Social Network Dynamics of Insider Threats: A Preliminary Model

Andrew P. Moore, apm@cert.org*
Kathleen M. Carley, kathleen.carley@cs.cmu.edu**
Matthew L. Collins, mlcollins@cert.org*
Neal W. Altman, na@cmu.edu**

*The CERT® Division of the Software Engineering Institute
**Center for Computational Analysis of Social and Organizational Systems
Carnegie Mellon University
Pittsburgh, PA 15213
412-268-5465

Abstract

In this paper, we describe a preliminary system dynamics model of insider espionage social networks. Social capital, which is measurable in terms of standard social network metrics, can serve to both indicate low or dwindling insider engagement with their jobs as well as a means to bolster an insider's connections in a way that disincentivizes insider threat and improves employee productivity. The model focuses on two forms of social capital: (1) obligations and expectations, and (2) social norms. We present our analysis of two widely known espionage incidents using the model to demonstrate the dynamics we are researching. We also describe four working hypotheses, based on our analysis and past experience, that form the basis of our research going forward. Finally, we describe possible uses of the model, including tracking early indicators of insider threat and evaluating the ways that organizations can disincentivize the threat by improving employee engagement and their overall job satisfaction. Clearly, no firm conclusions can yet be drawn and much work remains to analyze additional incidents and comparison data of the average employee. Nevertheless, the model that we describe here provides a useful "stake-in-the-ground" and vision for our future efforts.

Keywords: insider threat, cybersecurity, social network analysis, modeling and simulation, system dynamics, social capital, espionage, employee engagement

1 Introduction

Insider threat is the threat to an organization's critical assets posed by individuals—including employees, contractors, and business partners—who are authorized to use the organization's information technology systems (Cappelli, Moore, and Trzeciak 2012). Insider threat has become an increasing concern both for reasons of international security and industrial espionage (Chan 2003). Insider threat programs within an organization help it to manage the risks due to these threats through specific prevention, detection, and response practices and technologies. Such programs have been mandated by Executive Order 13587, *Structural Reforms to Improve the*

[®] CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, for all DoD and U.S. Government organizations that handle classified information.

A preliminary study of insider threat programs in the U.S. private sector by the Intelligence and National Security Alliance (INSA) found that many organizations have no insider threat program in place and most of those that do, have significant deficiencies (INSA 2013). Another major finding of the INSA study is that many insider threat programs are "technology-focused, centered on tools that monitor network traffic and online activity, and that [the programs] monitor only specific people that display concerning or suspicious online behavior" (INSA 2013, p. 2). INSA reported that the most mature programs document and track nontechnical information, such as badge records and phone records, in addition to online activity, such as websites visited and files downloaded. In addition to its findings, INSA recommended that robust programs monitor both technical and nontechnical behaviors "to provide a holistic view of an organization's insider threat risk" (INSA 2013, p. 2).

The research question that we address is, "What are the human behavioral processes that can increase the likelihood of an individual becoming an insider threat and engaging in the unauthorized sharing of information?" We are most concerned with the sharing of classified material, and this work is informed by a detailed understanding of such behavior. This paper develops a model of the mechanisms that could promote or reflect an insider's decision to commit a malicious act in terms of the insider's social networks. We use the system dynamics modeling approach, recognizing that such a model has the benefit of enabling managers to think about who might become threats (Sterman 2000)(Meadows 2008). We describe ongoing empirical research that is providing evidence for believing this model. Simulation of the model enables us to track findings from our data analysis and provides the potential to evaluate the benefits of organizational measures to improve employee social capital.[1] An overview of system dynamics modeling and notation is provided in Appendix A.

2 Background

Three factors stand out in identifying actors who are potential threats: organizational culture, personality, and social distancing. First, the organizational culture (Petty et al. 1995; Lee and Yu 2004; Kraemer, Carayon, and Clem 2009) can increase insider threat risk in one of three major ways (Colwill 2009):

1. Organizational culture may foster open interaction both in the workplace and with those outside of the workplace, thus reducing barriers to information transmittal (i.e., the ability to communicate).
2. A culture of autonomous work in which personnel can handle critical information in isolation reduces barriers to unauthorized access (i.e., the access to critical information).
3. Organizational culture can, through social barriers on acceptable lifestyles or organizational limitations, create high and unequal workloads, lack of or unequal compensation, or other forms of perceived inequities (i.e., perceived inequity).

Royds (2009) reported that 95% of data loss reported by the U.K. government were due to such factors. In general, corporate culture in conjunction with management style can serve to lower

[1] We use the VenSim environment by Ventana Systems, Inc.: http://www.vensim.com.

overall performance (Lim 1995), increase the perception of inequities (Ogbonna and Harris 2000), and therefore increase the likelihood of insider threat activities. The lack of fit between an employee and the organizational culture, either in terms of norms, beliefs, work style, or ethics, is often seen as a possible trigger for disgruntlement (O'Reilly, Chatman, and Caldwell 1991), which can, in turn, lead to insider threat activity.

Personality and personal issues combine to be a second factor commonly discussed with respect to who becomes an insider threat. Case studies point to a lack of money as driving individuals to engage in covert activity to improve their financial status; ideological motivations as driving individuals to act to address perceived problems; and lack of awareness that they are doing anything wrong and a need for adrenalin as driving individuals to engage in covert activity as a way to add excitement to their lives. Anger, revenge, divided loyalties, family problems, and so on are often listed as motivations (Federal Bureau of Investigation 2014). Other studies point to the technical competence or intelligence of the agent (Magklaras and Furnell 2005).

The third major factor has to do with social distancing. Those engaged in insider threat often act to distance themselves, or have been distanced, from family members and co-workers. This withdrawal of the employee is sometimes seen as introversion or depression (Shaw, Post, and Ruby 1999). Along the same lines, many of these agents are either distanced from or become increasingly distanced from their families or significant others—such as failure to maintain contact, acrimonious interactions, break-ups, and so on. At the same time, although they rarely discuss it, agents have growing contacts with those outside the organization. Such external contacts include increased contact with those to whom they will transmit information and increased contact with those who are "similar" to them on the relevant dimension and encourage them to live outside the corporate norms. From a network perspective, this process of creating social distance to certain groups and increasing contact with a different group, effectively increases the agent's *betweenness* in the network. The agent, in effect, becomes a broker between these different groups.

Economic sociologist Mark Granovetter argued that, within market economics, the social context is critical for understanding an individual's actions:

> *Actors do not behave or decide as atoms outside a social context, nor do they adhere slavishly to a script written for them by the particular intersection of social categories that they happen to occupy. Their attempts at purposive action are instead embedded in concrete, ongoing systems of social relations (Granovetter 1985, p. 487).*

This sociological concept of *embeddedness* applies just as well to understanding the behavior of cybersecurity threat behaviors as described by Bruce Schneier (Schneier 2012). We've adapted his view of this context for the insider threat to organizations in Figure 1.

Figure 1 shows the insider as a potential part of two social networks: one associated with his/her employer and one associated with a competing group or adversary. Loyal work with an employer requires adherence to those group norms as opposed to competing group norms. Societal pressures (including moral, reputational, institutional, and security technologies) motivate insiders to adhere to employer group norms. Though positive societal pressures exist, an insider may bow to stronger competing pressures, defecting from the obligations of their employment and potentially resulting in theft, sabotage, or worse.

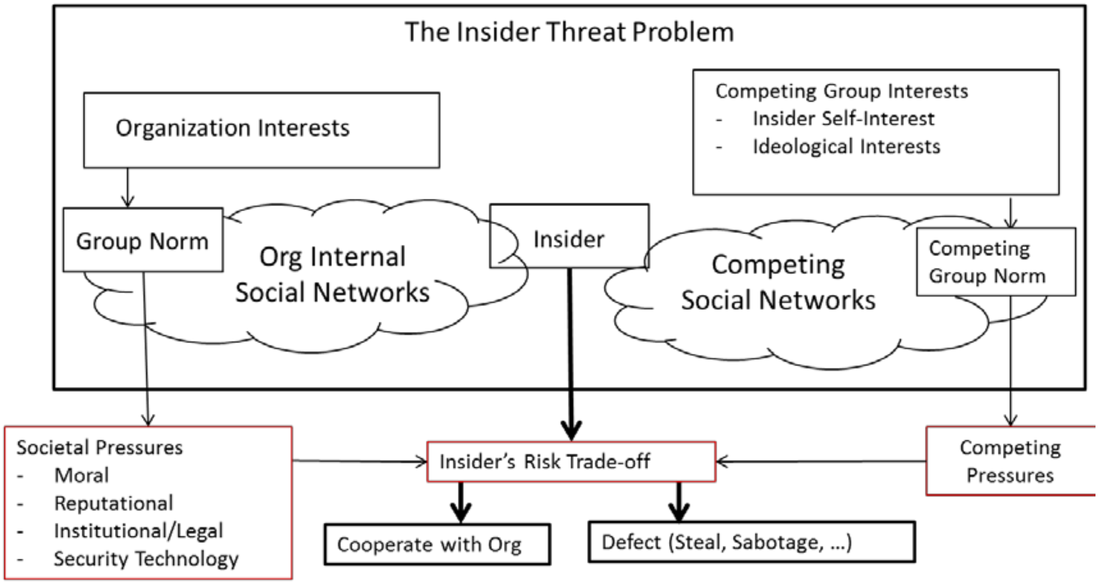


Figure 1: Insider National Security Threat in Context - Adapted from (Schneier 2012)

The above is consistent with social control theory, which proposes that people's relationships, values, reputation, beliefs, and agreements encourage abiding by the law (Hirschi 1969). Social capital can be thought of as the value that social networks provide to people (Kadushin 2012). Whereas *physical capital* is about the value derived from tangible assets and *human capital* is about the value derived from people doing work, *social capital* is about the value of the relationships between people. Social capital, which is measurable in terms of standard social network metrics (Burt 2000), can serve to both indicate low or dwindling insider engagement with their jobs as well as a means to bolster an insider's connections in a way that disincentivizes insider threat and improves employee productivity overall. In other words, the social capital that an individual has with his or her organization may discourage that individual from acting out against the organization in an unlawful manner. An organization's investment in employee social capital can therefore be a win-win for both employees and the organization.

3 Espionage Motivations

While low or dwindling social capital within the organization may be a factor in the insider's decision to spy, more traditional motivations include money, ideology, compromise/coercion, and ego/excitement (from the classic MICE acronym) as well as disaffection, and personal relations with individuals of influence. Some have called these traditionally described motives into question (Burkett 2013), but mostly from the perspective of what makes for effective agent recruitment. A comprehensive study by the Defense Personnel Security Research Center (PERSEREC) found that more recent incidents involved volunteers that had divided loyalties, giving the ideological motivation greater weight (Herbig 2008).

Another author found evidence that certain of the traditional motivations were more prevalent than others (Stone 2001). Stone sites statistically significant results that distinguish attributes of individuals who spied for financial reasons (money) compared with those who spied for ideological reasons. Likewise, he finds important distinctions between the attributes of individuals who were dissatisfied with their employment and the attributes of individuals who were coerced (a catchall category that Stone calls "other," which includes blackmail) into espionage. His analysis suggests that the *financial* and *ideology* motivations can be viewed as bipolar, as can the motivations of disaffection and coercion. Stone places these two pairs of motivations along a two-dimensional space with ideology and financial along the x-axis and disaffection and coercion (i.e., other) along the y-axis, as shown in Figure 2. He shows how 12 spies that he analyzed can be placed along this space. Another less formal observation made by Stone is that the motivations can be thought of in terms of whether the individual is oriented more toward *self* or more toward *others*. So motivations of financial and disaffection can be attributed to individuals who are more self-focused, whereas motivations of ideology and coercion can be attributed to individuals who are more other-focused.

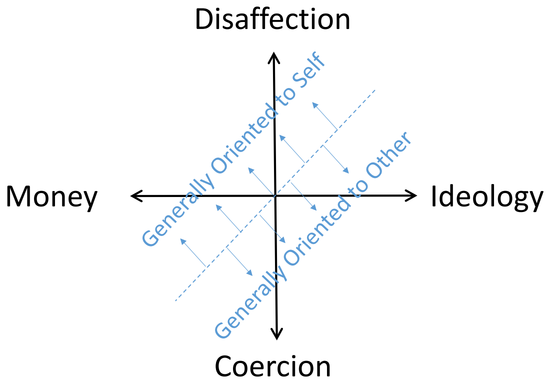


Figure 2: Stone's Two-Dimensional Spy Motivation Space (Stone 2001)

We use Stone's partitioning of the motivation space in our preliminary system dynamics model, with a variable for each of the four motivations. Stone's theory does not try to argue that real spies cannot have complex combinations of multiple motivations, as is evidenced by Stone's placement of subject spies continuously in the two-dimensional space. We, therefore, allow the four motivation variables to be changed somewhat independently. Ideally, we will ultimately be able to run the model with different settings of the motivation variables and reflect conditions and behaviors seen in real incidents involving insiders who exhibited those motivations.

We develop a measure of insider motivation based on Stone's four motivation variables. Consider each of the variables independent of one another. Let each of these variables range on the interval 0 to 1 where 0 is the least motivation and 1 is the largest possible motivation. Since the motivations of Money and Ideology are at opposite poles (and likewise for Disaffection and Coercion), for a particular individual, we take the maximum of the two as the dominant motivation along that axis.

Let X = max(Money, Ideology)
Let Y = max(Disaffection, Coercion)

Then the following also ranges over the interval 0 to 1 and accounts for both dimensions:

basic motivation = X+(1-X)*Y

Notice that X and Y are interchangeable in the equation.

We propose that the insider's allegiance to the U.S. and strength of connections to the family are going to determine whether and to what extent these motivations take hold to actually commit espionage. Therefore, letting the variables “insider’s allegiance to U.S.” and “strength of insider’s ties with family” range from 0 to 1, our measure for insider motivation is as follows:

insider’s motivation to spy
= (1-insider’s allegiance to U.S.)
* (1-strength of insider’s connections with family)
* basic motivation

We will use this measure as the starting point for our modeling effort. The inherent complexity of this domain will undoubtedly require refinement to this basic measure based on future research.

4 Espionage Data Collection and Analysis

We are in the process of collecting and analyzing public sources of data on insider espionage incidents. This preliminary report describes two such incidents. Using the data, we analyze the insider’s espionage actions and construct social networks that include the insider’s relationships, the time of the relationship, assets related to the incident, organizations related to the incident, and countries related to the incident. While the timeframe of the espionage cases may take place over many years, social network changes discovered in the data sources may be described at different levels of granularity—from hours to months to years. In addition, we have limited insight into the full scope of communication that the insider had with contacts at the victim organization and with the enemy. We must rely on reports from others, including that the insider “became distant” to infer that social capital was decreasing over time at the victim organization, while using known illicit contacts to show an increasing level of social capital with the adversary.

4.1 Specific Incidents

The two incidents described in this report provide examples of the variations in motivation seen in documented incidents. In both cases, the principals were arrested, tried, convicted, and sentenced for espionage against the United States.

In the *Walker* incident, John Anthony Walker, Jr. used his position as a military communications technician in the U.S. Navy to provide a stream of classified materials to the Soviet Union over a period of 18 years. Walker voluntarily initiated contact through the Soviet embassy in Washington to reverse his then current financial difficulties and, subsequently, to enjoy an affluent lifestyle far beyond his military salary. (Walker and his Soviet handlers retrospectively confirmed the primacy of money over ideology and the lack of coercion (Earley 2014).) Walker was considered capable and was generally well regarded by coworkers and superiors. Disaffection seems to have had little role in this case; it is questionable whether Walker ever felt great loyalty to anyone beyond himself (Earley 1988). At the same time, it is likely that successful espionage fed his sense of superiority and self-importance. As Walker’s personal access to classified materials ended due to voluntary retirement from the military, he subsequently recruited or encouraged other individuals, primarily family members, to feed classified information through Walker so that he could continue to receive payments.

In the *Manning* incident, Bradley Edward Manning (and subsequently Chelsea Elizabeth Manning) was employed as a low-level military intelligence analyst. Although technically competent, Manning was not happy with military life and was not well regarded by his peers. Considered a marginal soldier by his superiors, a shortage of individuals with the requisite technical skills ensured his continued access to classified materials. Concurrent with the Manning's military training and deployment to a war zone, he developed contacts with civilian computer hackers and was exposed to their ideological orientation. Subsequently, Manning copied classified materials and provided them for public access. In this case, there was no monetary compensation and the insider asserted the ideological motivation. Disaffection with the military was a major motivating factor while overt coercion does not seem to have been in play. Indirect coercion, in the sense of meeting the expectation of a group or organization (in this instance, the hacker community), may have been a factor. The insider's unhappiness and unreliability was evident to associates, friends, and strangers, which led to rapid detection and arrest through self-incrimination ("Chelsea Manning" 2015)(Nicks 2012).

4.2 Limitations of Current Work

Clearly, more than two cases need to be studied to come to firm conclusions about insider spy social networks. In addition, we need to understand how the spy's social networks differ from that of the average employee if we are to say anything about using the information as a means to detect suspicious activities early, or prioritize the caseload of intelligence analysts. Future work will progress in both of these directions, as we'll discuss in the conclusion to the paper.

5 A Causal Loop Model of Insider Threat Emergence

In his seminal paper (Coleman 1988), James Coleman describes three forms of social capital:

1. *Obligations and expectations* social capital is in the form of reciprocity—if I do something for you, I expect that you are obligated to do something for me in the future. As this back and forth continues through time, trust between parties grows. Likewise, the social capital grows as people can count on others for help when they need it.

2. *Information channels* social capital is specifically in the form of information that people can provide each other. It is similar to the previous form, except that it is information that is being exchanged between people rather than generally helpful acts.

3. *Social norms* social capital is in the form of the benefit people gain from being assured that people in the community behave responsibly according to a set of social norms that the community has either implicitly or explicitly established. The community may pressure its members to follow the rules through a set of sanctions that may be implicit or explicit.

In our model of the social capital aspects of insider threat, we focus on the first and third of these forms of social capital. In the context of national security espionage, the norms and sanctions are well established, but each community decides how it will interpret and enforce the rules subject to the constraints set by the U.S. Government. Insiders who decide to spy may be affected by the organization's local policies or just the general lack of social capital he or she has with others in the organization. The second form of social capital—information channels—is related to the first, but is not explicitly considered as part of our current modeling efforts. Future work may consider it more directly, especially as part of the information collection activity the insider conducts as part of the espionage. This additional information may add noise to our analysis of insider social capital within the organization during the espionage.

The starting point for our modeling effort is a system dynamics model of social capital developed by Richard Dudley (Dudley 2004). Dudley develops a generic model of the dynamic structure of social capital as well as a submodel for each of the three forms of social capital identified by Coleman, as described in the previous section. Our model considers three primary social networks within which social capital can grow or decline: the (victim) organization, the adversary (non-U.S. state actor), and the spy's family. For our current effort, we consider the network of colluding insiders, if any, to be a part of the adversary social network. We adapt Dudley’s submodel of reciprocity (i.e., Coleman’s obligations and expectations) for both the victim organization and adversary models. It is based on the primary mechanisms of trust and reciprocity, which have been investigated most in the research on social capital (Burt 2000) (Torsvik 2000). We also adapt aspects of Dudley’s submodel on community norms, particularly those describing the negative effects of the insider’s perceptions of overly restrictive community norms, as an influence on the insider’s potential disaffection with the victim organization.

The following subsections respectively describe aspects of the model related to the victim organization, the adversary, and the integration of these into a model that describes the transfer of social capital incrementally from the victim to the adversary.

5.1 Organizational Social Network Growth and Decline

Figure 3 shows how social networks can grow within the organization, at least partially, due to the value (social capital) that the networks provide in conducting collaborative work with others. The social capital grows through successful cooperative activities and the increased trust that results from those activities. The (dark blue) reinforcing feedback loop *R1a* reflects the growth of the insider’s social network as successful cooperative activities are conducted and trust within the insider’s social network grows based on this success. Increased trust strengthens the insider’s social connections, and associated social network even further. The growth of the cooperative activities depends on the number of people within the organization and the strength of the social connections between people, including the insider. Of course, there are limits to the growth of the social network, as depicted in the (brown) balancing feedback loop *B1a*. As the number of activities that the insider engages in increases, the perceived personal cost of additional connections to the insider increases. This cost limits the growth of the insider’s social network to a size within which the insider is comfortable, based on the success of the insider’s past activities.

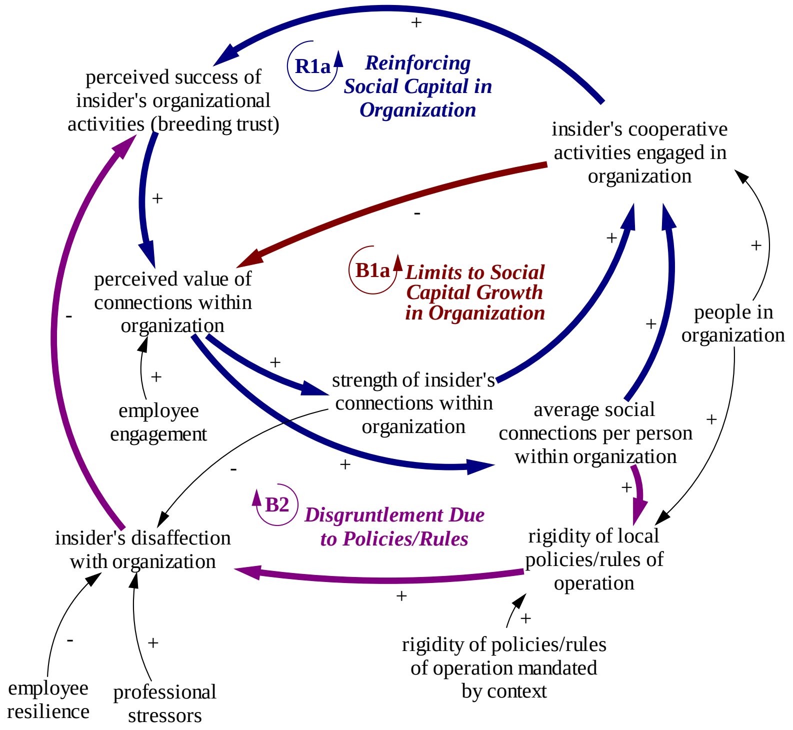

perceived success of insider's organizational activities (breeding trust)
R1a
Reinforcing Social Capital in Organization
insider's cooperative activities engaged in organization
perceived value of connections within organization
B1a
Limits to Social Capital Growth in Organization
people in organization
employee engagement
strength of insider's connections within organization
average social connections per person within organization
B2
Disgruntlement Due to Policies/Rules
insider's disaffection with organization
rigidity of local policies/rules of operation
rigidity of policies/rules of operation mandated by context
employee resilience
professional stressors

Figure 3: Organizational Social Capital Growth

As seen in the lower left of Figure 3, disaffection with the organization may come about for multiple reasons. Past CERT research shows that professional stressors (e.g., negative performance reviews, lack of promotion, being reassigned to a less attractive position) can have a huge impact on the insider and potentially influence his/her decision to spy (Band et al. 2006). Resilient employees will be less impacted by the setbacks, but disaffection may still occur (Seligman 2012). The (purple) balancing feedback loop, *B2,* shows that as the organizational social network grows, there is a greater need for constraints on employee behavior in the form of policies and rules. Research has shown that dense social networks at the aggregate level lead to norm enforcement (Kadushin 2012, page 184) (Glanville and Bienenstock 2009). In many ways, such constraints help the social network operate more efficiently since assumptions about coworker behaviors can be made. Local rules and policies can only constrain the contextual rules and policies further. These rules and policies should be consistent with the contextual constraints, but may become burdensome, at least as perceived by the insider, and result in greater disaffection with the organization. The *B2* feedback loop may limit the growth of the insider's social capital and engagement within the organization, and be a source of disconnection for the insider. This disconnection may be the cause of the insider turning to the adversary, which we will discuss in the next section.

5.2 Adversary and Family Social Capital

Figure 4 describes the aspects that grow the insider's social capital with the adversary, which is based on a subset of the primary mechanisms underlying growth of the organizational social capital. The feedback loops *R1b* and *B1b* reflect the growth and limits to growth in the adversary social network that were described in *R1a* and *B1a* in the victim organizational social network. The adversary social network, except for colluding insiders, will not be as interconnected and may be more ephemeral than the organizational social networks, just because the nature of the relationship between the insider and the adversary is a covert activity that both sides will be very cautious with, at least in the early stages. As shown in the lower left of Figure 4, the insider's incentive to spy is influenced by the insider's ideological motivation, financial desperation, and coercion. The link with organizational disaffection will be made in the next section.

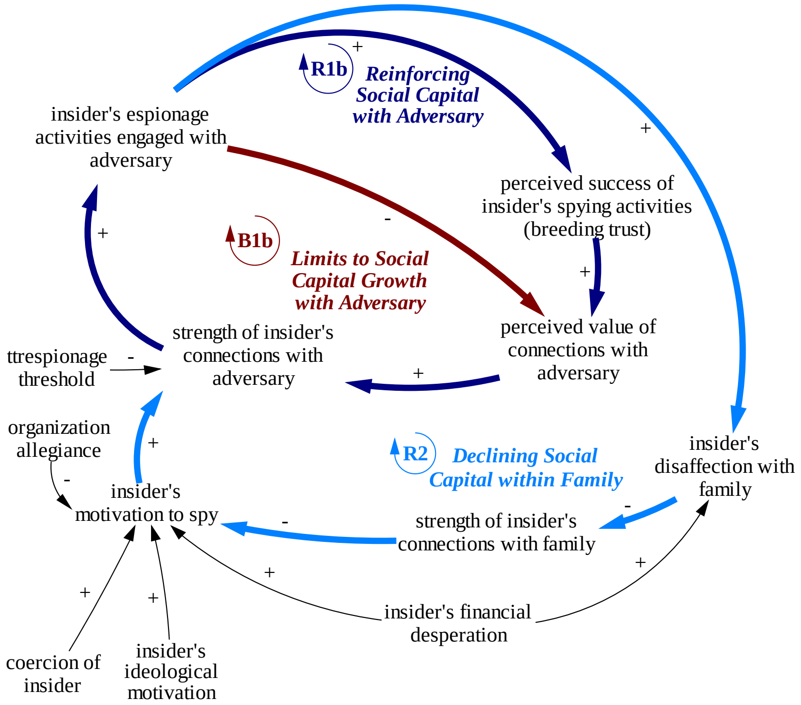

insider's espionage activities engaged with adversary
R1b
Reinforcing Social Capital with Adversary
+
+
perceived success of insider's spying activities (breeding trust)
-
B1b
Limits to Social Capital Growth with Adversary
+
+
perceived value of connections with adversary
ttrespionage threshold
-
strength of insider's connections with adversary
+
organization allegiance
-
+
insider's motivation to spy
R2
Declining Social Capital within Family
insider's disaffection with family
-
-
strength of insider's connections with family
+
+
insider's financial desperation
+
+
coercion of insider
insider's ideological motivation

Figure 4: Adversary and Family Social Capital

As shown in the (light blue) reinforcing feedback loop *R2*, the insider's financial desperation also has a negative influence on the strength of the insider's connections with family, creating its own incentive to spy. The reinforcing aspect of this dynamic is that, as the insider spies, it creates additional stress on the insider and weakens the connections even further. While not all families will respond this way to financial desperation, we hypothesize that this desperation is the cause behind many of the spies' disaffection with family that we see in the incidents.

5.3 Pulling It All Together

Figure 5 shows the primary interconnections between the submodels described in the previous two sections. As alluded to previously, the insider's disaffection with the organization influences the insider's incentive to spy, as shown in the bottom middle of Figure 5. As discussed previously, the motivation variables are somewhat independent, reflecting the fact that spies can have multiple motivations. However, the bipolar nature of these motivations are reflected in the simulation model discussed later.

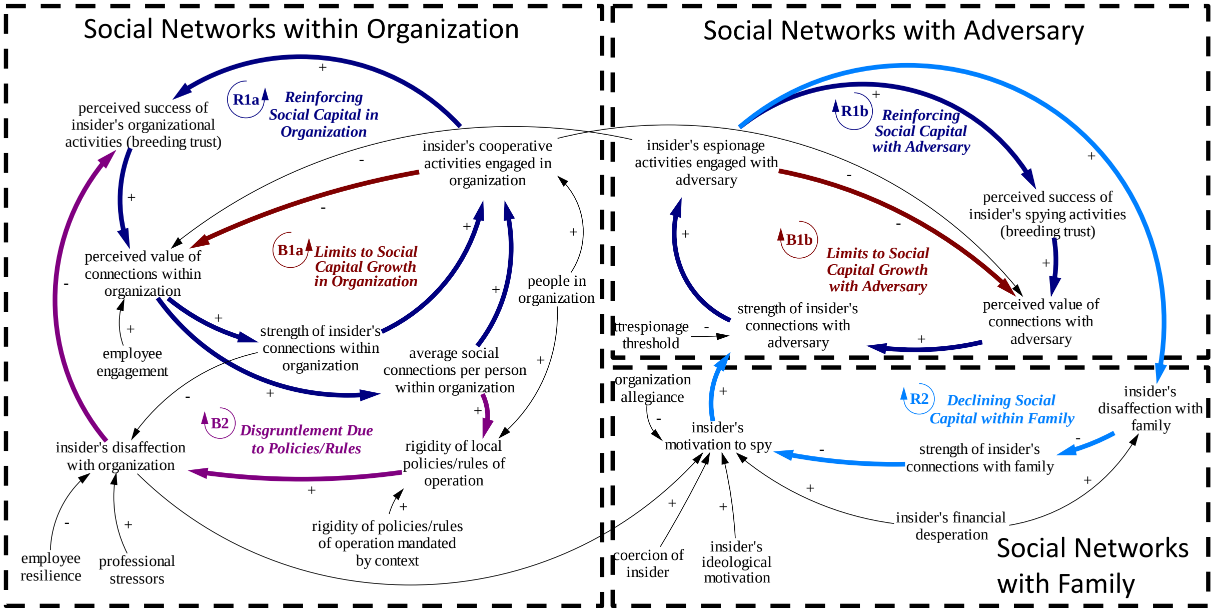

Social Networks within Organization
R1a
Reinforcing Social Capital in Organization
perceived success of insider's organizational activities (breeding trust)
insider's cooperative activities engaged in organization
B1a
Limits to Social Capital Growth in Organization
perceived value of connections within organization
people in organization
strength of insider's connections within organization
employee engagement
average social connections per person within organization
B2
Disgruntlement Due to Policies/Rules
insider's disaffection with organization
rigidity of local policies/rules of operation
rigidity of policies/rules of operation mandated by context
employee resilience
professional stressors
Social Networks with Adversary
R1b
Reinforcing Social Capital with Adversary
insider's espionage activities engaged with adversary
perceived success of insider's spying activities (breeding trust)
B1b
Limits to Social Capital Growth with Adversary
ttrespionage threshold
strength of insider's connections with adversary
perceived value of connections with adversary
organization allegiance
R2
Declining Social Capital within Family
insider's disaffection with family
insider's motivation to spy
strength of insider's connections with family
insider's financial desperation
coercion of insider
insider's ideological motivation
Social Networks with Family
+
-

Figure 5: Social Capital Transfer Causal Loop Diagram

The crossing influences between the two submodels in the middle of Figure 5 reflect the assumption that keeping up the social connections within the organization makes it harder to keep up the connections with the adversary and vice versa. Thus, the growth in either domain is limited by the activity going on in the other domain.

6 Simulation Modeling and Analysis

The causal loop diagram presented above is an abstraction of the system dynamics simulation model on which our analysis is based, which is shown in Appendix B. Appendix C shows an abstract interface for interacting with the model. The causal loop diagram simplifies various aspects of the simulation model for ease of presentation and understanding. For example, the causal loop diagram refers abstractly to the strength of social network connections. Dudley's original model uses the number of connections as the basis for social capital accumulation. (Dudley 2004) In addition to connection count, we also track the strength of dyadic, interpersonal connections, referred to as "ties" in the literature. (Marsden and Campbell 1984)(Marsden and Campbell 2012)(Friedkin 1990) This combinations forms what we call the "insider's composite connection strength" in the simulation model.

The simulation model that we describe here is a preliminary model in the sense that it is a vision of what we expect to find in our research, not the actual findings themselves. We continue to refine and ground the model on future research. Nevertheless, the current model is exhibiting certain aspects of the incidents that we have studied and common sense attributes that one would expect these incidents to possess. For example, the current model shows that while a medium level of motivation in a single dimension is not enough to spur espionage, a high level of motivation is. In addition, a medium level of motivation across orthogonal motivational attributes can spur espionage (e.g., a medium level of disaffection as well as medium ideological motivation). As in Stone's analysis previously described, real incidents can be spurred by multiple motivations across the two axes.

6.1 Working Hypotheses

Based on our previous experience analyzing social networks of various individuals and groups, we identified four working hypotheses that are the subject of our research. While these hypotheses may be refined based on our ongoing modeling and analyses, this section describes our current understanding of these hypotheses, including possible measures for their evaluation and initial support based on past work and established theory.

Hypothesis 1) The strength of the spy's social network connections with non-colluders in the organization is low (compared to the average employee) and generally decreases through time.

Weak connections with others in the organization may indicate that the insider has less to lose through spying, or less of a perceived obligation to the organization and coworkers, and therefore may promote spying as an alternative. In addition, Ronald Burt reported that dense networks facilitate sanctions (possibly through improved detection/deterrence of wrongdoing) because there are more people who can “act in concert against someone who violates their norms of conduct” (Burt 2000).

With regard to the specific incidents studied, Walker was generally well regarded at work (Hunter 1999, 25–26)(Barron 1987, 61–62, 173) and socialized with coworkers when off duty. He was careful to cultivate individuals useful to him; at the same time, his marriage was deteriorating and his relations with his wife and children were abusive. He was able to cultivate a series of friends throughout his life and kept some degree of contact with his extended family (Earley 1988). In contrast, Manning had trouble connecting with coworkers and regarded his entry into the military as a mistake almost immediately. He completed basic training on the second try, but despite desirable technical skills then in short supply, his commanders considered leaving him behind when the unit deployed to Iraq. Manning’s sexual orientation reportedly alienated him from his fellow soldiers. His family relationships were troubled, although he did develop relationships outside the military and his family (Nicks 2012).

Our preliminary model reflects the downward trend in the organizational social network of someone who starts spying. Figure 6 through Figure 8 shows this trend for the number of connections the insider has with others in his social network, interpersonal tie strength, and composite connection strength measures. The composite measure is simply the product of connection count and the tie strength. These measures of the insider’s connection with others are represented as array variables, one for each the organization (org), the adversary (adv), and the family (fam).

This simulation was generated with the follow settings:

insider’s allegiance to the US = 0.4

insider’s disaffection with organization = 0.5

insider’s financial desperation = 0.5

espionage threshold = 0.25

With these settings, the espionage began at about month 36, as illustrated in the graph, upon the rise of the social network connections with the adversary. As shown in Figure 4, the other input to the insider’s motivation to spy - the strength of the insider’s connections to family - is an endogenous variable whose value depends on disaffection due to financial desperation and the stress of spying.

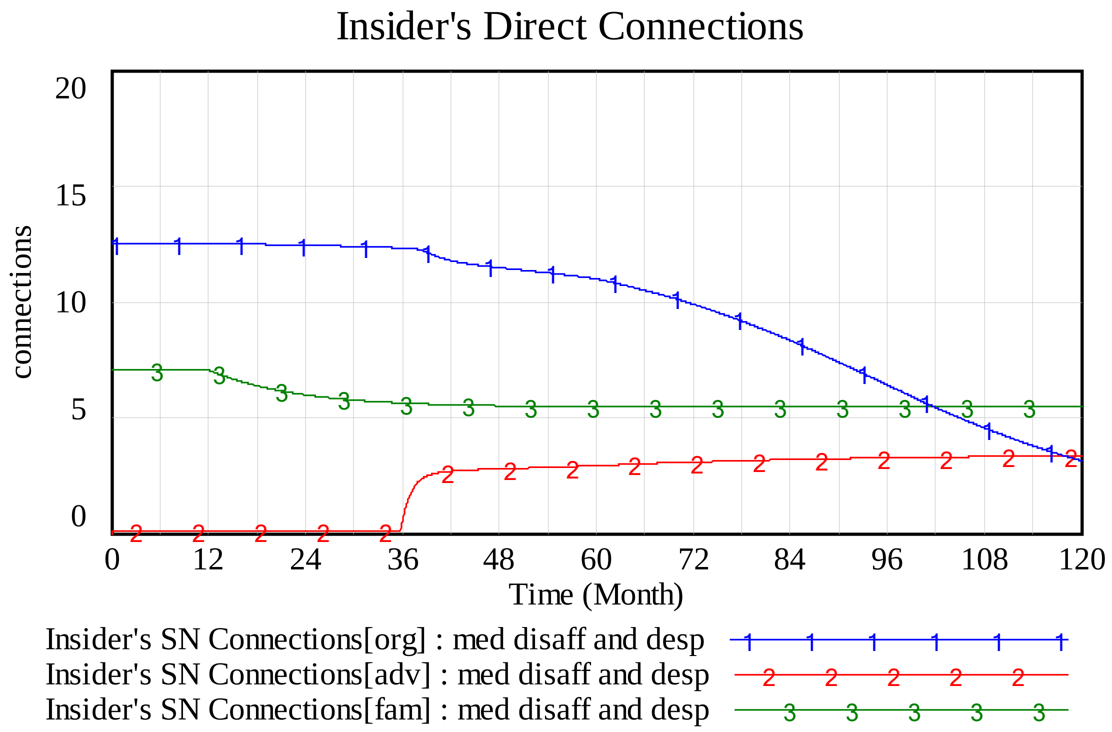


Figure 6: Connection Count with Medium Disaffection and Desperation

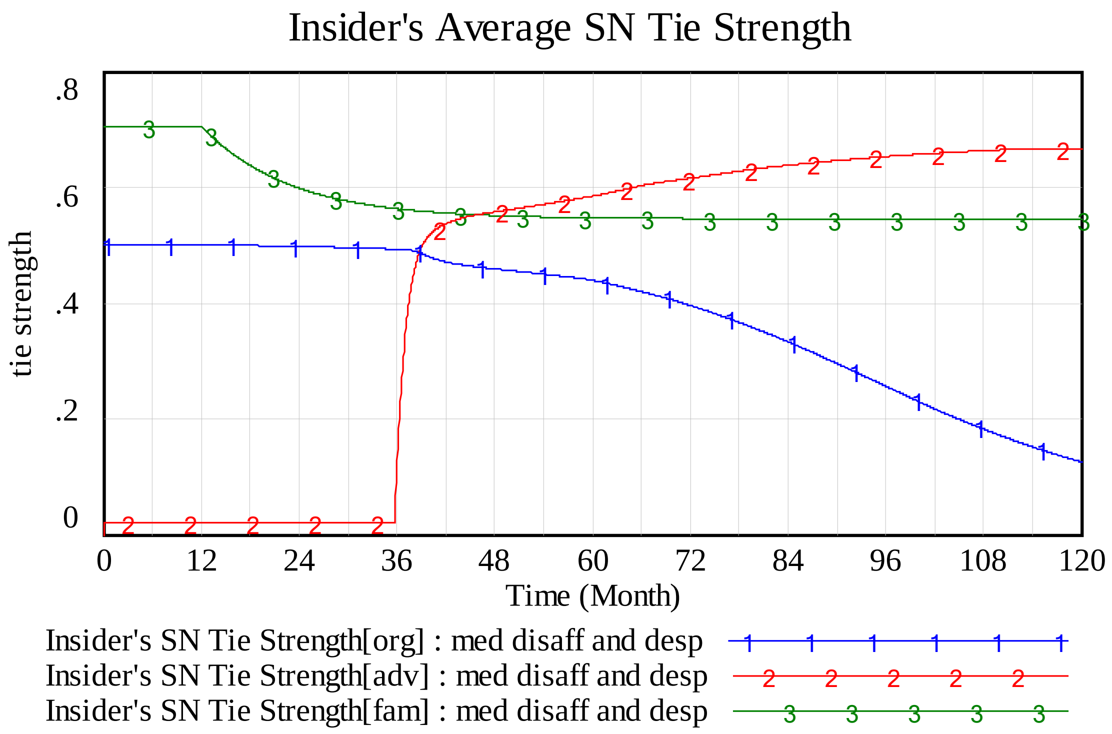


Figure 7: Social Network Tie Strength with Medium Disaffection and Desperation

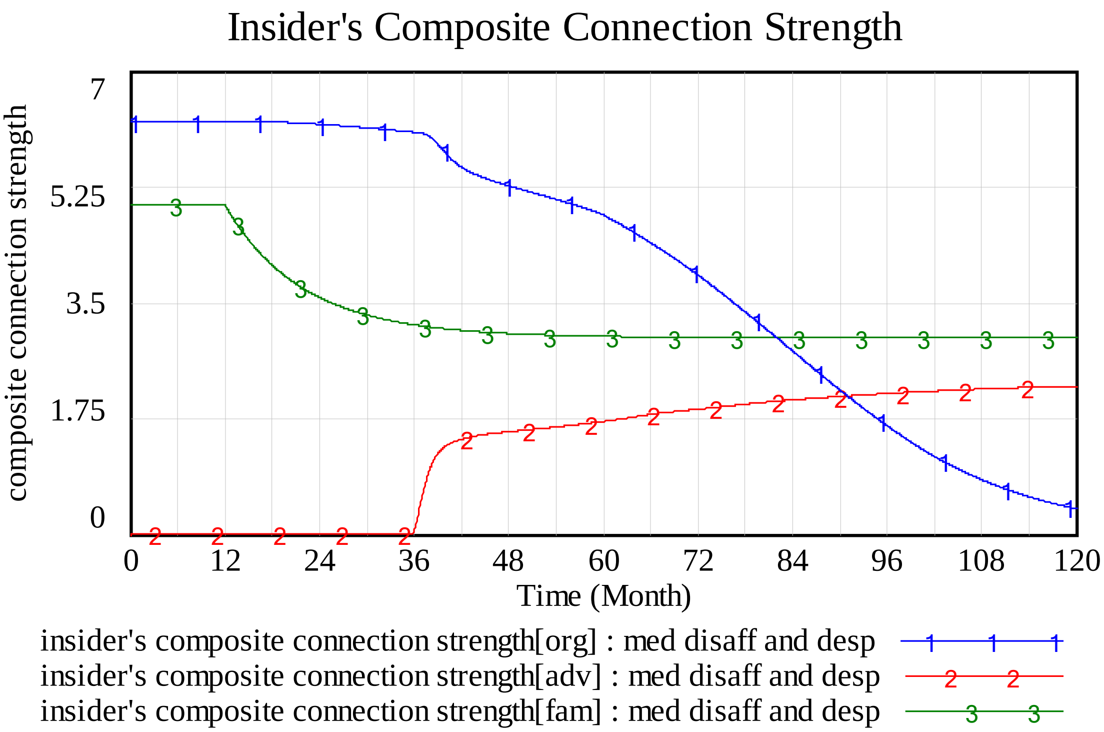


Figure 8: Composite Connection Strength with Medium Disaffection and Desperation

Hypothesis 2) The social network connections between the spy and the adversary will generally grow stronger, but may be ephemeral.

We expect the social network that the spy has with the adversary will grow, but will plateau fairly early on to keep a relatively low profile from U.S. authorities. This social network may be ephemeral both from the perspective of substitutions of contacts that the spy has with the adversaries, as well as possibly on-again, off-again spying activity. However, once the spy starts spying, the adversary will always have a "stick" to keep them going.

We see two patterns for espionage, based on the two case studies. Walker's espionage was a connection with a disciplined adversary who aimed to preserve their source by

- limiting contacts to dead drops within the U.S. augmented by occasional face-to-face meetings abroad
- strictly controlling knowledge about the contact

The initial connections were face-to-face (Walker simply walked into the Soviet Embassy with follow-up meetings in the Washington, D.C. area), but thereafter the contacts were restricted. However, the flow of cash payments, notes, and occasional personal contacts were aimed at supporting relatively good feelings, even through periods of strain when the information flow or payment amounts were at issue (Earley 1988; Prados 2010). In Manning's case, his contacts with the hacker community were undisciplined (in the espionage sense) and played out in an environment where information and access to information were both entrée and demonstrations of worth. Manning initiated and cultivated his contacts as a social network, reinforcing his sense of self-worth. Because Manning’s arrest followed fairly quickly after he started spying, it is difficult to determine the trajectory of the network over time (Fishman 2011).

With regard to the simulation model, the graphs in Figure 6 through Figure 8 show the social network connection between the insider and the adversary increasing for about the first three months upon the start of the espionage. This increase is not surprising given that the starting point of the simulation was established to be when there were no connections with the adversary. While this increase is not necessarily the case in all incidents, it is fairly common. Another relevant measure is the ratio of the social network connections to the total number of connections as shown in Figure 9 with the same settings as for Figure 6 through Figure 8. The sharp rise in the ratio of the adversary to organization social connections commences first with the rise of connections with the adversary at month 36 and later with the collapse of the insider’s social network with the organization at about month 78. Also note that spies are exploiting the "structural holes" between the competitor and the organizational social networks, and thus may gain a sense of power through that exploitation (Coleman 1988).

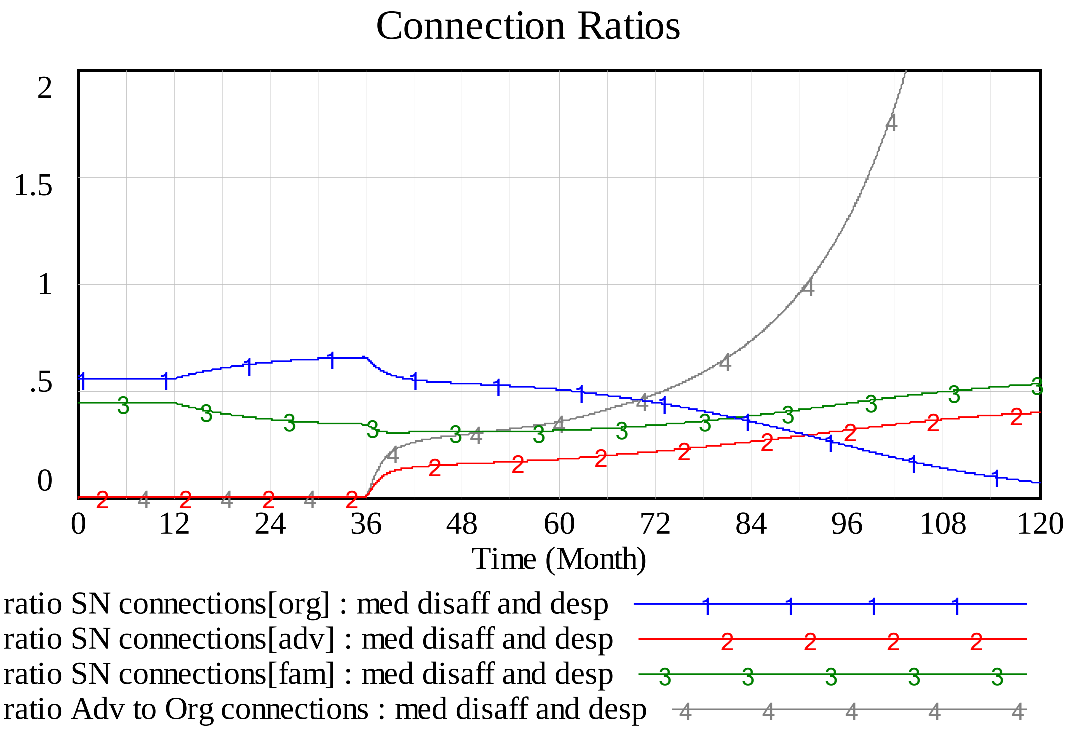


Figure 9: Ratio of Social Network Connections with Medium Disaffection and Desperation

Hypothesis 3) The strength of the spy's social network connections with family decreases during the early stages of spying, especially financially-motivated spying.

Figure 6 through Figure 8 shows the social network connection between the insider and his/her family decreasing at the point at which the equilibrium was perturbed with organizational disaffection and financial desperation. This behavior is consistent with findings of the disrupted family networks associated with criminals. In our case, the model assumes that the family is disrupted due to a financial crisis; the decision on the part of the insider to spy is to help resolve that crisis; and the stress due to the spying is likely to impact family relationships. There is still a fair degree of uncertainty regarding the strength of family connections for strictly ideological or disaffected spies.

In the two incident studies, both individuals came from troubled family backgrounds. In Walker's case, his entry to the military was engineered by his older brother as a way of helping him avoid criminal charges, although he generally did well in his U.S. Navy career as an enlisted man and warrant officer. For a period of time, Walker was optimistic about his marriage and family, but this optimism rapidly deteriorated when his wife did not meet his demands and expectations. Still, when Walker initiated spying, and particularly after his wife became aware of this fact, further stress was placed on an already troubled relationship (Earley 1988). In Manning's case, monetary reward did not figure as an important motivation in his turn to espionage.

Hypothesis 4) The strength of the spy's social network connections increases among the colluders, if any.

Colluders include those who help the subject spy and may work for the victim organization (insider colluders) or third parties (outsider colluders), but are not part of the adversary organization. We have not modeled colluders as a distinct subgroup in our current modeling efforts. We expect to expand the model in this direction as we find out more. We expect this working hypothesis to hold as it has in analyses in similar domains (e.g., Enron insiders formed a densely connected subgroup (Diesner, Frantz, and Carley 2005)).

In the incident studies, Walker cultivated two kinds of insider contacts: one with his Soviet paymasters and the other with members of his personal spy ring. In the former case, tradecraft and Soviet espionage techniques limited contacts, and the third-party Soviet connection was always subject to tension and fear (although the Soviets went to some pains to curry Walker's favor and feed his vanity through written and face-to-face contacts). Walker's home-grown network centered on Walker and reflected his approach of identifying people useful to him and manipulating them to his needs. This manipulation could take the form of friendship, but Walker's demands and the stress of espionage tended to break down the cultivated connections over a period of time. However, it is notable that a great many individuals knew with reasonable certainty that Walker was a spy but did not communicate this information to authorities (although his ex-wife eventually did so) (Earley 1988; Earley 2014; Barron 1987).

In the Manning incident, he did not have colluders inside his workplace (the military) but did cultivate contacts in the hacker community using his access to information as a means of forging contacts. An ill-judged contact with a publically known hacker was the immediate cause of Manning's arrest. Given the potential legal consequences of his contacts, much debate and discussion has occurred about how much Manning's contacts in the hacker community influenced his decision to reveal secret information (versus self-motivation) (Nicks 2012).

6.2 Possible Uses of the Model

Indicators that might be derived from our research in sociotechnical network analyses are, of course, a major source of detection controls. Low levels of social capital combined with suspicious information flows are likely to be a good source of early indicators with relatively low levels of false positives. Employee privacy will be a major concern for organizations wishing to use such indicators to monitor employee behavior. We believe that the details of these indicators and the extent to which they can be used while preserving employee privacy rights will be managed with continued progress in our research, but perhaps the greatest potential for reducing the insider threat is by disincentivizing employees using management strategies to increase employee job engagement (Adler and Kwon 2002)(Ellinger et al. 2013). This proactive, preventative approach improves employee satisfaction, productivity, and organization performance, as well as (probably) reduces the insider threat.

How effectively these approaches reduce the threat will require long- term study, but this approach is important and often overlooked in an environment where existing insider threat controls may have negative unintended consequences associated with their use as well as unknown effectiveness. Of course, deterrence of insider threat is a more often prescribed strategy by insider threat experts, but we distinguish disincentivization from deterrence. Deterrence involves the use of a "stick" (e.g., punishment for violations of an acceptable use policy), whereas disincentivization of the threat involves approaches that benefit the employee as much as the organization. The former is in place in case the insider acts or is tempted to act maliciously, while the latter is more about setting up the conditions under which the insider would never consider acting maliciously.

We can increase the level of engagement virtually in our model to test the potential effectiveness of approaches proven to improve employee engagement. A recent survey indicates that the following organizational practices are key to improving employee engagement (TinyHR 2014):

- showing employee appreciation and recognition
- fostering a positive work culture
- mapping professional growth plans
- recruiting collegial, hard-working colleagues
- hiring managers that are truly (transformational) leaders
- empowering employees with tools to succeed
- enabling peer recognition

Of course, the quality of relationships among co-workers is important (Ryan and Deci 2000)(Shuffler, DiazGranados, and Salas 2011) as is social capital generally (Ellinger et al. 2013) (Fishbein and Ajzen 1975).

Employee engagement is currently linked into the model in a way that influences the insider's perceptions regarding the value of the organization's social network connection in the causal loop diagram of Figure 3 and the stock and flow diagram in Figure 11 of Appendix B. This simple influence (not affected at all by likely feedback from other parts of the model) increases employee engagement and simply delays the onset of the espionage without addressing the underlying cause. Additional future research is necessary to understand and model the feedback effects on employee engagement to assess the likely impacts more realistically. An important example of such effects are the alignment of management style with employee motivational focus (Higgins 2005)(Higgins 2006)(Brockner and Higgins 2001)(Johnson, Chang, and Yang 2010). The resilience of employees is also important so that natural employee engagement is not undermined by personal and professional setbacks and disappointments (Seligman 2012)(Reivich and Shatte 2003)

7 Conclusion

This paper describes a model of insider espionage social networks based on our preliminary analysis of two espionage incidents. Clearly, no firm conclusions can yet be drawn and much work remains in the areas of analysis of additional incidents and comparison data of the average employee. The model that we present in this paper will surely change, perhaps a great deal, as we continue our research. Nevertheless, it provides a useful "stake-in-the-ground" and vision for our future efforts.

We continue to make progress analyzing the social networks of actual espionage incidents. Simultaneously, we are analyzing the social networks using a large email corpus of an assumed-normal population, representative of organizations in the espionage cases. The email corpus, while limiting the medium of communication, provides a way to easily construct a baseline level of communication for an organization over time. Additionally, it is possible to build a large number of social networks for everyone in the organization. These social networks can be used to compare the social networks among employees, especially for changes over time. This analysis will also be useful for determining the significance of changes in the spy incident social networks. Lastly, this analysis will provide a more granular timeframe for the analysis of employee social networks.

8 Acknowledgements

The authors would like to thank Randy Trzeciak and Sandy Shrum for their reviews and editing of this paper, and to Bill Claycomb and Craig Lewis for their ongoing collection and preparation of the comparison data.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0002179

References

Adler, Paul S., and Seok-Woo Kwon. 2002. "Social Capital: Prospects for a New Concept." *The Academy of Management Review* 27 (1): 17.

Andersen, David, Andrew P. Moore, Jeffrey M. Stanton, Eliot Rich, Elise A. Weaver, Jose J. Gonzalez, Jose Maria Sarriegui, Paseo Manuel De, Aldo Zagonel, and Mohammad Mojtahedzadeh. 2004. "Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem." In *Proceedings of the International Conference of the System Dynamics Society*.

Band, Stephen R., Dawn M. Cappelli, Lynn Fischer, Andrew P. Moore, Eric Shaw, and Randall F. Trzeciak. 2006. "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis." Software Engineering Institute Technical Report CMU/SEI-2006-TR-026.

Barron, John. 1987. *Breaking the Ring: The Bizarre Case of the Walker Family Spy Ring*. Boston, MA: Houghton Mifflin Company.

Brockner, Joel, and E. Tory Higgins. 2001. "Regulatory Focus Theory: Implications for the Study of Emotions at Work." *Organizational Behavior and Human Decision Processes* 86 (1): 35–66. doi:10.1006/obhd.2001.2972.

Burkett, Randy. 2013. "An Alternative Framework for Agent Recruitment: From MICE to RASCLS." *Studies in Intelligence* 57 (1): 7–17.

Burt, Ronald S. 2000. "The Network Structure of Social Capital." *Research in Organizational Behavior* 22: 345–423.

Cappelli, Dawn M., Akash G. Desai, Andrew P. Moore, Timothy J. Shimeall, Elise A. Weaver, and Bradford J. Willke. 2007. "Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks." ADA468801. Defense Technical Information Center (DTIC). http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA468801.

Cappelli, Dawn M., Andrew P. Moore, and Randall F. Trzeciak. 2012. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley.

Chan, Marjorie. 2003. "Corporate Espionage and Workplace Trust/Distrust." *Journal of Business Ethics* 42 (1): 45–58.

"Chelsea Manning." 2015. *Wikipedia, the Free Encyclopedia*. http://en.wikipedia.org/w/index.php?title=Chelsea_Manning&oldid=642114007.

Coleman, James S. 1988. "Social Capital in the Creation of Human Capital." *The American Journal of Sociology*.

Colwill, Carl. 2009. "Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days?" *Information Security Technical Report*, Human Factors in Information Security, 14 (4): 186–96. doi:10.1016/j.istr.2010.04.004.

Diesner, Jana, Terrill L. Frantz, and Kathleen M. Carley. 2005. "Communication Networks from the Enron Email Corpus 'It's Always about the People. Enron Is No Different.'" *Comput. Math. Organ. Theory* 11 (3): 201–28.

Dudley, Richard G. 2004. "The Dynamic Structure of Social Capital: How Interpersonal Connections Create Communitywide Benefits."

Earley, Pete. 1988. *Family of Spies: Inside the John Walker Spy Ring*. New York, NY: Bantam Books.

———. 2014. “Boris Solomatin Interview.” *Crime Library*. Accessed December 8. http://www.crimelibrary.com/terrorists_spies/spies/solomatin/1.html.

Ellinger, Alexander E., Carolyn (Casey) Findley Musgrove, Andrea D. Ellinger, Daniel G. Bachrach, Ayşe Banu Elmadağ Baş, and Yu-Lin Wang. 2013. “Influences of Organizational Investments in Social Capital on Service Employee Commitment and Performance.” *Journal of Business Research*, Recent Advances in Globalization, Culture and Marketing Strategy, 66 (8): 1124–33. doi:10.1016/j.jbusres.2012.03.008.

Federal Bureau of Investigation. 2014. “The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy.” *FBI*. September. http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat.

Fishbein, Martin, and I. Ajzen. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, Mass: Addison-Wesley Pub.

Fishman, Steve. 2011. “Bradley Manning’s Army of One.” *New York Magazine*, July 3. http://nymag.com/news/features/bradley-manning-2011-7/.

Forrester, Jay Wright. 1961. *Industrial Dynamics*. M.I.T. Press.

———. 1969. *Urban Dynamics*. M.I.T. Press.

———. 1971. *World Dynamics*. Wright-Allen Press.

Friedkin, Noah E. 1990. “A Guttman Scale for the Strength of an Interpersonal Tie.” *Social Networks* 12: 239–52.

Glanville, Jennifer L., and Elisa Jayne Bienenstock. 2009. “A Typology for Understanding the Connections among Different Forms of Social Capital.” *American Behavioral Scientist* 52 (11): 1507–30.

Granovetter, Mark. 1985. “Economic Action and Social Structure: The Problem of Embeddedness.” *American Journal of Sociology* 91 (3): 481–510.

Herbig, Katherine L. 2008. “Changes in Espionage by Americans, 1947-2007.” PERSEREC Technical Report 08-05. Defense Personnel and Security Research Center (PERSEREC). https://www.scribd.com/doc/192035027/Katherine-L-Herbig-Changes-in-Espionage-by-Americans-1947-2007-Technical-Report-08-05-Northrop-Grumman-March-2008.

Higgins, E. Tory. 2005. “Value from Regulatory Fit.” *Current Directions in Psychological Science* 14 (4): 209–13. doi:10.1111/j.0963-7214.2005.00366.x.

———. 2006. “Value from Hedonic Experience and Engagement.” *Psychological Review* 113 (3): 439–60.

Hirschi, Travis. 1969. *Causes of Delinquency*. University of California Press.

Hunter, Robert. 1999. *Spy Hunter: Inside the FBI Investigation of the Walker Espionage Case*. Annapolis, MD: Naval Institute Press.

INSA. 2013. “A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector.” Intelligence and National Security Alliance. http://www.insaonline.org/i/d/a/b/InsiderThreat_embed.aspx.

Johnson, Russell E., Chu-Hsiang (Daisy) Chang, and Liu-Qin Yang. 2010. “Commitment and Motivation at Work: The Relevance of Employee Identity and Regulatory Focus.” *Academy of Management Review* 35 (2): 226–45.

Kadushin, Charles. 2012. *Understanding Social Networks: Theories, Concepts, and Findings*. New York: Oxford University Press.

Kermack, W. O., and A. G. McKendrick. 1927. “A Contribution to the Mathematical Theory of Epidemics.” *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 115 (772): 700–721. doi:10.1098/rspa.1927.0118.

Kraemer, Sara, Pascale Carayon, and John Clem. 2009. “Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities.” *Computers & Security* 28 (7): 509–20. doi:10.1016/j.cose.2009.04.006.

Lee, Siew Kim Jean, and Kelvin Yu. 2004. “Corporate Culture and Organizational Performance.” *Journal of Managerial Psychology* 19 (4): 340–59.

Lim, Bernard. 1995. “Examining the Organizational Culture and Organizational Performance Link.” *Leadership & Organization Development Journal* 16 (5): 16–21.

Magklaras, G. B., and S. M. Furnell. 2005. “A Preliminary Model of End User Sophistication for Insider Threat Prediction in IT Systems.” *Computers & Security* 24 (5): 371–80. doi:10.1016/j.cose.2004.10.003.

Marsden, Peter V., and Karen E. Campbell. 1984. “Measuring Tie Strength.” *Social Forces* 63 (2): 482–501.

———. 2012. “Reflections on Conceptualizing and Measuring Ties Strength” 91 (1): 17–23.

Martinez-Moyano, Ignacio J., Eliot Rich, Stephen Conrad, David F. Andersen, and Thomas R. Stewart. 2008. “A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach.” *ACM Transactions on Modeling and Computer Simulation (TOMACS)* 18 (July): 2.

Meadows, Donella H. 2008. *Thinking in Systems: A Primer*. Edited by Diana Wright. White River Junction, VT: Chelsea Green Publishing.

Melara, C., J.M. Sarriegi, J. Gonzalez, A. Sawicka, and D.L. Cooke. 2003. “A System Dynamics Model of an Insider Attack on an Information System.” In *Proceedings of the International Conference of the System Dynamics Society*.

Moore, Andrew, P., Dawn M. Cappelli, H. Joseph, and Randall F. Trzeciak. 2007. “An Experience Using System Dynamics to Facilitate an Insider Threat Workshop.” *Proceedings of the International Conference of the System Dynamics Society*.

Morecroft, John. 2007. *Strategic Modelling and Business Dynamics: A Feedback Systems Approach*. John Wiley & Sons.

Nicks, Denver. 2012. *Private: Bradley Manning, WikiLeaks, and the Biggest Exposure of Official Secrets in American History*. Chicago, IL: Chicago Review Press.

Ogbonna, Emmanuel, and Lloyd C. Harris. 2000. “Leadership Style, Organizational Culture and Performance: Empirical Evidence from UK Companies.” *The International Journal of Human Resource Management* 11 (4): 766–88.

O’Reilly, Charles A., Jennifer Chatman, and David F. Caldwell. 1991. “People and Organizational Culture: A Profile Comparison Approach to Assessing Person-Organization Fit.” *Academy of Management Journal* 34 (3): 487–516.

Petty, M. M., N. A. Beadles, Christopher M. Lowery, Deborah F. Chapman, and David W. Connell. 1995. “Relationships between Organizational Culture and Organizational Performance.” *Psychological Reports* 76 (2): 483–92. doi:10.2466/pr0.1995.76.2.483.

Prados, John. 2010. “The Navy’s Biggest Betrayal.” *Naval History Magazine* 24 (3). http://www.usni.org/magazines/navalhistory/2010-06/navys-biggest-betrayal.

Reivich, Karen, and Andrew Shatte. 2003. *The Resilience Factor: 7 Keys to Finding Your Inner Strength and Overcoming Life’s Hurdles*. Reprint edition. New York: Harmony.

Royds, J. 2009. “Virtual Battlefield.” *CIR Magazine*.

Ryan, Richard M., and Edward L. Deci. 2000. “Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being.” *American Psychologist*, 68–78.

Schneier, Bruce. 2012. *Liars and Outliers: Enabling the Trust That Society Needs to Thrive*. Wiley. http://www.barnesandnoble.com/w/liars-and-outliers-bruce-schneier/1104530608.

Seligman, Martin E. P. 2012. *Flourish: A Visionary New Understanding of Happiness and Well-Being*. Reprint edition. New York: Atria Books.

Shaw, E. D., J. M. Post, and K. G. Ruby. 1999. “Inside the Mind of the Insider.” *Security Management* 43 (12): 34–44.

Shuffler, Marissa l., Deborah DiazGranados, and Eduardo Salas. 2011. “There’s a Science for That: Team Development Interventions in Organizations.” *Current Directions in Psychological Science - CURR DIRECTIONS PSYCHOL SCI* 20 (6): 365–72.

Sterman, John D. 2000. *Business Dynamics: Systems Thinking and Modeling for a Complex World with CD-ROM*. Boston: McGraw-Hill/Irwin.

Stone, LeRoy A. 2001. “A Two-Factor Motivational Theory for Spying Behavior.” *Psychology of Espionage Reports* 2.

TinyHR. 2014. “The 7 Key Trends Impacting Today’s Workplace: Results from the 2014 TINY Pulse Employee Engagement and Organizational Culture Report.” Survey Results and Recommendations. TinyHR. http://www.tinyhr.com/2014-employee-engagement-organizational-culture-report.

Torsvik, Gaute. 2000. “Social Capital and Economic Development a Plea for the Mechanisms.” *Rationality and Society* 12 (4): 451–76.

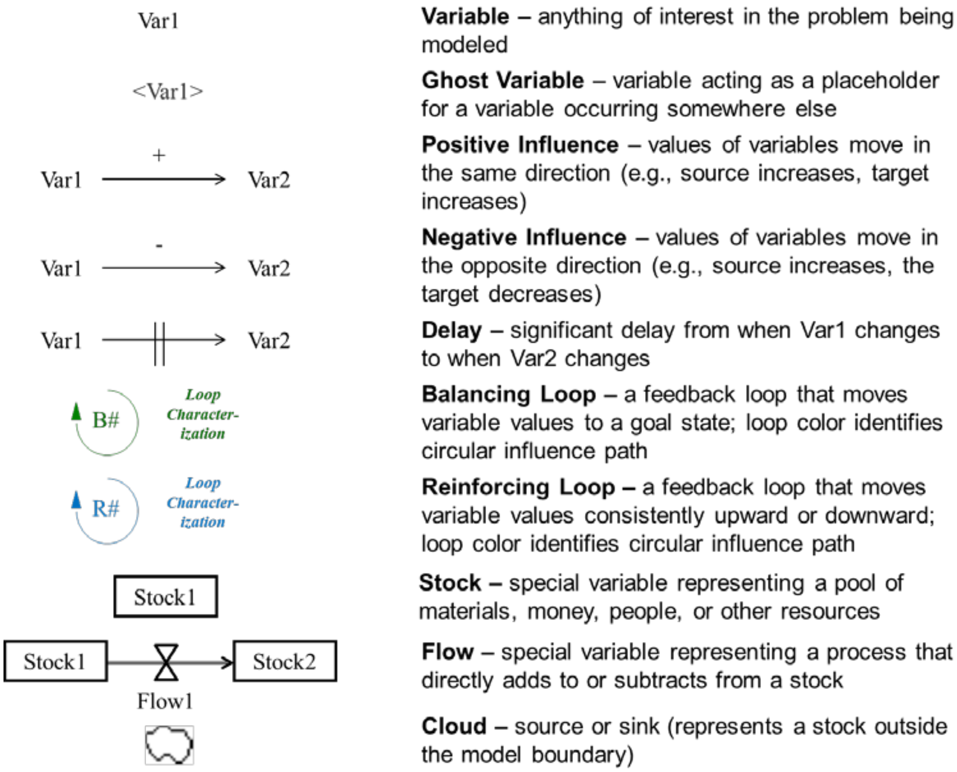
Appendix A: System Dynamics Modeling

A common form of computational model is a system dynamics model. System dynamics helps analysts model and analyze critical behavior as it evolves over time within complex socio-technical domains. System dynamics models (Forrester 1961) have been used to model a variety of complex socio-technical systems, such as population growth and resource depletion (Forrester 1969), epidemics (Kermack and McKendrick 1927), and business dynamics (Forrester 1971; Sterman 2000; Morecroft 2007). In these models, the system is represented in terms of stocks and flows and the feedback loops and time delays that effect change in the stocks.

Specifying a system dynamics model starts by describing a high-level structure of how the system behaves and adding more detail to each component iteratively. It requires that those constructing the model know, or have hypothesized, how the system behaves in the real world. System dynamics models, because they promote thinking about causal mechanisms and the interplay between the engineered and the social environment, are ideal for reasoning about insider threat. Prior work has used causal loop diagrams to describe the nature of the insider threat problem (Cappelli, Moore, and Trzeciak 2012) (Andersen et al. 2004) and system dynamics simulation models to assess the risk of insider cyber sabotage threat (Cappelli et al. 2007)(Melara et al. 2003). Still, other system dynamics models have focused on training, attention, and judgment (Martinez-Moyano et al. 2008)(Moore et al. 2007) for mitigating threat. In none of these models has the position of the insider in the social networks, connecting colluders, family, the organization, and the recipients, been examined.

Figure 10 summarizes the notation used by system dynamics modeling. The primary elements are variables of interest, stocks (which represent collection points of resources), and flows (which represent the transition of resources between stocks). Signed arrows represent causal relationships, where the sign indicates how the variable at the arrow's source influences the variable at the arrow's target. A positive (+) influence indicates that the values of the variables move in the same direction, and a negative (–) influence indicates that they move in opposite directions. A connected group of variables, stocks, and flows can create a path that is referred to as a feedback loop. System dynamics models identify two types of feedback loops: balancing and reinforcing. The type of feedback loop is determined by counting the number of negative influences along the path of the loop. An odd number of negative influences indicates a balancing loop; an even (or zero) number of negative influences indicates a reinforcing loop.

Significant feedback loops identified within a model are indicated by a loop symbol and a loop name in italics. Balancing loops—indicated with the label *B* followed by a number in the loop symbol—describe aspects of the system that oppose change, seeking to drive variables to some goal state. Balancing loops often represent actions that an organization takes to mitigate a problem. Reinforcing loops—indicated with the label *R* followed by a number in the loop symbol—describe system aspects that tend to drive variable values consistently upward or downward. Reinforcing loops often represent the escalation of problems, but may include problem mitigation behaviors.



Variable – anything of interest in the problem being modeled

Ghost Variable – variable acting as a placeholder for a variable occurring somewhere else

Positive Influence – values of variables move in the same direction (e.g., source increases, target increases)

Negative Influence – values of variables move in the opposite direction (e.g., source increases, the target decreases)

Delay – significant delay from when Var1 changes to when Var2 changes

Balancing Loop – a feedback loop that moves variable values to a goal state; loop color identifies circular influence path

Reinforcing Loop – a feedback loop that moves variable values consistently upward or downward; loop color identifies circular influence path

Stock – special variable representing a pool of materials, money, people, or other resources

Flow – special variable representing a process that directly adds to or subtracts from a stock

Cloud – source or sink (represents a stock outside the model boundary)

Figure 10: System Dynamics Notation

Appendix B: Simulation Model of Social Capital Transfer

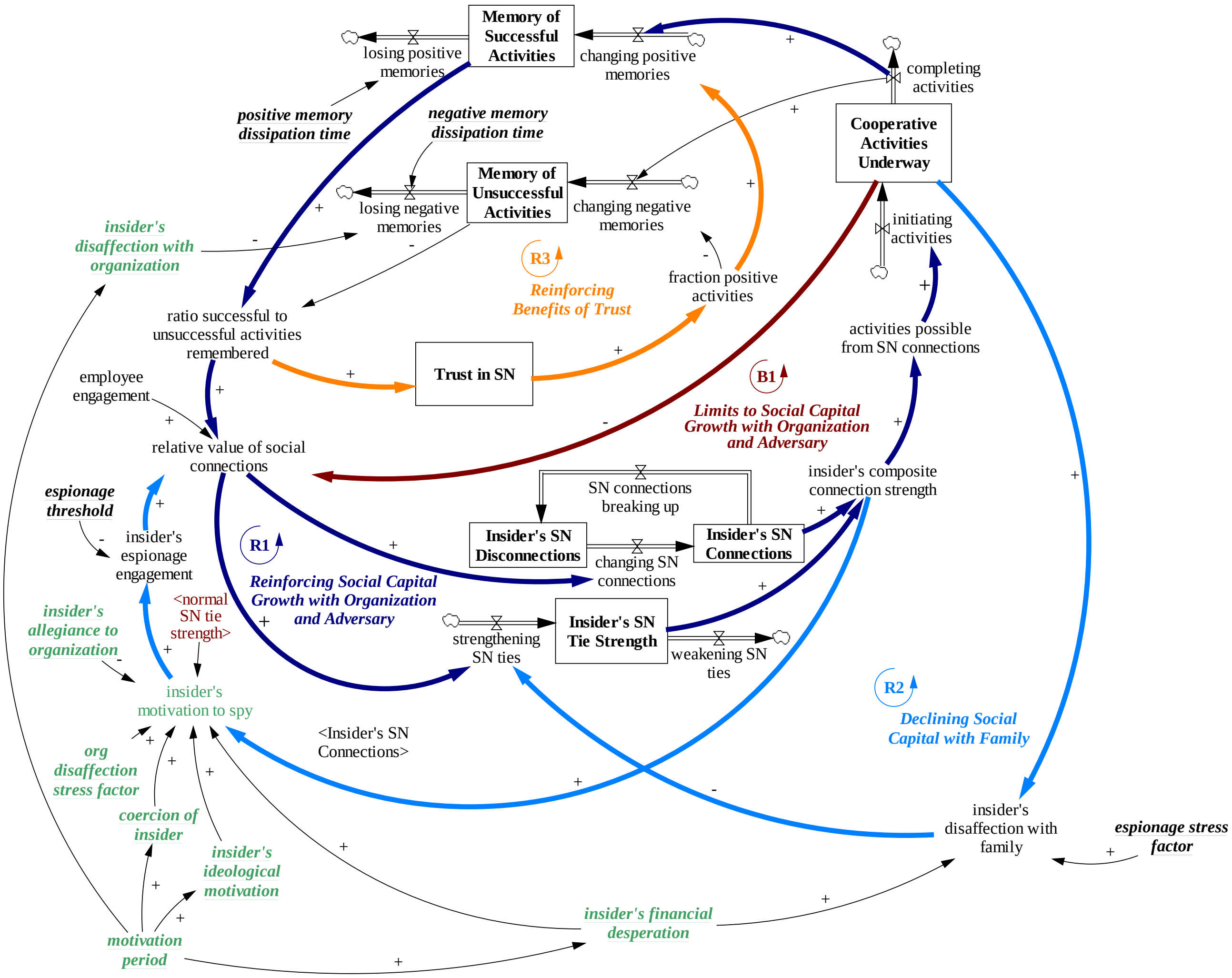
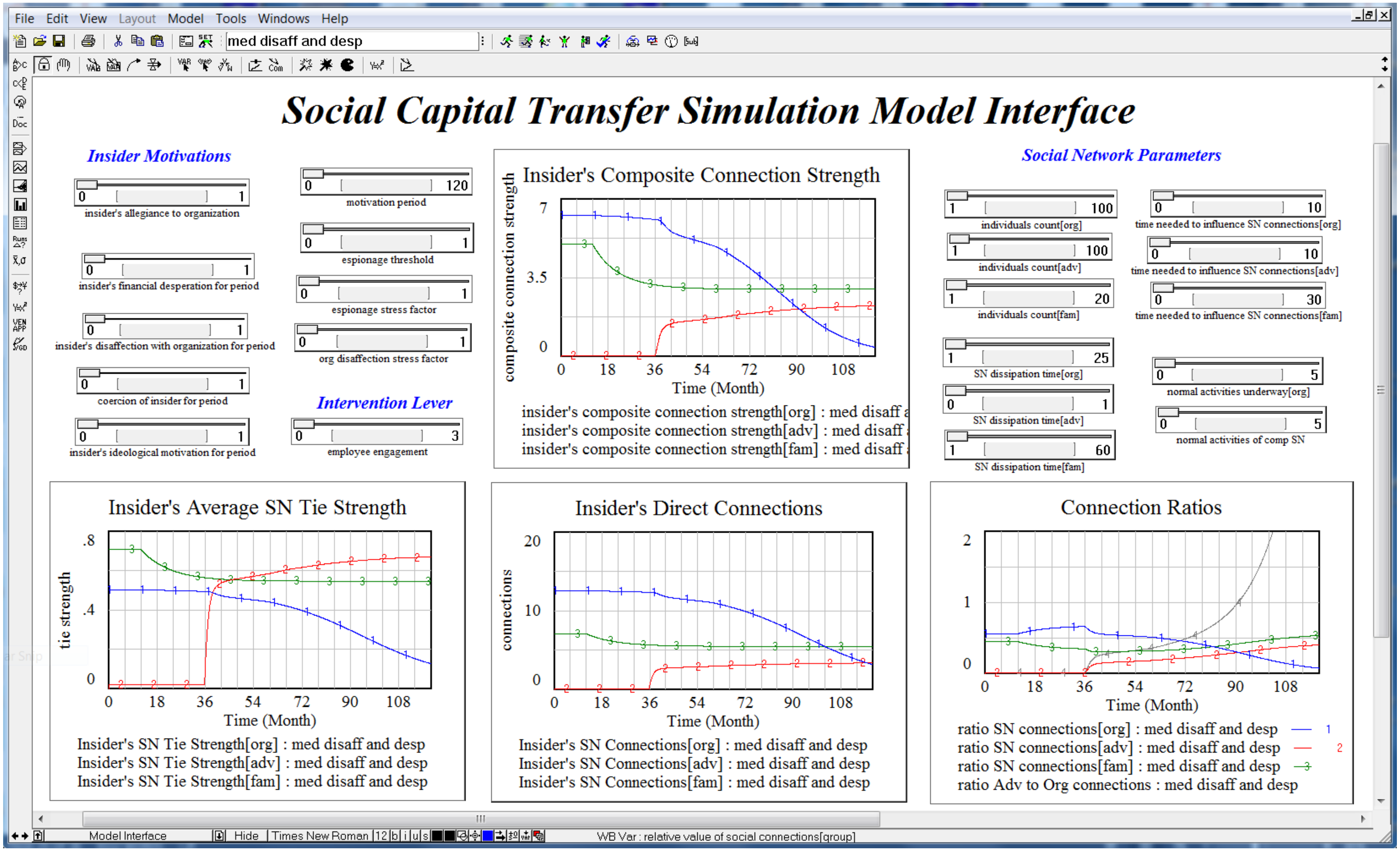

Memory of Successful Activities
losing positive memories
changing positive memories
completing activities
positive memory dissipation time
negative memory dissipation time
Memory of Unsuccessful Activities
losing negative memories
changing negative memories
Cooperative Activities Underway
initiating activities
insider's disaffection with organization
R3
Reinforcing Benefits of Trust
fraction positive activities
ratio successful to unsuccessful activities remembered
Trust in SN
activities possible from SN connections
employee engagement
B1
Limits to Social Capital Growth with Organization and Adversary
relative value of social connections
insider's composite connection strength
SN connections breaking up
espionage threshold
insider's espionage engagement
R1
Reinforcing Social Capital Growth with Organization and Adversary
Insider's SN Disconnections
changing SN connections
Insider's SN Connections
insider's allegiance to organization
<normal SN tie strength>
strengthening SN ties
Insider's SN Tie Strength
weakening SN ties
insider's motivation to spy
R2
Declining Social Capital with Family
<Insider's SN Connections>
org disaffection stress factor
coercion of insider
insider's disaffection with family
espionage stress factor
insider's ideological motivation
insider's financial desperation
motivation period
+
-

Figure 11: Simulation Model of Social Capital Transfer

Appendix C: Simulation Model Interface



File Edit View Layout Model Tools Windows Help
med disaff and desp
Doc
Model Interface
Hide
Times New Roman
12
b
i
u
s
WB Var : relative value of social connections[group]

Social Capital Transfer Simulation Model Interface

Insider Motivations

0 1 insider's allegiance to organization

0 1 insider's financial desperation for period

0 1 insider's disaffection with organization for period

0 1 coercion of insider for period

0 1 insider's ideological motivation for period

0 120 motivation period

0 1 espionage threshold

0 1 espionage stress factor

0 1 org disaffection stress factor

Intervention Lever

0 3 employee engagement

Social Network Parameters

1 100 individuals count[org]

1 100 individuals count[adv]

1 20 individuals count[fam]

1 25 SN dissipation time[org]

0 1 SN dissipation time[adv]

1 60 SN dissipation time[fam]

0 10 time needed to influence SN connections[org]

0 10 time needed to influence SN connections[adv]

0 30 time needed to influence SN connections[fam]

0 5 normal activities underway[org]

0 5 normal activities of comp SN

Insider's Composite Connection Strength
composite connection strength
7
3.5
0
0 18 36 54 72 90 108
Time (Month)
1
2
3

insider's composite connection strength[org] : med disaff a
insider's composite connection strength[adv] : med disaff a
insider's composite connection strength[fam] : med disaff a

Insider's SN Tie Strength[org] : med disaff and desp
Insider's SN Tie Strength[adv] : med disaff and desp
Insider's SN Tie Strength[fam] : med disaff and desp

Insider's SN Connections[org] : med disaff and desp
Insider's SN Connections[adv] : med disaff and desp
Insider's SN Connections[fam] : med disaff and desp

ratio SN connections[org] : med disaff and desp 1
ratio SN connections[adv] : med disaff and desp 2
ratio SN connections[fam] : med disaff and desp 3
ratio Adv to Org connections : med disaff and desp

Figure 12: Simulation Model Interface