# Modelling the Enemies of an IT Security Systems - A Socio-Technical System Security Model

Stewart KOWALSKI and Jeffy MWAKALINGA
Department of Computer and Systems Sciences,
Stockholm University, 16440 Kista, Sweden,
stewart@dsv.su.se, jeffy@dsv.su.se

ABSTRACT

This paper presents a socio-technical security model for security systems that include both the system being defended and the attacking system. We first model security as a ratio or function of the states that an attacker can produce over the states that defend can control. We then sub divided the control states of a defending systems using the security value chain and socio technical system security model. The paper then presents two attempts to validate the acceptance of the defense model using cross culture surveys of individuals from over 20 different countries indicate culture variation in security modeling. An example of how an attacker can model an attack strategy is given at the end of the paper. The paper concludes with a discussion of how the modeling can be new research in modeling criminal organization using effective based operations methodology.

KEY WORDS

Enemy of IT, deterrence, prevention, detection, response, and socio-technical model, center of gravity

## 1. BACKGROUND AND INTRODUCTION

One of the systemic security problems with information and communication technology (ICT) is that it is a double-edged sword. That is to say it can be used for constructive and destructive purposes [10]. For example, remote computing technologies permit individuals to work from home but they also permit hacks to attack them from their homes. Over the years, we have seen continuous waves of new technologies to construct better and better security solutions for ICT systems. First, simple reference monitors were developed to monitor and separate different users. Then, multipurpose operating systems, firewalls, intrusion detection systems, and prevention systems were developed. These point security products provide solutions to a single problem rather than systems solutions. However, many of these technologies do not meet stakeholders' expectations and it could take between two and ten years for a security product to mature [1]. But how long shall we continue to be reactive [18] to yesterday's hacker technologies? We have to be proactive by studying hackers' technologies and by predicting their next moves and making our systems adaptive [18].

In the beginning of ICT era, hacking was for fun and to get attention, but hackers developed it into a business and the cyber criminals created their own business models [18]. The goal of cyber criminal or hackers like all criminals is to increase revenue flows at minimum costs [18]. One of the cheapest ways of obtaining information is by social engineering. Results presented by [11] show that social engineering is a technology that has a good probability to succeed at minimal cost. Social engineering is a type of attack against the human factors in which a victim is persuaded to hand over sensitive information. Hackers succeed in social engineering because people are not trained to be suspicious of each other [2]. Technical and non-technical means were used by Mitnick [2] to obtain the source codes of operating systems and telecommunications devices to study their vulnerabilities. The security systems today protect information against amateur computer intruders like the script kiddies but not against professional criminals [2].

For hackers information is the currency and consequently more information implies more money [18]. To get more information one should perform more attacks. Since one of the primary goal of computer science is to automate and therefore in order to gain more information the hackers automate attacks. In order to cut costs the hackers use downloadable toolkits to perform almost any kind of IT systems attack. But there is some exception in the community to focus on cutting costs. There are other groups like the Advanced Persistent and Threat (ATP) hacker groups, which tend to perform attacks independent of the cost [13]. Their goal is to gain access to the defense, financial or governmental information at any price. Bar-Josef has suggested that some possible example of ATP activities can include the Stuxnet worm and the attacks on Estonian and Georgian governments in 2007 [23].

This paper is divided into 5 sections. Following this introduction in section 2 we briefly describe the history and organization of IT hacking. In section 3 we introduce a socio-technical systems security model. In section 4 we combine the IT security model and the IT hacking organization model and give an example of a high level insecurity attack strategy matrix. The paper concludes in section 5 with a discussion on methods that can be used to collect more information on the enemy's socio-technical systems models to better understand predict and control them.

## 2. GENERATIONS AND ORGANIZATION OF THE ENEMY OF IT SECURITY

### 2.1 Generations of the Enemy of IT

According to Rogers there are four generations of hackers or as the author refer to enemies of IT systems security [8] [9]. The first generation was a group of creative programmers and scientists in the 1960s mostly from MIT and Stanford institutes. This group was much respected. The members of this group were called "gurus". The second generation was a group of computer hackers of both hardware and software for mainframes and personal computers in the 1970s. Some of them founded major computer companies. The third generation concentrated on breaking computer games and copyrights in the 1980s. The fourth generation is a group of hackers from the 1990s up to today. This is a group of script kiddies, cyber punks, insiders, coders, professionals, and

cyber terrorists. Script kiddies have very limited computer skills and depend on programs and tools that are freely available on the Internet. Script kiddies are motivated by media attention. They can cause a great deal of damage by launching attacks like distributed denial of service attacks (DDoS), but they do not necessary understand how a computer attack works. Cyber punks have better computer skills than script kiddies and have some understanding of how a computer attack works. Insiders are usually computer knowledgeable and who are employees or ex-employees or contractors. They are able to carry attacks because they have access privileges to computer and information systems. Most of them appear to be are motivated by revenge. Coders are those hackers with technical skills to write scripts and automated tools for attacking computer and information systems. They act as mentors to the script kiddies and other related groups. This is a dangerous group and is motivated by power and prestige. Professionals are a group of thieves, criminals, corporate espionage who are highly trained and motivated; they are like guns for hire. There is not much information about this group. Cyber terrorists appear to be having its back ground after the fall of the intelligence agencies in the Eastern bloc. They are well funded and well trained and could carry out information warfare. They are motivated by political and criminal activities [8] [9]. Next we discuss the organization of hackers.

### 2.2 The Organization of Hackers

The hacking community appears to be organized in the following way as Figure 1 outlines. There are six groups in the organization. The first group is of researchers. They investigate systems to find vulnerabilities in applications, operative systems, frameworks, and in different products [19]. Notice here that there are two dimensions of vulnerabilities [9] the objective and subjective vulnerabilities. The objective vulnerabilities depend on the social, political, economical, and demographical entity that determine the vulnerability to cyber attacks. Subjective vulnerabilities depend on the person's or entities self-perception on the risk of becoming a victim of an attack.

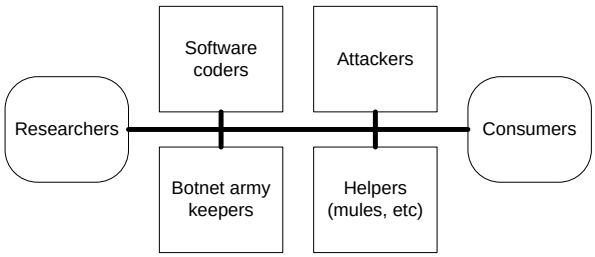


Figure 1: Overview of Hackers Types

The next group is software coders, who write intelligent malicious toolkits and programs like Trojans for monitoring, capturing, retrieving information, and covering their activities. The marketing for their programs is done in the underground forums. As an example one master hacker wrote a phishing toolkit for gathering information from victims and put it on the Internet [21]. The other hackers downloaded the toolkit and started using it on the websites of their choices. The master hacker had provided cloud storage for the gathered information. Once retrieved the information would securely stay in the cloud where only the proxy hacker who was applying the toolkit would access the information. It was supposed to work exactly as in the cloud computing. But what the proxy hackers did not know was that the master hacker was able to access all the information that was gathered by all the proxy hackers [19]. The next group is botnets army keepers, which maintain and increase the army of botnets [21]. They control the botnets using modern technologies by issuing commands and controls [21]. Now hackers are using the social networks to control the botnet armies [18]. Social networks have brought trust among friends of sharing different kind of information and since social networks are very tender there appear to have much vulnerability with very few strong security controls. The next group consists of attackers, which include all kinds of hackers that perform the attacks. Some attackers use botnets which they hire at prices that are set by botnet army keepers to gain information. Some attackers use free tools that are available on The Internet. One example of the botnet is called 'Mumba' [20]. The botnet was created by a criminal group called Avalanche group, which had installed information stealing software in 55000 computers. As a result, hackers retrieved 60 GB data. The data include bank accounts credit card numbers and social networking web sites that were stored in one server [20]. The acquired information is sold to the consumers [21]. The next group consists of consumers who use the stolen information and translate it into money [21]. Consumers use the stolen information by creating fake credit cards, transferring money from victims' online banking accounts and to create fake identities. The helpers group includes mules and entities who offer free hosting servers for storage of stolen information. Mules are a network of people who transfer stolen money from banks in one country to other countries at commissions. The next section presents the social-technical economic model.

## 3. THE SOCIO-TECHNICAL SECURITY MODEL

The Social-technical model is aimed at addressing security problems at different levels and perspectives and is outlined in figure 2.

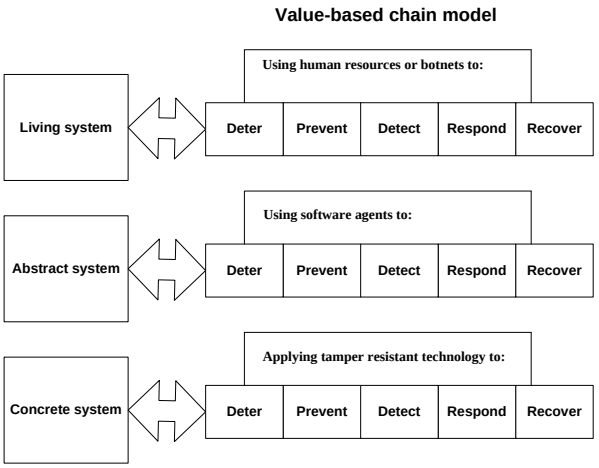


Figure 2: The Socio-technical security model

This model has two main components: the value chain and three general abstraction levels. The value chain model was established in industry to describe the concept of value creation security activities in a large telecommunication supplier [15]. The abstraction levels of the model are taken from security modeling work in the early 1990 [3]. In system science the general premise is that are three types of systems: living; abstract; and concrete. These systems share some properties which can be used to explain, predict, control,

create, and destroy any systems with a given degree of certainty [3]. The security value based chain model was developed for commercial security targets in the telecom industry [7]. Applying this to value based chains we have an abstract information security value chains which contains deterrence, protection, detection, response, and recovery sub systems [5]. A security system should have measures to deter attackers from attacking an information system. If the security system can not deter attackers then it has to have measures to control or prevent attacks to an information system. If the security system can not deter or prevent attacks, the next step is to detect attacks. If the information security system can not deter, prevent or detect, it has to have measurers to respond to attacks. If an information system can not deter, prevent, detect, or respond then it should have measures to recover after attacks

### 3.1 Value Chain Model

The value chain model is a general security model that could be applied at different personal, family, organizational, national, and supranational levels. For example, at the national level there are sub systems that control measures: for deterring intruders; for protecting the inside of the nation and natural boundaries; for detecting pies; for responding to an attack; and for recovering from an attack. When the government makes a budget for the defence ministry they have to allocate the budget to the different departments of the ministry. The question is how much of the total military budget to allocate for deterrence department? How much of the total military budget should be allocated for protection, detection, response, and recovery departments?

In the same way an analysis is needed to determine how much of the total security resources should be allocated to the different sub–systems of the of an information security system in a company. If a security manager of a company was to be given a budget of two million dollars to spend on information security in the company how will it be spent? [3] That is to say, how much would the manager use on the deterrence sub-system, on protection sub-system, on detection sub-system, on response sub-system, and on recovery sub-system. Some sub systems may require more resources depending on the nature of the information system.

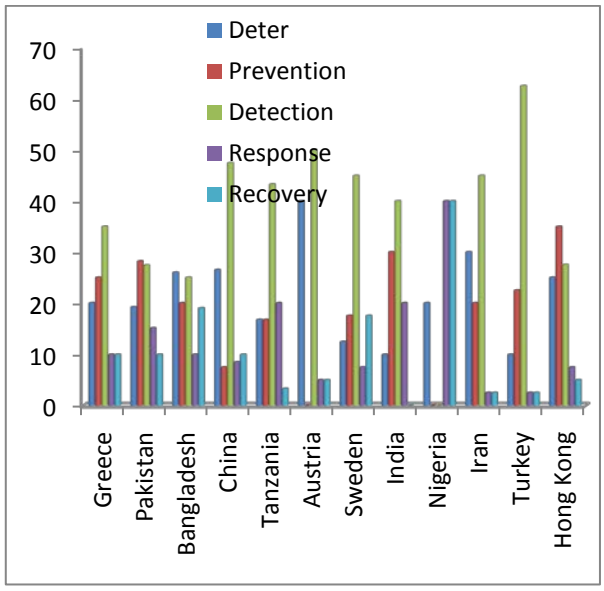


Figure 3: Average allocation of resources on deterrence, prevention, detection, response, and recovery

A survey was made of master students in information security to help understand which value-based chain functions are perceived to be the more important. We asked respondent to imagine they were security managers of companies. We made a survey of 60 students from France, Sweden, Sri Lanka, Libya, USA, Libya, Taiwan, Thailand, Uzbekistan, Spain, Peru, Pakistan, Nepal, Iran, India, Iceland, China, Brazil, Bangladesh, and Serbia Montenegro. We made this survey to understand whether culture affect the decisions, which users make when deciding, which of the five security value-based chain were more important. The average of the allocations is shown on figure 4 below. We also compared results of bachelor and master students.

A second survey was made on 37 international master students in information security from Austria, Bangladesh, China, Greece, Hong Kong, India, Iran, Nigeria, Pakistan, Sweden, Tanzania, and Turkey. Every student was to assume to be working for a Global Socio-Technical Security Group. The student was to setup a social technical security system to decrease plagiarism at the Stockholm University. The students were to outline a budget of how 10 million monetary units would be spent using the security value chain of deter, protect, detect, respond, and recover functions.

The results from the second survey are outlined in figure 3. It is interesting to note that all the students from China allocated less than 10% on the prevention, response, and recovery sub systems but allocated around 47 % of the total budget on detection sub system. Note also that Nigeria allocated nothing on the prevention and detection sub systems. Turkey on other hand spent 62 % of the whole budget on detection sub system. In this scenario, the detection function was perceived to be more important than other functions with the average of 37 % of the whole budget. The recovery sub system got the lowest allocation with average 10, 4% of the whole budget.

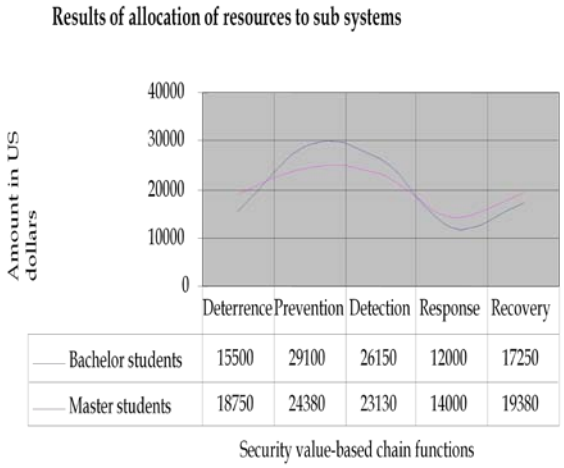


Figure 4: Average allocation of resources on deterrence, prevention, detection, response, and recovery

Another example of the security value chain concept can be applied in a more concrete manor [6]. This concrete information security value chain consists of the hardware, software, systems, and services in a computer. The manufactures of hardware add some value when they create hardware and put into computers. The software producers add another value when the put software into the computer. The other vendors add value by putting systems into the

computer. Then other vendors add value to the computer by putting services. Let us assume that computer hardware producers spend 100 dollars to create the hardware and expect to sell for 150 dollars as shown in figure 5. In the same way software producers spend 50 dollars to create computer software and sell it for 70 dollars. Let us assume those who create systems spend 60 dollars and sell them for 80 dollars. Assume that vendors who create services spend 40 dollars and sell for 60 dollars. Let us assume that distributors, whole sellers and retailers charge 100 dollars and so the end customer buys a computer for 460 dollars.

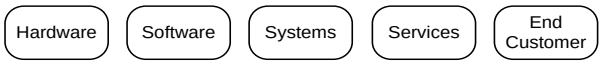


Figure 5: Value based chain for computers

The computer in this case has no security services. Let us assume that producers and vendors decide to add the basic security services into the computers. As a result of this the computer hardware producers spend 120 dollars to add security measures and expect to sell it for 180. The software vendors spend now 70 dollars to produce software with security and expect to sell them for 100 dollars. The vendors of systems now spend 80 dollars and expect to sell for 110 dollars. The vendors of services spend now 60 dollars and are expected to sell for 80 dollars. Let us assume that the distributors, whole sellers, and retailers charge now 150 dollars per computer. Now the end customer has to pay 590 dollars for the computer. A customer has to choose between a computer without security that costs 460 dollars and the one with security that costs 590 dollars. The decision will depend on the security knowledge that a customer has and also the size of customer's wallet. With the current situation where there is an asymmetric knowledge about security in computers between vendors and customers it would be interesting to see how end customers react to the prices. In this scenario the middle men are gaining more profits than the producers of computer hardware, software, systems and services. So this could imply that in future they could be reluctant to add any other security measures because they are not the ones that gain from additional security measures

### 3.2 A Socio-Technical System

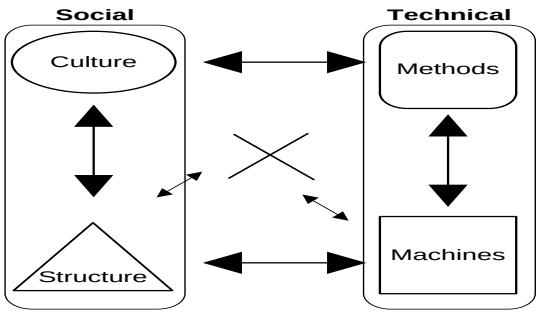


Figure 6: A Socio-technical System [8]

As figure 6 suggests, an information system could be broken down into a socio and technical sub-system. The social subsystem can be sub divided into culture and structural sub systems. People using an information system have culture like ethics, traditions, laws and other social values. The technical part consists of methods and machines.

Every system strives to be in balance so when any of the components or subsystems of the socio-technical system change then other components change too, to keep the balance. In an IT system the social sub system can include ethical/cultural, legal/contractual, administrational managerial and operational procedural layers. The Technical sub system can include the following layers: mechanical/electronic; hardware; operating system; application; data, store, process, and collect information [3]. When a new machine is introduced into a company it can require that changes be made in procedures, ethical, legal, and administrational issues. Insecurity is the result of instability that is created when social and technical systems adapting at different levels at the same rate to each other and the environment [3]. The Socio-technical system consists of the living, abstract, and concrete systems.

**3.2.1 Living Systems:** At the living system the enemy could apply human resources in social engineering to gather information and architecture of an information system. In the next generation information systems one could use botnets which act on behalf of human being to perform different activities. In the living system an information security system one could use human resources to deter attackers, prevent attacks, to detect attacks, to respond to attacks, and to recover from attacks. It is also possible to train users or immunize them from attacks by injecting small doses of spams and phishing in the same way that medical systems vaccinate people with small doses of the diseases [11]. Even training users against undue influence from others, such as used for instance in social engineering, could be done by the same inoculation method, as argued by Levine [12]. Here users are exposed to small, controlled, doses of influence, and then taught about influence in order to strengthen their defense.

**3.2.2 Abstract Systems:** With these systems the enemy of IT could automate an attack on information system by applying mobile software agents. To defend an information system at this level one could apply different agents to deter attackers, to prevent attacks, to detect attacks, to respond to attacks, and to recover from attacks. It will be not feasible to use human recourses to deter, protect, detect, and respond to different attacks.

**3.2.3 Concrete Systems:** With these systems level the attackers use different technologies like inside channel attacks to attack physical components. These include probing, fault-based analysis, timing analysis, and power analysis [4]. We could apply tamper resistant technology to deter attacks, prevent attacks, to detect attacks, to respond to attacks, and to recover from attacks. At this level one can apply cryptographic modules in deterrence, prevention, detection, response, and recovery sub systems [5]. In timing attacks one could apply randomizing timings' technology [4]. Cryptographic modules can also apply data masking [4].

## 4. ATTACKING A SYSTEM USING THE SOCIO-TECHNICAL MODEL

As figure 7 outlines all the groups in the organization of the enemy of IT have socio-technical systems. A defender's information system, with inputs and outputs, is also a system consisting of culture (people who have culture), structure, methods and machines.

The enemy of IT scan the defenders systems to understand the culture of users, the structure, the methods and machines of an information system. The enemy of IT will try to find out the tools, methods and processes that an information system is applying to defend in the different subsystems: deterrence, prevention, detection, response and recovery at

the living, abstract and concrete systems. The aim is to understand the number of states that the hacker could control in an information system. Security can also be defined as the ratio of the states known and unknown that could be controlled by the enemy of IT to the states that can be controlled by the information systems [3]. There are states that are controlled by the enemy of IT but are unknown [3] to the defending information system. The smaller the ratio of the states controlled by the hacker to the states that are controlled by an information system the harder it is to succeed when attacking. If this ratio is high it is easier for the attacker to succeed the information system and difficult to control the information system.

Vulnerabilities in an information system could be exploited by an enemy of IT. Assume that there are N vulnerabilities. Assume also that the enemy of IT has vulnerabilities 1, 2, 3 … N and has 1, 2, 3… k methods and tools for exploiting the vulnerabilities. Assume that an information system could defend H% of the K methods and tools that an enemy of IT could use for the first vulnerability. The H% methods ant tools are the states that an information system could control for this vulnerability while (K-H) % methods and tools are the states that the enemy could control. By analyzing the number of states in this way for all the vulnerabilities, we will get the total number of states that could be controlled by the enemy versus the states that could be controlled by an information system.

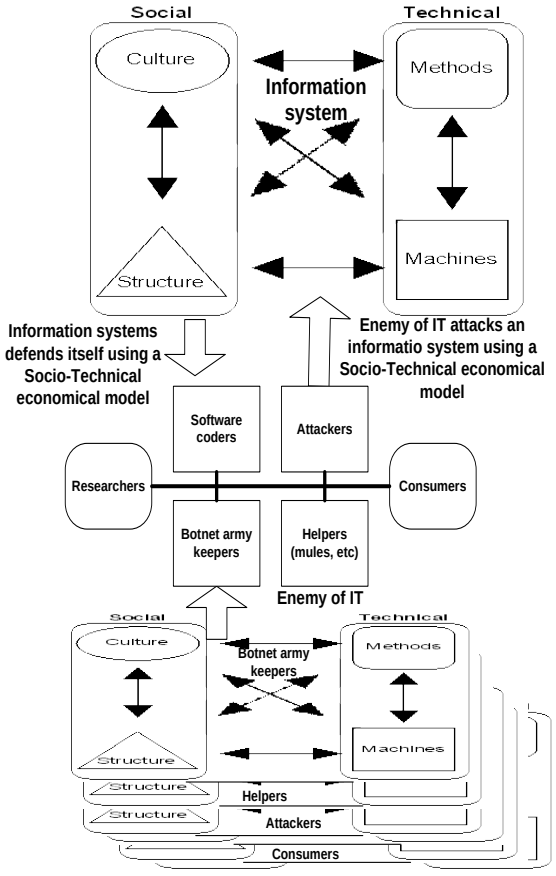


Figure 7: Applying the Socio-technical security model to attack and to defend

The scanning of the defenders socio-technical systems could also be done at all three levels the living, abstract and concrete systems. For example at the living system they apply so called social engineering methods to scan. Social engineering methods can be automated or manual. In manual social engineering the attacker makes phone calls or just listens to conversations of system administrators during lunches etc. In automated living engineering the enemy of IT could for instance use botnets to gather the information. At the abstract system level one could use manual or automated mechanisms to utilize the information gathered during the social engineering to attack an information system. In automated mechanisms, the enemy of IT can use software agents [agents] for instance. The same is applied at the concrete and physical systems of the defender's system. This information will help the enemy of IT to determine weaknesses in the different sub systems and in the whole information system. The enemy of IT could analyze the allocation of economical resources of different sub systems on the defenders information system. For example an authentication system can be implemented to provide strong authentication, which can be more expensive to attack than a system providing simple authentication. The enemy of IT could use these results to decide whether attacking the IT security system could bring a good economic outcome.

## 5. CONCLUSIONS AND DISCUSSION

We have described a model for understating and explaining possible attack strategies of the enemies of IT: The enemy tests the strength of information systems before attacking. By checking tools, methods and processes that a defender uses to deter attackers, to prevent attacks, to detect attacks, respond, and recover an information system after attacks at the . The enemy uses Socio-technical security model to attack an information system at the living, abstract and concrete layers. As figure 8 indicates in some information systems much more resources are spent on detecting and preventing attacks while very little is spent on deterrence, response and recovery subsystems.

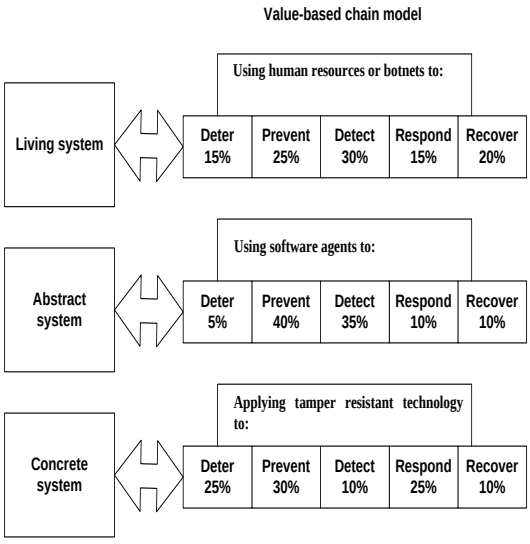


Figure 8: Example of security attack budget using value-based chain

For instance in the abstract system, figure 8, 5% was spent on deterring attackers, 40% was spent on preventing attacks, 35% of the security budget was spent on detecting attacks, 10% was spent on responding to attacks, and 10% was spent on recovering from attacks. The enemy of IT could find out that the deterrence subsystem is the weakest and attack the information system through the deterrence subsystem. As a defender this model could help to analyze the subsystem or the point in the information system that has weakness and strengthen it. A security manager could use this model to determine the potential victims in a company by analyzing all

the computers and information systems in a corporation. The results of the analysis should indicate in which systems to add security measures.

In future, we intend to extend the research work done by Z. Alach on applying Effects-based operations (EBO) to model methamphetamine criminal behavior and organize in New Zealand [14]. The aim of Alach's research is to holistically identify key processes, behaviors, criminal groups, critical paths and the interactions in order to identify the center of gravity of the criminal organizations. Alach believes that by identifying the center of gravity of a drug organization, police could more effectively combat these organizations. We intend to investigate the center of gravity of the enemy of IT by using the socio-technical system. There are nine possible centers of gravity in the socio-technical system as outlined in figure 9. The center of gravity of the enemy could be methods, machines, culture, structure or some kind of combinations. If for example the center of gravity is the methods that an enemy of IT is using to attack, then a defending system could modify the deterrence, prevention, detection, responding sub systems to make it harder for the enemy of IT to succeed.

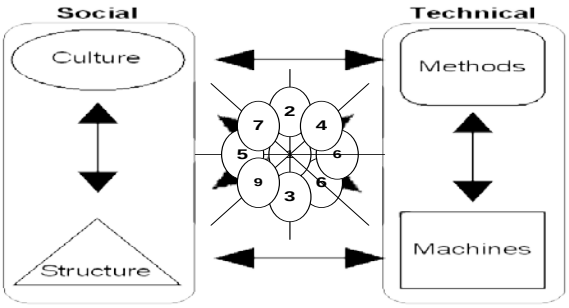

Figure 9: Centre of gravity

## 6 REFERENCES


[1] Gartner Inc, **A hype cycle for information security, Building secure applications**, Gartner, Inc. 56 Top Gallant Road, Stamford, USA, 2006

[2] Mitnick, D.K., Simon, W. L The art of deception: Controlling the human element of security, Wiley Publishing, 2002

[3] Kowalski, S. Lectures Research in Information systems security. **Scientific methodology course**, Department of Computer systems sciences. University of Stockholm and Royal Institute of Technology Stockholm Sweden, 2008

[4] Kawamura, S., Matsumoto, T., Fujisaki, K., Torii, N., Ishida, S., Tsunoo, Y., Saeki, M., & Yamagishi, A. TSRC and Side Channel Security Requirement. Physical Security Testing Workshop. Tamper-resistance Standardization Research Committee (TSRC), 2005

[5] Kowalski, S. **IT Insecurity: A Multi-disciplinary Inquiry.** Doctoral thesis, Department of Computer Systems Sciences. Stockholm University and Royal Institute of Technology. Stockholm, Sweden.

[6] Mwakalinga, J., Yngström, L., Kowalski, S. A holistic and immune system inspired security framework. **Proceedings for the 2009 International Conference on information Security and Privacy (ISP-09),** Orlando, FL, USA, 2009

[7] Kowalski, S., & Boden, M. Value Based Risk Analysis: The Key to Successful Commercial Security Target for the Telecom Industry, **2nd Annual International Common Criteria CC Conference** Ottawa, 2002

[8] Rogers, M, **A new hacker Taxonomy**, Department of Psychology University of Manitoba, Winnipeg RSA Security Conference, 2001

[9] Rogers, M., A Social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study, Doctoral Thesis. Dept of Psychology. University of Manitoba. Winnipeg, 1999

[10] P. Dalal, Cyber Crime and Cyber terrorism: Preventive defense for cyberspace violations, **Cyber crime research center,** www.crime-research.org/articles/1873, 2006

[11] Nohlberg, M. **Securing information assets: understanding, measuring and protecting against social engineering attacks**, Doctoral thesis. DSV Report Series no. 09-001. The Department of Computer systems and sciences, Stockholm University, Stockholm, Sweden, 2009

[12] Levine, R. **The Power of Persuasion**, Hoboken, NJ: John Wiley & Sons Inc.

[13] M. Daly, Advanced Persistent Threat, **LISA 09 conference**, USENIX, 2009

[14] Z. Alach, policing and effects-based operations: modeling methamphetamine, www.emeraldinsight.com/1363-951X.htm, **pijpsm, 33(3),** New Zealand, 2009

[15] Porter, M. E., **Competitive Advantage**, The Free Press. New York, 1985

[16] Stallings W, Brown, L, **Computer Security – Principles and practice,** ISBN 0-13-513711-X Person Prentice Hall, 2008

[17] D. Steflick, **Hackers, crackers and Network Intruders,** www.cs.binghamton.edu/~steflik/cs455/Hackers.ppt

[18] N. Bar-Josef, Social Networks as an Attack Platform: Cybercriminals Love Social Media Too, **Security Week**, www.securityweek.com, 2010

[19] N. Bar-Josef, An Inside Look at the Hacker Business Models, **Security Week,** www.securityweek.com**,** 2010

[20] AVG Technologies, The 'Mumba', botnet disclosed, http://avg.typepad.com/files/revised-mumba-botnet-whitepaper_approved_yi_fv-2.pdf

[21] N. Bar-Josef, The Structure of Cybercrime Organization- hackers have Supply Chains Too! **Security Week**, www.securityweek.com, 2010

[22] N. Kshetri, The Global Cybercrime Industry, Institutional and Strategic perspectives, Springer Verlag, ISBN: 978-3-642-11521, 2010

[23] N. Bar-Josef, When the Advanced Persistent Threat , **Security Week**, www.securityweek.com/when-advanced-persistent-threat-apt-meets-industrialization**,** 2010