fig. 10. Decision tree in a cyber attack domain model
- Fig. 11. A hierarchical structure of a Threat Model
- Fig. 12. Factor selection in FPS web application
- Fig. 13. Graphical display of result the propositions probability of consequences
- Fig. 14. Factor selected as Level 3 (High) and Level 1 (Low) for social motives
- Fig. 15 Final Results Display showing the consequences for the news about “WikiLeaks”

Table Captions

- Table 1. Mapping words and phrases that infer to the factors of cyber attack domain model
- Table 2. Formal Context Table
- Table 3: Formal context table with cyber attack news articles as objects and cyber attack factors as attributes
- Table 4. Formal context table with social motive as objects and other factors as attributes
- Table 5. Formal context with “Social Motive” as objects and “Attack Agents” as attributes
- Table 6. Overlap coefficients for “Social Motive” as objects and “Attack Agents” as attributes
- Table 7. Formal Context with “Attack Agents” as objects and “Means, Victims, and Technological Aspects” as attributes
- Table 8. Overlap coefficients for “Attack Agents” as objects and “Means, Victims, and Technological Aspects” as attributes
- Table 9. Formal Context with “Means” as objects and “Victims, and Technological Aspects” as attributes
- Table 10. Overlap coefficients for “Means” as objects and “Victims, and Technological Aspects” as attributes

Appendix: Major Cyber attack news articles and reports used in this paper.

1. Web attack against French Government websites, France, 12/1995

"A group called the "Strano Network" launched an hour long Net strike attack against government web sites to protest French Government nuclear and social policy. Attack organizers encouraged protesters to point their browser at the government website, which generated a high volume of web traffic and rendering it unavailable for other users."

Source: Arquilla John, Ronfeldt David, "Networks and Netwars: the future of terror, crime, and militancy", Rand, 2001.

2. Website of DOJ attack, USA, 1996

"When the Communications Decency Act was passed several protestors were involved in deleting the contents on the U.S. DOJ (United States Department of Justice)"

Source: Cross, Michael, Scene of the Cybercrime, Syngress Publication, 2008, 443-450

3. Attack on atomic research center, India, 5/1998

"Hackers from the United States, England, the Netherlands, and New Zealand (calling themselves "Milworm") attacked the website of India's Bhabha Atomic Research Center (BARC) to protest nuclear testing. The attackers posted text to the web site and destroyed data."

Source: Arquilla John, Ronfeldt David, "Networks and Netwars: the future of terror, crime, and militancy", Rand, 2001.

4. Attack on websites to protest against human right abuse in East Timor, 11/1998

"Portuguese hackers modified the websites from 40 Indonesian servers to protest against human right abuses in East Timor. The hackers posted the slogan "Free East Timor" on the websites."

Source: Arquilla John, Ronfeldt David, "Networks and Netwars: the future of terror, crime, and militancy", Rand, 2001.

5. CIH/Chernobyl, 4/1999

"The CIH/Chernobyl, a time bomb virus, was spread over the network causing great damage to business and home computer users. These specific viruses were activated on a predefined date on the anniversary of Chernobyl nuclear disaster. When activated, the virus would overwrite a portion of the hard disk."

Source: http://www.symantec.com/security_response/writeup.jsp?docid=2000-122010-2655-99, Last Accessed: 3/7/11

6. Attack Hits Swedish Signals Agency's Website, 11/6/2009

"The website of the Swedish National Defence Radio Establishment (Forsvarets Radioanstalt) has been the target of a prolonged denial of service (DoS) attack this week. There was some speculation that the incident was caused to protest to the agency's new role of intercepting and monitoring Internet traffic passing through Sweden. Forsvarets Radioanstalt (FRA) is an intelligence agency of the Swedish government, subordinated to the country's Ministry of Defence. The total downtime suffered was of almost 29 hours, but according to an official announcement (in Swedish), it did not affect the agency's work."

Source: <http://news.softpedia.com/news/Attack-Hits-Swedish-Signals-Intelligence-Agency-s-Website-126289.shtml>, Last Accessed: 3/7/11

7. Climate Change E-mail Hack, 11/23/2009

"A hack that exposed thousands of private e-mails and documents about global warming from a University of East Anglia climate change research center could be used for more malicious attacks down the road, as hackers use cybercrime to further political agendas, security experts said. Hackers broke into the e-mail server of the Climate Research Unit at the University of East Anglia on Nov 20, stealing more than 1,000 e-mails and more than 3,800 documents. Hackers then posted the e-mails and documents onto an anonymous FTP server in Russia, as well as a link to the 61-MB file on the blog Air Vent, accompanied by a note that read, 'We feel that climate science is, in the current situation, too important to be kept under wraps. We hereby release a random selection for correspondence, code and documents.'"

Source: <http://www.crn.com/security/221900742;jsessionid=RDEKOUOVD4YIZQE1GHRSKH4ATMY32JVN>, Last Accessed: 3/7/11

8. Chinese human rights Web sites suffer attacks, 1/25/2010

"The *sites of Chinese Human Rights Defenders* and four related groups were *targeted by cyberattacks*. A *distributed denial of service (DDOS)* attack paralyzed the Chinese Human Rights Defenders site for about 16 hours on Saturday, January 23rd and Sunday, January 24th. Also *attacked* were *Civil Rights and Livelihood Watch*, *Independent Chinese Pen Center*, *New Century News*, and *Canyu*. "*Chinese government is the most likely suspect for these attacks*," the organization said, though it wasn't able to locate the source and didn't share specific evidence beyond saying such attacks require significant resources. Earlier *attacks* have rendered its site "*inaccessible* for days, especially during 'sensitive' periods in China," the group said."

Source: http://news.cnet.com/8301-30685_3-10440342-264.html, Last Accessed: 3/7/11

9. Government sites crumple -Operation Titstorm, 2/10/2010

"Following the announced *Internet censorship plans* of the *Australian government*, which will likely include *Internet filtering* and the banning of some forms of pornography, the *group Anonymous* - made famous for its attacks and demonstrations against Scientology - has voiced a "call to arms" to all that are *opposed to the proposed legislations*. The operation was dubbed "*Titstorm*", and it was comprised of a *DDoS attack on government servers*. Attorney-General's department confirmed that the Parliament of Australia website was down for a while, and that the website of the Department of Broadband, Communications and the Digital Economy was *difficult to access*. "No government should have the *right to refuse its citizens access to information* solely because they perceive it to be 'unwanted'," said the email sent by Anonymous to media outlets."

Source: <http://www.net-security.org/secworld.php?id=8856>, Last Accessed: 3/7/11

10. Web site of China-based journalist club attacked, 4/2/2010

"An *organization for foreign journalists* based in *China* has become the latest *victim of cyberattacks* targeting the *Web sites or e-mail accounts* of human rights groups and reporters focused on China. Cyberattacks linked to China have gained more attention since Google Inc. accused Chinese hackers in January of trying to plunder its software coding and of hijacking the *Gmail accounts of human rights activists* protesting Beijing's policies. The Foreign Correspondents' Club of China said in an e-mailed statement Friday that its *Web site* was taken *down* because of *denial-of-service attacks* apparently launched over the last two days by computers within China and in the United States. *Yahoo e-mail accounts* belonging to *foreign journalists in China* have also apparently been *hacked* in recent weeks, and the *Web site* of the *Hong Kong-based China Human Rights Defenders* remained *shut down* Friday after a *denial-of-service attack* hit it last week."

Source: <http://abcnews.go.com/International/wireStory?id=10266124>, Last Accessed: 3/7/11

11. Hackers shut down EU carbon-trading website, 7/26/2010

"*Hackers hijacked Europe's carbon-trading website* and replaced it with *spoof page* detailing flaws in cap and trade scheme. *Anti-carbon trading activists* shut down the *website* of the *European Climate Exchange (ECX)*, replacing the site with a *spoof page* lampooning the industry. The *website* of the London-based carbon credit trading platform was *hacked* and showed the *spoof homepage for around 22 hours*. It then took technical staff another day to restore the official homepage. Explaining the "carbon trade scam", the *spoof site decried* how the *EU's flagship environmental policy* is "*susceptible to corporate lobbying*," offers industry "*licences to pollute* so they can continue business-as-usual," and "generates outrageous profits for big industry polluters, investors in fraudulent offset projects [and] opportunist traders." "Attempting to cause as much inconvenience, economical loss and image damage as possible, we deliberately tried to *maximise the virtual damage*," said the *hacker*, who spoke on condition of anonymity."

Source: <http://www.guardian.co.uk/environment/2010/jul/26/eu-carbon-trading-website-hacked>, Last Accessed: 3/7/11

Figures

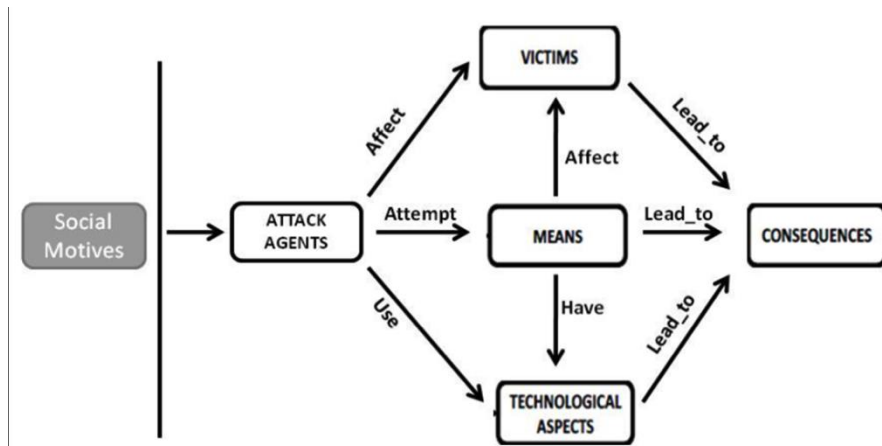


Fig. 1. Cyber Attack domain model

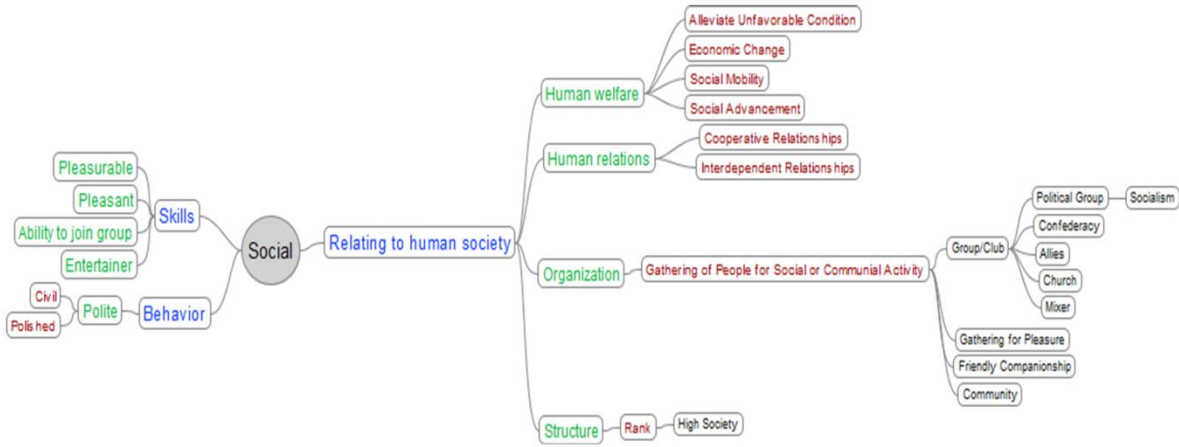


Fig. 2a. Dictionary Interpretations of the Word “Social”

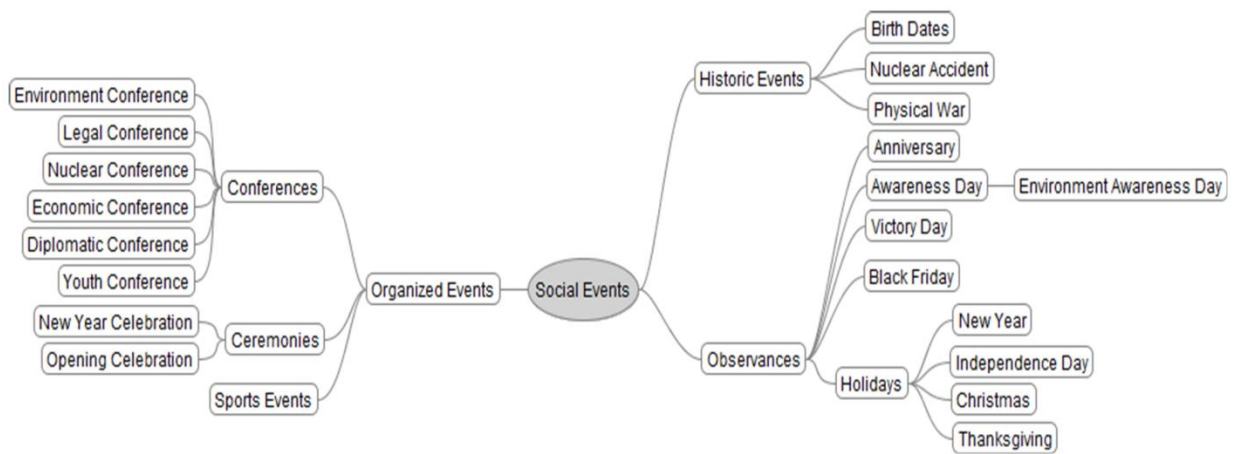


Fig. 2b. A Partial Taxonomy of Social Events

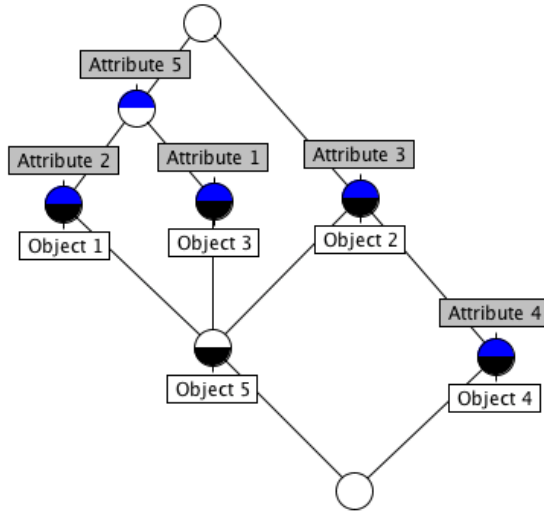


Fig. 3. Concept Lattice of the Formal Context

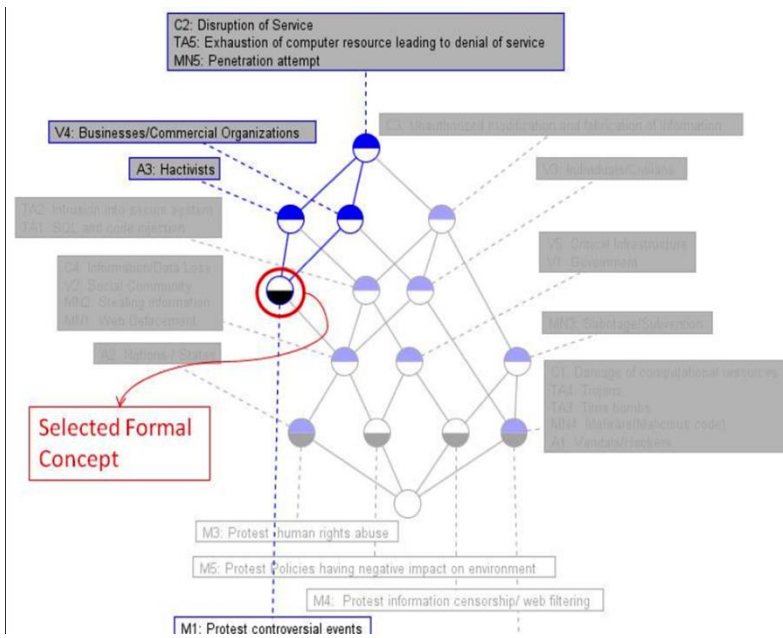


Fig. 4. Concept lattice with social motive “M1: Protest Controversial events” as a selected formal concept, with concepts in its intent highlighted

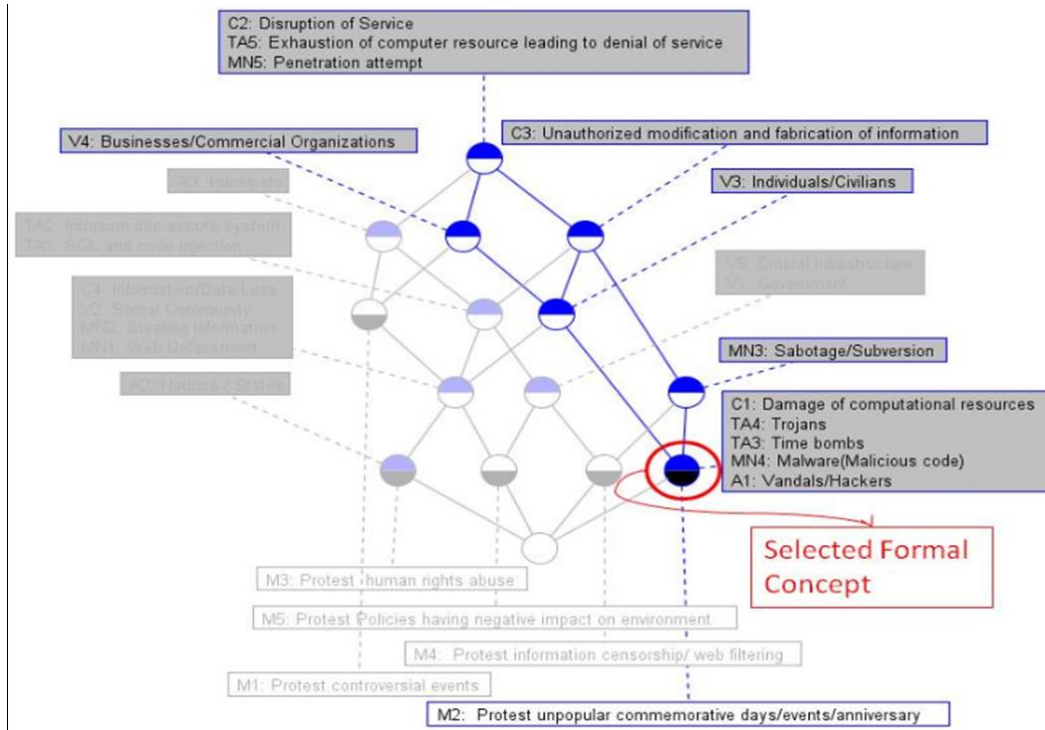


Fig. 5. Concept lattice with attack agents “A3: Hacktivists” as a selected formal concept, with concepts in its intent highlighted

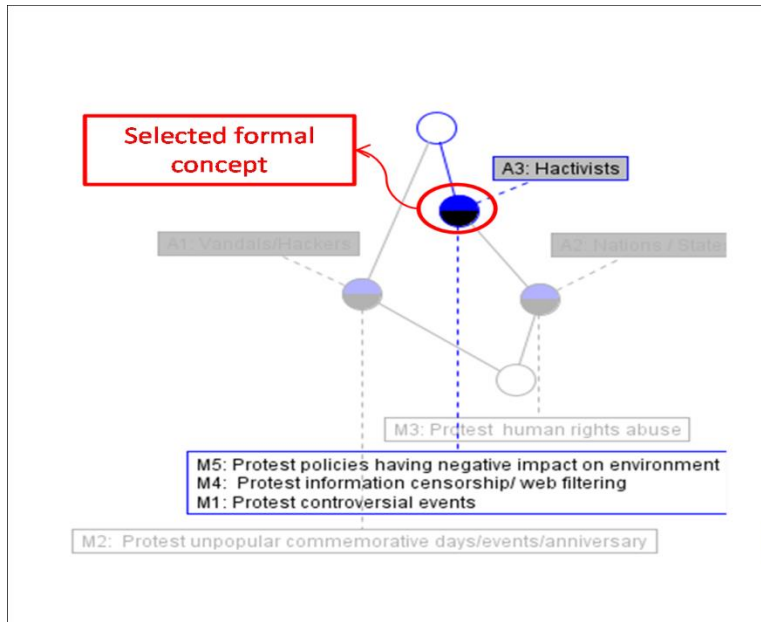


Fig. 6a. A formal concept node representing the object selected

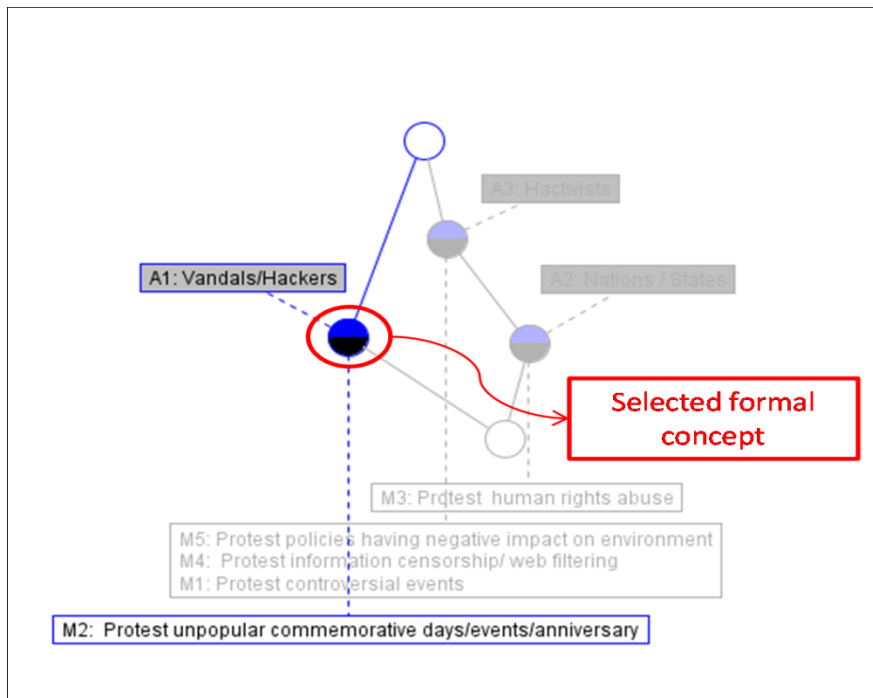


Fig. 6b. A formal concept node representing an attribute selected

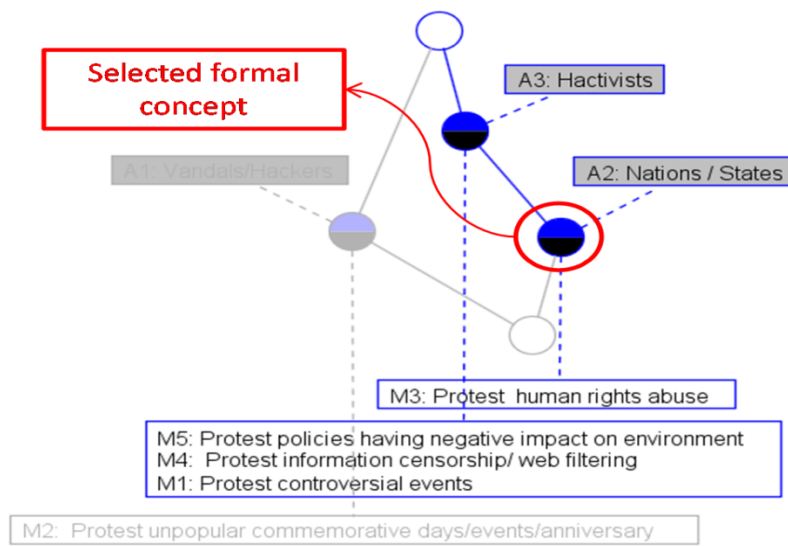


Fig. 7a. A formal concept node representing the object selected

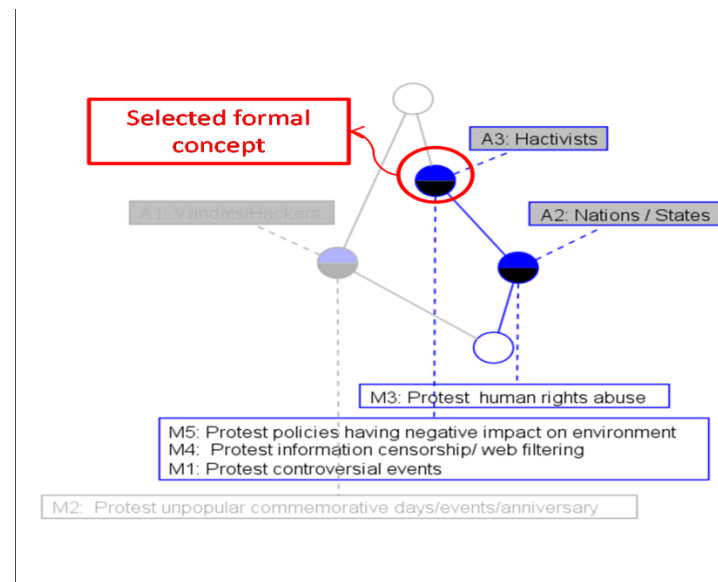


Fig. 7b. A formal concept node representing the attribute selected

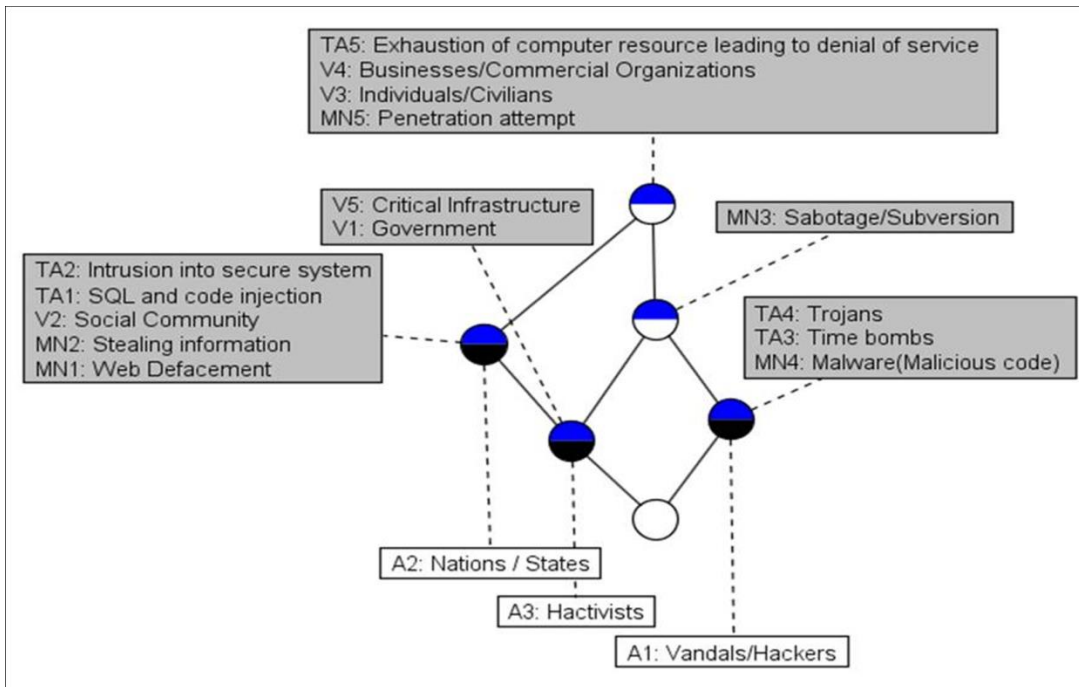


Fig. 8. Concept lattice with “Attack Agents” as objects and “Means, Victims, and Technological Aspects” as attributes

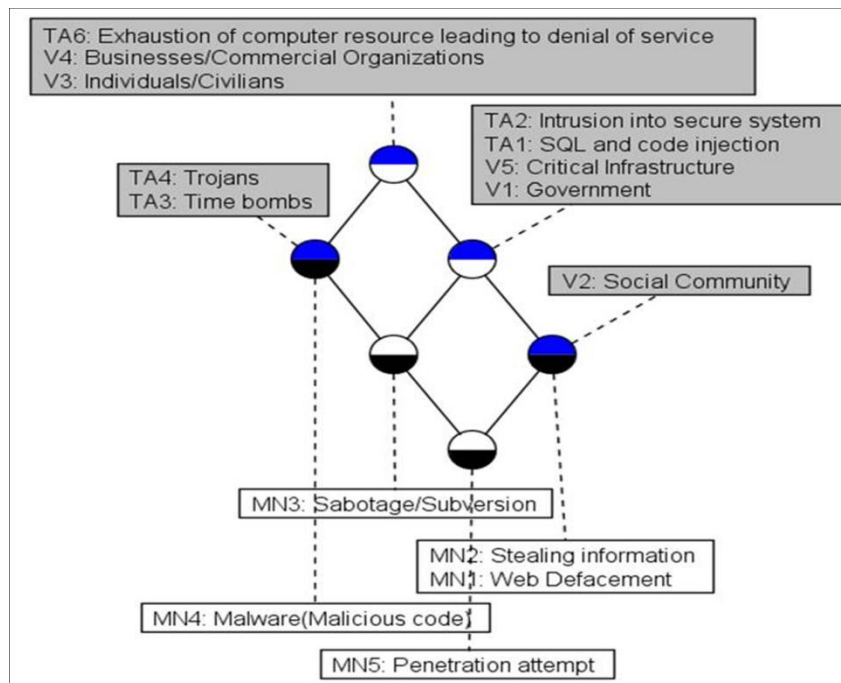


Fig. 9. Concept lattice with “Means” as objects and “Victims, and Technological Aspects” as attributes

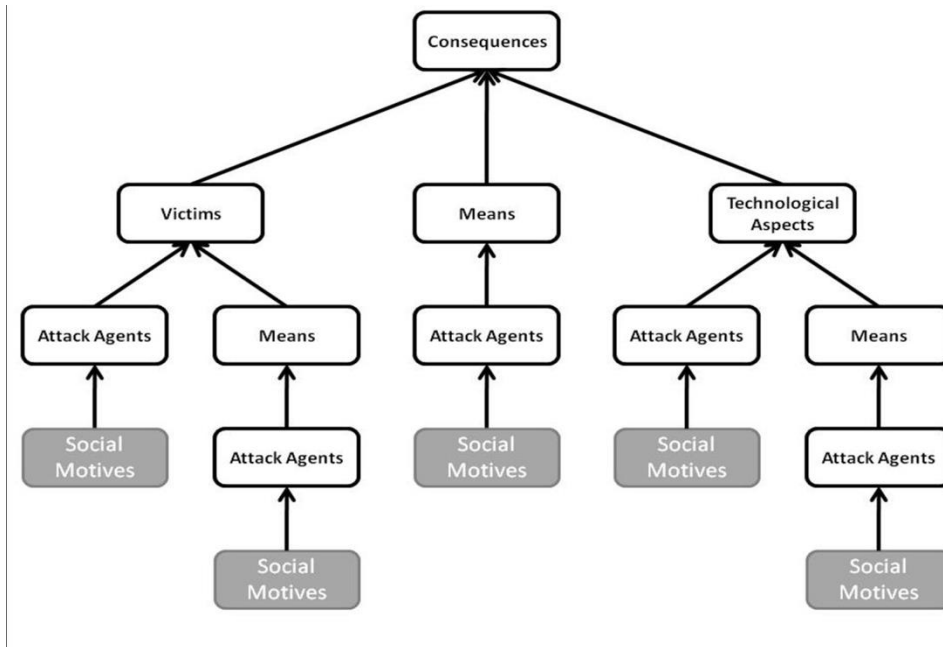


Fig. 10. Decision tree in a cyber attack domain model

The Main Page

File View Function

Ready

Hierarchical Tree View Display

- [-] Consequences
 - [-] Means
 - [-] AttackAgents
 - ProtestControversialEvents
 - ProtestUnpopularEvents
 - ProtestHumanRightsAbuse
 - ProtestInformationCensorship
 - ProtestPoliciesHavingNegativImpactOnEnvironment
 - [-] Victims
 - + AttackAgents
 - + Means
 - [-] TechnologicalAspects
 - + Means
 - + AttackAgents

Fact and Proposition Set Display

Conditional probability distribution function table of fact ProtestControversialEvents, given propositions of AttackAgents

	Level 1	Level 2	Level 3
P1	0.9	0.075	0.025
P2	0.9	0.075	0.025
P3	0.025	0.075	0.9

Modify Select Level

Log Display

Opening scenario: Consequences_10132010-193230.txt

Fig. 11. A hierarchical structure of a Threat Model

Select Each Leaf Factor Level

Select the level for each leaf node or select "Deselect" for no selection.
 Press "Randomize" to generate a random selection

Factor: ProtestControversialEvents
 Level 1 Level 2 Level 3

Factor: ProtestUnpopularEvents
 Level 1 Level 2 Level 3

Factor: ProtestHumanRightsAbuse
 Level 1 Level 2 Level 3

Factor: ProtestInformationCensorship
 Level 1 Level 2 Level 3

Factor: ProtestPoliciesHavingNegativeImpactOnEnvironment
 Level 1 Level 2 Level 3

Fig. 12. Factor selection in FPS web application

File View Function Ready

Hierarchical Tree View Display

- [-] Consequences
 - [-] Means
 - + AttackAgents
 - [-] Victims
 - + AttackAgents
 - + Means
 - [-] TechnologicalAspects
 - + Means
 - + AttackAgents

Fact and Proposition Set Display

Propositions' probability table of Consequences

P1	P2	P3	P4
0.1376	0.344	0.344	0.1744

Log Display

Opening scenario: Consequences_10132010-1!
 Scenario recommendation: Damage of computational resources

Final Results Display

Conclusion: Damage of computational resources
Click on topic name to expand node

Consequences		
0.582		
0.2		
0.2		
0.017		

Victims	Means	TechnologicalAspects
0.0	0.0060	0.0050
0.0	0.0060	0.0050
0.5	0.249	0.422
0.5	0.366	0.422
0.0	0.374	0.148

Fig. 13. Graphical display of result the propositions probability of consequences

Select Each Leaf Factor Level

Select the level for each leaf node or select "Deselect" for no selection.
 Press "Randomize" to generate a random selection

Factor: ProtestControversialEvents
 Level 1 Level 2 Level 3

Factor: ProtestUnpopularEvents
 Level 1 Level 2 Level 3

Factor: ProtestHumanRightsAbuse
 Level 1 Level 2 Level 3

Factor: ProtestInformationCensorship
 Level 1 Level 2 Level 3

Factor: ProtestPoliciesHavingNegativeImpactOnEnvironment
 Level 1 Level 2 Level 3

Fig. 14. Factor selected as Level 3 (High) and Level 1 (Low) for social motives

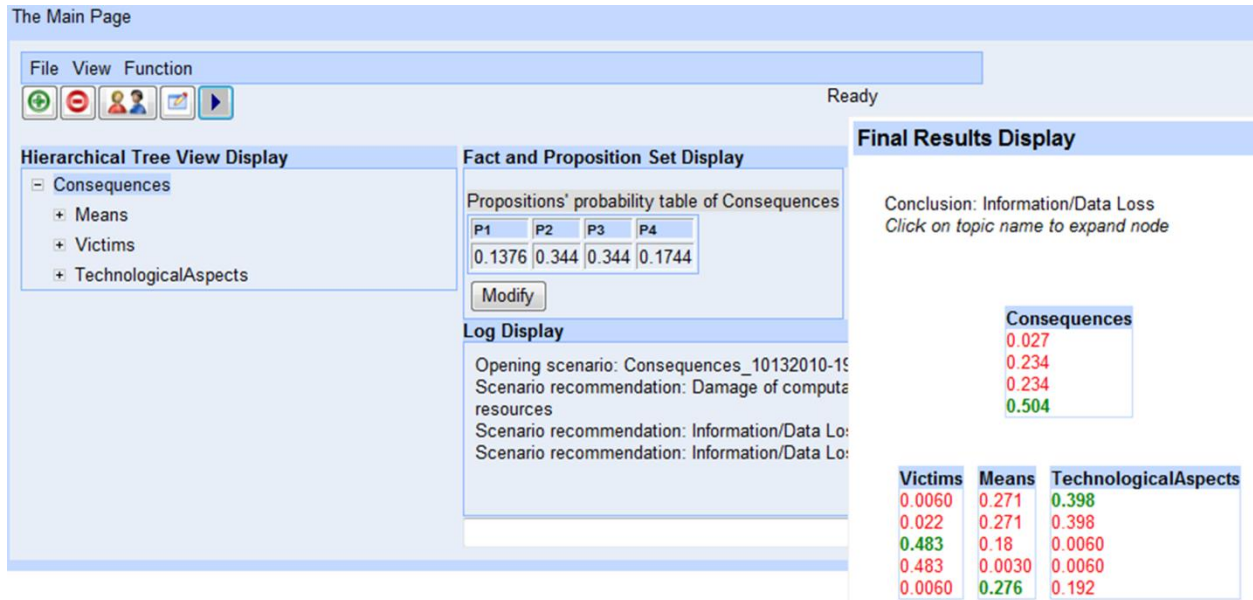


Fig. 15 Final Results Display showing the consequences for the news about “WikiLeaks”

Tables

Table 1. Mapping words and phrases that infer to the factors of cyber attack domain model

Cyber attack news articles	Social Motive	Attack Agents	Means	Technological Aspects	Victims	Consequences
1. Web attack against French Government websites	Government nuclear and social policy	Group – Strano Network	Net strike attack, point browser to governments website	...	French government	...
2. Website of DOJ attack, USA	Communication's Decency Act passed	Protesters	Deleting contents	...	United States Department of Justice	...
3. Attack on atomic research center	Protest: nuclear testing	Hackers	Attacked website, posted text, destroyed data	...	India's Bhabha Atomic Research Center	...
4. Attack on websites to protest against human right abuse in East Timor	Human right abuses	Hackers	Modified the websites	...	Indonesian servers	...
5. CIH/Chernobyl	Anniversary of Chernobyl disaster	...	Viruses, spread over the network	Overwrite, hard disk, Time bomb	Business and home computer users	...
6. Cyber attack to protest against G8 summit, Germany	Protesting, G8, meeting	Hackers	Launched 10,000 cyber attacks	...	Disrupt financial centers, business	...

Table 2. Formal Context Table

Objects\Attributes	Attribute1	Attribute2	Attribute3	Attribute4	Attribute5
Object1		x			x
Object2			x		
Object3	x				x
Object4			x	x	
Object5	x	x	x		x

Table 3: Formal context table with cyber attack news articles as objects and cyber attack factors as attributes

	A1: Vandals/Hackers	A2: Nations / States	A3: Hacktivists	M1: Protest controversial events	M2: Protest unpopular events	M3: Protest human rights abuse	M4: Protest information censorship	M5: Protest env. affecting policies	MN1: Web Defacement	MN2: Stealing information	MN3: Sabotage/Subversion	MN4: Malware(Malicious code)	MN5: Penetration attempt	TA1: SQL and code injection	TA2: Intrusion into secure system	TA3: Time bombs	TA4: Trojans	TA5: Exhaustion of computer resource	V1: Government	V2: Social Community	V3: Individuals/Civilians	V4: Business/Commercial Organization	V5: Critical Infrastructure	C1: Damage of computational resources	C2: Disruption of Service	C3: Unauthorized modification	C4: Information/Data Loss
N1: Web site of China-based journalist club attacked	X				X				X			X						X		X				X		X	
N2: Government sites crumple -Operation Titstorm			X			X						X					X	X						X			
N3: Climate Change E-mail Hack			X				X		X						X					X	X					X	
N4: Attack Hits Swedish Signals Agency's Website			X			X							X					X					X		X		
N5: April fool's day, Conficker worm	X			X								X					X				X					X	
N6: Cyber attack to protest against G8 summit			X	X								X					X							X		X	
N7: CIH/Chernobyl	X			X						X	X				X	X					X	X	X	X	X	X	
N8: Chinese human rights Web sites suffer attacks		X			X							X						X		X	X				X		
N9: Hackers shut down EU carbon-trading website.			X				X	X				X	X								X			X	X		
N10: DoS attack, Belarus /Eastern Europe	X			X								X						X			X			X			
N11: Websites attacked to protest human right abuse in E. Timor			X		X			X					X							X	X					X	
N12: Attack on atomic research center			X				X	X						X									X			X	
N13: Website of DOJ attack			X			X				X		X	X	X					X							X	
N14: Web attack against French Government websites			X				X					X						X	X						X		

Table 4. Formal context table with social motive as objects and other factors as attributes

	A1: Vandals/Hackers	A2: Nations / States	A3: Hacktivists	MN1: Web Defacement	MN2: Stealing information	MN3: Sabotage/Subversion	MN4: Malware(Malicious code)	MN5: Penetration attempt	TA1: SQL and code injection	TA2: Intrusion into secure system	TA3: Time bombs	TA4: Trojans	TA5: Exhaustion of computer resource	V1: Government	V2: Social Community	V3: Individuals/Civilians	V4: Business/Commercial Organization	V5: Critical Infrastructure	C1: Damage of computational resources	C2: Disruption of Service	C3: Unauthorized modification	C4: Information/Data Loss
M1: Protest controversial events			X				X						X				X			X		
M2: Protest unpopular events	X					X	X	X		X	X	X				X	X		X	X	X	
M3: Protest human rights abuse		X	X	X	X		X	X	X				X		X	X	X			X	X	X
M4: Protest information censorship			X		X		X	X	X				X	X			X			X	X	
M5: Protest policies having negative impact on environment			X	X	X		X	X	X				X	X	X	X	X			X	X	X

Table 5. Formal context with “Social Motive” as objects and “Attack Agents” as attributes

	A1: Vandals/Hackers	A2: Nations / States	A3: Hactivists
Legend			
N: News			
A: Attack Agents			
M: Motives			
MN: Means			
TA: Technological aspects			
V: Victims			
C: Consequences			
M1: Protest controversial events			x
M2: Protest unpopular events	x		
M3: Protest human rights abuse		x	x
M4: Protest information censorship			x
M5: Protest policies having negative impact on environment			x

Table 6. Overlap coefficients for “Social Motive” as objects and “Attack Agents” as attributes

	A1: Vandals/Hackers	A2: Nations / States	A3: Hactivists
Attributes			
Objects			
M1: Protest controversial events	0	0	1
M2: Protest unpopular commemorative days/events/anniversary	1	0	0
M3: Protest human rights abuse	0	1	1
M4: Protest information censorship/ web filtering	0	0	1
M5: Protest policies having negative impact on Environment	0	0	1

Table 7. Formal Context with “Attack Agents” as objects and “Means, Victims, and Technological Aspects” as attributes

Legend																
N: News																
A: Attack Agents																
M: Motives																
MN: Means																
TA: Technological aspects																
V: Victims																
C: Consequences																
		MN1: Web Defacement	MN2: Stealing information	MN3: Sabotage/Subversion	MN4: Malware(Malicious code)	MN5: Penetration attempt	V1: Government	V2: Social Community	V3: Individuals/Civilians	V4: Businesses/Commercial Org.	V5: Critical Infrastructure	TA1: SQL and code injection	TA2: Intrusion into secure system	TA3: Time bombs	TA4: Trojans	TA5: Exhaustion of computer res
A1: Vandals/Hackers				X	X	X			X	X				X	X	X
A2: Nations / States		X	X			X		X	X	X		X	X			X
A3: Hactivists		X	X	X		X	X	X	X	X	X	X	X			X

Table 8. Overlap coefficients for “Attack Agents” as objects and “Means, Victims, and Technological Aspects” as attributes

Objects \ Attributes	Attributes														
	MN1: Web Defacement	MN2: Stealing information	MN3: Sabotage/Subversion	MN4: Malware(Malicious code)	MN5: Penetration attempt	TA1: SQL and code injection	TA2: Intrusion into secure system	TA3: Time bombs	TA4: Trojans	TA5: Exhaustion of computer resource leading to denial of service	V1: Government	V2: Social Community	V3: Individuals/Civilians	V4: Businesses/Commercial Organizations	V5: Critical Infrastructure
A1: Vandals/Hackers	0	0	0.67	1	1	0	0	1	1	1	0	0	1	1	0
A2: Nations / States	0.5	0.5	0	0	1	0.5	0.5	0	0	1	0	0.5	1	1	0
A3: Hactivists	1	1	0.67	0	1	1	1	0	0	1	1	1	1	1	1

