Beyond Security: A Data Quality Perspective on Defensive Information Warfare

Peter Kaomea, Information Consulting Company
Susan Hearold and Ward Page, Navy Command Control and Ocean Surveillance Center
Research and Development Division*

Abstract

Conventional approaches to defensive information warfare (IW) focus primarily on physical security, electronic countermeasures and encryption techniques. These areas focus on preserving system availability and data secrecy. However, these areas control only a small subset of the range of impacts that information warfare attacks can have on information data quality attributes provided to users. For example, subtle changes to information timeliness, accuracy and credibility can have significant impact on military command and control yet pass undetected through standard computer security safeguards.
In this paper, we take an information quality perspective to investigate how compromises to information quality can propagate through a data flow with implications for operational users. We describe a capability to help the IW warrior predict the propagation of corrupted data and it's meta-data quality attributes through a complex information system. This capability can have a significant impact on command and control operations.

*This paper is the opinion of the authors and should not be construed as having the concurrence or endorsement of their agencies.

1. Introduction

The revolution in military affairs has elevated the role of information in military operations to center stage. Information is now a primary instrument in national power. In response to the challenges posed by the increasing power of information and information systems, Information Warfare is emerging as a major new area of conflict. The first official directive on information warfare is Department of Defense Directive TS3600.1, "Information Warfare," 21 December 1992. This document provided a definition, but Information Warfare stakeholders are still hotly debating its meaning and scope. One working definition provided by the Office of the Assistant Secretary of Defense (C3I) is "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending oneís own information, information-based processes, information systems and

computer-based networks.." Dr. Frederick Cohen, SAIC, provided another more general, and perhaps more powerful, definition of information warfare. Beginning with dictionary definitions of information and warfare he defines Information Warfare as ìthe role of symbolic representations in conflict between opposing forces.î

The purpose of this paper is to frame defensive information warfare in terms of protecting data quality. It will be shown that information warriors are handicapped by the imprecision of current terminology to specify expected and desired defensive states and that data quality concepts can provide for more precise attack assessment and security targeting. An information warrior system architecture for providing this capability is described.

2. Operational Need

One warfare goal is to decrease the enemy's ability to wage war. Successfully bombing a runway will immediately reduce the enemyís short term ability to get planes in the sky. Bombing the water supply to a base will not affect its immediate capabilities, but is likely to reduce the staying power of its forces. If such attacks cannot be prevented by defensive measures, they must be quickly detected, and recovery measures initiated as quickly as possible.

The defense of information systems requires similar measures, but providing them is often much more complex. Information systems tend to have more layers of abstraction and more interdependencies between nodes. Some attacks are easily detected and their implications readily understood. However, many types of attacks are very difficult to detect until the consequences are noted from effects that have rippled through the information network to another component or location. Even when an attack is detected, it is often difficult to track it to its source. Additionally, it can be very difficult to understand all the implications of such an attack. Just as bombing attacks on physical assets have an impact and blast zone, information attacks can also be thought of as having an initial information impact and corresponding secondary information effects (see Figure 1). A method is needed for rapidly assessing the implications of an information attack. In this paper we discuss a framework and system for automatically performing this analysis.

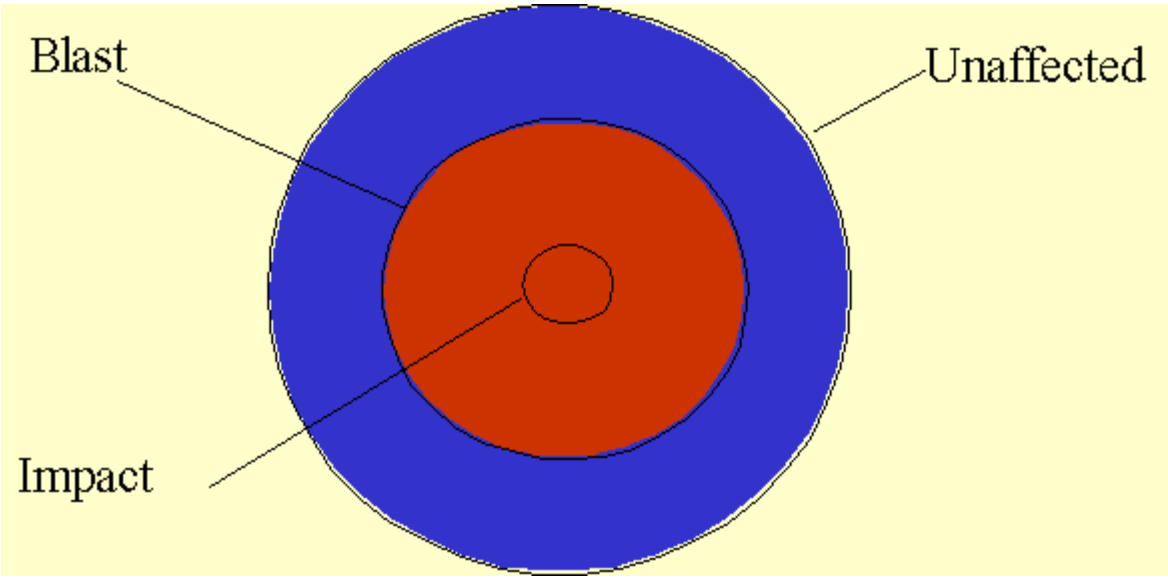

Figure 1. Information Blast Zone

3. Background

The National Institute of Standards and Technology (NIST) and the Organization for Economic Co-operation and Development (OECD), among others, provides assistance in securing computer-based resources. A NIST handbook and OECD guidelines provide a broad overview of computer security and the selection of appropriate security controls. Common threats include: errors and omissions, fraud and theft, employee sabotage, loss of physical and infrastructure support, malicious hackers, industrial espionage, malicious code, and foreign government espionage. This paper deals with the impact of those threats that alter data and thus data quality attributes.

One set of technical tools are those that can identify system vulnerabilities. Many are available on the internet. One highly publicized tool is ìSATANî, Security Administrator Tool for Analyzing Networks.

Another set of tools tests for intrusions and misuse. (Misuse refers to actions by people who have access to a system for specific tasks, but are performing functions or accessing data which exceed their authority.) Currently most intrusions and misuse are identified by smart security administrators who use audit data to identify anomalies in system and user behavior patterns. Tools are available to assist in analyzing the audit data by incorporating security rules and checking for violations and by checking for changes in behavioral trends. An example of one commercial tool to assist in these analyses is Computer Misuse Detection System (CMDS) by

SAIC. Such tools identify the specific behavior, e.g. requesting root access, but do not attempt to predict the consequences of a successful break-in.

In practice, most of these tools and techniques are useful for supporting off-line risk analysis, designing security systems and procedures, and identifying computer misuse. However, none attempts to address the effects of information attacks on information quality and the potential for widely distributed consequences.

Defensive information warfare, framed as data quality states and changes to data quality clarify security attributes that currently are ignored or ambiguous. Typically security guidance specifies that the goal of information protection is to maintain availability, integrity, and confidentiality.

ï Availability, meaning accessible for use, is also an important data quality attribute. The attack on availability is denial of services. Even short eclipse of service can reduce the effectiveness of communications, weapon systems, and command and control.

ï Integrity is a security term for an information system that has not been tampered with, i.e. corrupted. Corruption causes information systems to make decisions they were not originally designed to make. Current automated information systems have little or no integrity protection and thus are susceptible to viruses, Trojan horses, errors etc. To say a system is corrupted leads to the next, more interesting question: What is the alteration?-- Is the data accuracy reduced? Is the data precision reduced? Is the data timeliness reduced? These are data qualities of interest to information warfare.

ï Confidentiality is ability to make information available only to those expressly given access and out of sight of all others. Leakage, unfortunately, is a common phenomena. Confidentiality is the inverse of availability. Confidentiality reducing availability of our information to our enemies. The data quality attribute of availability will capture the meaning of leakage or confidentiality.

4. Organization of Paper

To explain the unique contribution of data quality concepts, a Scud missile attack during Desert Storm is used as the military operational context. Key Scud missile-related events are presented in the Scenario section of this paper. Then data quality concepts are defined, their relationships specified and propagation rules developed. An architecture is then described for a system to support the information warrior in analyzing information attacks in terms of changes in data quality attributes. A summary of the contribution of a data quality framework applied to defensive information warfare concludes the paper.

5. Scenario

Desert Storm often proved that the image becomes the reality. The war on CNN was televised in real-time. Thus the narrow focus and random selection of the unfiltered, real-time images distorted the true scope and nature of events. What was really known about the enemyís relative strengths and weaknesses was often erroneously-shaped by television.

A murderous dictator of a fifth-rate country is put on the same plane as the democratically elected President of the most powerful nation on Earth. The perception of invincibility was so strong however, that many well-informed Americans really believed that the ìelite republican guardsî would make the US forces ìswim in a river of bloodî in the ìMother of All Battles.î

Saddam Hussein attacked our sense of vulnerability by using it to send a message of terror to the Israeli people via Scud missile attacks and threats of gas warfare to the US press. On day two of the war, as Israel came under Scud attack, CNN went live to its Jerusalem Bureau showing the bedlam of newsmen who believed they were being gassed, trying to don gas masks, earpieces and microphones simultaneously, while the camera bucked and panned wildly. They were completely wrong about the gas attack, but the perception scared the watching public.

Israeli officials responded to the Scud attacks with threats of military retaliation. Pressure from the Israeli government and from graphic imagery of Scud missiles hurtling toward Israeli population centers can be viewed as information attacks on the US. The US government controls this information attack with information controls. One shaping event was of a Scud being intercepted by Patriots over Israel at night. More important militarily was the shelling of Khafji, but reality was skewed because there was more action, drama and suspense in the Scud tape.

First attempts at countering Scuds were to try to knock them out of the air with a Patriot missile after Iraq fired them. The Patriot missile guidance radar increased the availability of launched missile data. Then direct linkage of the radar to the missiles increased the timeliness with which the data reached the missile guidance. And a local radar aboard the Patriot missile increased the precision of target location data.

Attempts were also made to visually find and destroy Scud launchers on the ground. Saddam decreased the availability of Scud visual location data by hiding his missiles and moving them only at night. He would move them frequently to decrease the timeliness of Scud location data to the US forces. The US response was to use F-16ís equipped with radar and infrared sensors provided availability of radar and infrared imagery of the missiles even in the dark. Saddam decreased the accuracy of this data by deploying a host of decoys with similar radar and IR signatures.

Scud ìeyes and earsî were attacked by eliminating scud radar, relays and telecommunication links. Scud ìbrainsî were attacked when the US used Saddamís centralized command and control against him by cutting communication links between himself and his troops, leaving the Scud operators to plan alone.

6. Concepts

To fight a war of information, it is useful to conceptualize the assets being protected are data units and their associated data qualities.

6.1 Definitions

Vulnerabilities

Vulnerabilities are specific events which can potentially result in a change in the quality of a unit of data. A system may be vulnerable to events initiated by attackers, accidents, improper use by legitimate users, system failures, etc. As will be shown later, a particular vulnerability can imply other vulnerabilities. In the Desert Storm example cited above, the US was vulnerable to Saddamís propaganda because he had unfiltered access to US news cameras which could rapidly spread his messages and to US reporters who had much to gain by presenting sensational footage of the war.
Such a vulnerability is modeled as follows:

Vulnerability Description	unfiltered access to US news cameras & US reporters
Data Unit	message
Data Quality	availability increase to world
	credibility increase to world
	accuracy decrease to world
	relevance misrepresentation to world

Attacks

An attack is the attempted exploitation of vulnerabilities. The instantiation of an attack is the signal that an attack has actually occurred and that the consequences of the corresponding vulnerability could potentially be realized. Saddam Hussein attempted to exploit the US press vulnerabilities when he released threats and statements of his strength. This increased the availability of his inaccurate message of invincibility. In launching Scud missiles at night with non-nuclear or gas warheads, Saddam was not only launching a physical attack, but more importantly he was launching an information attack. He was sending a message of terror in order to increase the credibility of this threats. By exploiting the US press, he was able to spread terror and influence behavior.

These attacks are modeled as an attempt to exploit a known vulnerability:

	threats of invincibility via press
Attack Description	televised launching of SCUD missiles
Vulnerability Description	unfiltered access to US news cameras & US reporters

Controls

The condition which could prevent the realization of effects is a control to protect a given vulnerability from a particular attack.. The US tried to decrease the credibility of Saddam's message of terror by releasing pictures of Patriot missiles deployed to stop the Scud's. This control was heightened by sensational pictures of Patriots intercepting Scud's in flight.

A control is modeled as a defensive measure to help detect, prevent, or recover from a specific attack on a specific vulnerability:

Control Description	message of competent defense via Patriot imagery
	threats of invincibility via press
Attack Description	televised launching of SCUD missiles
Vulnerability Description	unfiltered access to US news cameras & US reporters
Control Effect	decreased credibility of Saddam's threats and ability to spread terror

Exposures

An exposure occurs when a vulnerability is attacked, but there is no control. Thus, an exposure results from a successful attack. Before the US could control the attacks launched by Saddam, it was exposed to the spread of inaccurate data concerning Saddam's ability to project terror. The televised images were highly credible, and highly relevant.

Exposure Description	message of Saddam's ability to project terror inaccurate highly credible apparently relevant
Attack Description	threats of invincibility via press launching of SCUD missiles which were televised
Vulnerability Description	unfiltered access to US news cameras & US reporters

6.2 Relations (Facts)

Framing information vulnerabilities, attacks, and exposures in terms of their effects on data qualities adds a useful perspective to information warfare, but does not in itself help to manage the information battlefield. It is necessary, as well, to understand the relations between data units, vulnerabilities, attacks, controls, and exposures. Some of the relations used to associate data units to one another are:

Aggregation	Data unit x is an aggregation of data unit y if and only if y is contained in or referenced by x.
Copy	Data unit x is a copy of data unit y if it x is a physically separate replication of y.
Function	Data unit x is a function of data unit y if and only if y is used along with an analytic method and possibly other data units to compute x.
Past / Future	Data unit relations are time sensitive. Any of the basic relations may therefore be augmented with a Past / Future descriptor which specifies whether the relation already exists, or whether it will exist in the future.

Figure 2 shows some of the physical communications links which allowed Saddam's message of terror to propagate much farther than the range of his missiles.

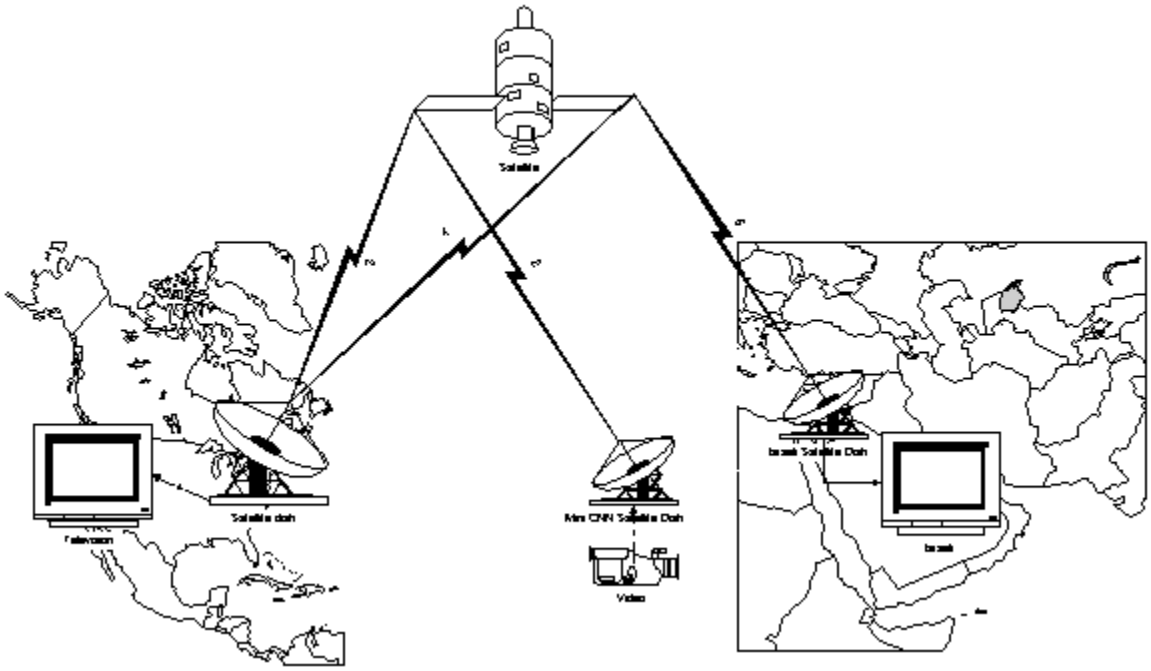

Figure 2. Example of Saddam Propaganda Communication Links

Figure 3 shows how data units can be aggregated to increase the credibility of the parts into a highly credible whole. In addition, the figure demonstrates how copies of data units can increase the availability of data across a region of interest.

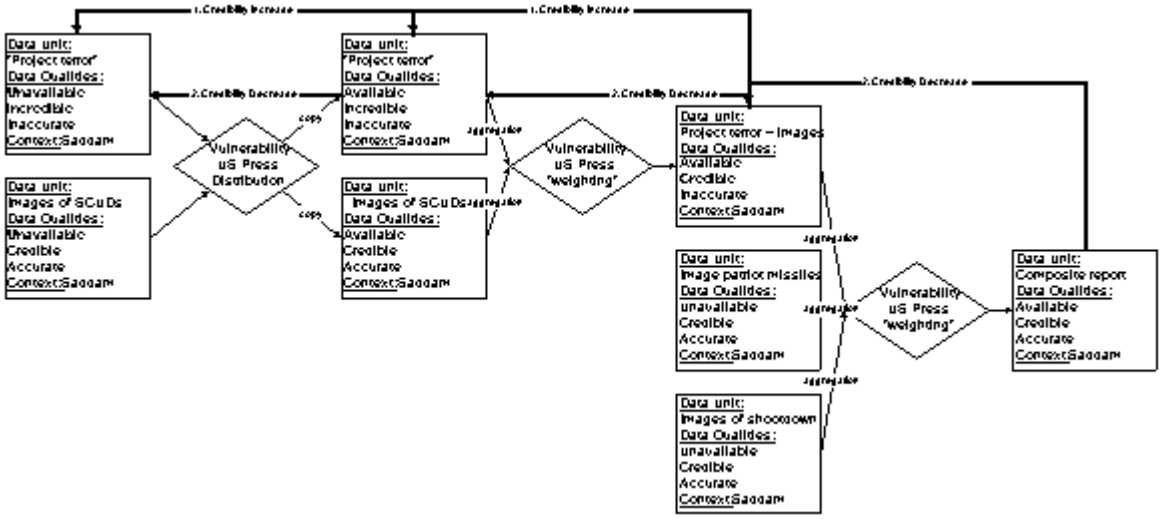

Figure 3. Relations of Data Units in Desert Storm Example

6.3 Propagation (Rules)

The complex interrelations of data units in even simple cases like Figure 3 enable the propagation of data qualities through the system. Vulnerabilities, attacks, controls and exposures are all described in terms of their real or potential effects on data qualities. Similarly, their effects can propagate through the system as a chain reaction of changes in data quality. This section presents a small sample of propagation rules used to determine the implications of a given attack on an information flow.

Vulnerability Propagation

Vulnerabilities which are known to apply to particular data units can automatically be deduced to apply to other units - depending on their interrelations. For example:

ï If a data unit is vulnerable to availability increase to the enemy, then each unit of which it is an copy is also vulnerable.

ï If a data unit is vulnerable to availability increase to the enemy, then each unit which is a copy of it is also vulnerable.

ï If the credibility of a data unit is increased, then each data unit which it is an aggregation of may also be vulnerable.

ï If a data unit is vulnerable to a decrease in timeliness, then every unit which is a future function of it is also vulnerable.

ï If a data unit is vulnerable to a decrease in accuracy, then each data unit which is a future function of it is also vulnerable.

In Figure 3, the arrows labeled "1. Credibility Increase" show how an aggregation of Saddam's statements and CNN imagery of Scud missiles streaking across the sky increased the credibility of Saddam's original boasts of being able to project terror in the "Mother of all battles." Also aware of the vulnerability of the press to exciting imagery, the US countered these attacks with pictures of Patriot missiles being deployed and video of the missiles intercepting Scuds. This had the effect of decreasing the credibility of Saddam's statements. This decrease propagated through both the aggregations and copies of data.

Exposure Propagation

In the example, both Saddam and the US exploited the existing vulnerabilities and the vulnerabilities which followed from the relations of the data units to one another. The resulting exposures worked first in favor of Saddam by increasing the availability and credibility of his message, then in favor of the US by decreasing the credibility of Saddam's message.

Some characteristic exposure propagation are listed below:

ï An exposure occurs if there is an attack on a vulnerability, but no control.

ï An exposure can cause further attacks.

ï An exposure can degrade the effectiveness of a control.

ï An exposure can cause further vulnerabilities.

Perhaps the most basic of these is that an exposure occurs given an attack on a vulnerability with no control. For our system this allows successful attacks to be distinguished from unsuccessful attempts. Also of interest, an exposure can cause further attacks. Consider, for example the increased availability to the enemy of a page of data when he exploits the vulnerability of data left in the trash by conducting a "dumpster diving" attack. This "attack" on the page of data is also an attack on all the units of data on the page of which it is an aggregation.

The basic premise of considering each of the propagation rules is that together they can flesh out the implications of attacks on a given information flow. It is important to note that different data qualities propagate differently through a data flow. Each must be considered separately.

7. System

7.1 System Architecture

The system is structured as shown in Figure 4. The processing center of the system is an inference engine with complementary fact and rule bases.

Error! No topic specified.

Figure 4. System Architecture

The fact base stores information about system hardware, software and data interdependencies as well as vulnerabilities of these assets. At run time, the fact base can receive updates to the basic structure of the system as well as updates concerning newly discovered or published vulnerabilities (as are typically published by CERT). These updates can be entered manually by users observing the situation, or automatically from system interrogators such as COPS or SATAN. Furthermore, knowledge concerning observed or detected attacks to the system infrastructure can also be entered as facts.

The rule base stores knowledge concerning the propagation of effects of changes in system structure, vulnerabilities, attacks or exposures throughout the rest of the system. A basic structure of the rule base as it affects the facts is shown in Figure 5. The fact types are shown with curved edges and the rule types are shown as rectangles. For example, at the center of the diagram is a type of "exposure" rule.

The diagram shows that an exposure results when an attack occurs on a vulnerability without a control. Under such conditions, an exposure rule actually generates a new exposure fact. The diagram also shows a rule "vulnerability" with a two way arrow to a class of fact vulnerabilities. This is to say that there are "vulnerability rules" that generate vulnerability facts. These rules are, in turn, dependent on vulnerability facts. For example, consider that a given frequency and modulation scheme are known to be vulnerable to jamming. There is a vulnerability rule which says that if a physical communication method can be jammed, then the message units which traverses the medium can be jammed. Consider further that a given message unit contains sub-units - as a file folder that contains many files. In this case, if a message folder is jammed, then all the data units which it contains are jammed. These examples demonstrate rules which can propagate the existence of a given vulnerability to others.

Figure 5. Fact / Rule Structure

Given the rules and facts the inference engine deduces the logical conclusions and implications of new vulnerabilities, attacks and exposures. These implications are communicated to the user via the user interface, and potentially to automated attack response systems. Users can also enter hypothetical situations - a "what if" capability - and check to see what the ultimate effects might be.

7.2 Entity Relationship (Structure of fact base)

The entity relationship diagram for the system is shown in figure 6. It is important to note that vulnerabilities, controls, exposures and attacks are each associated with a set of assets (data units for the pusposes of this discussion) and qualities. This is important since it forces all focus onto the effects as they relate to specific data quality changes.

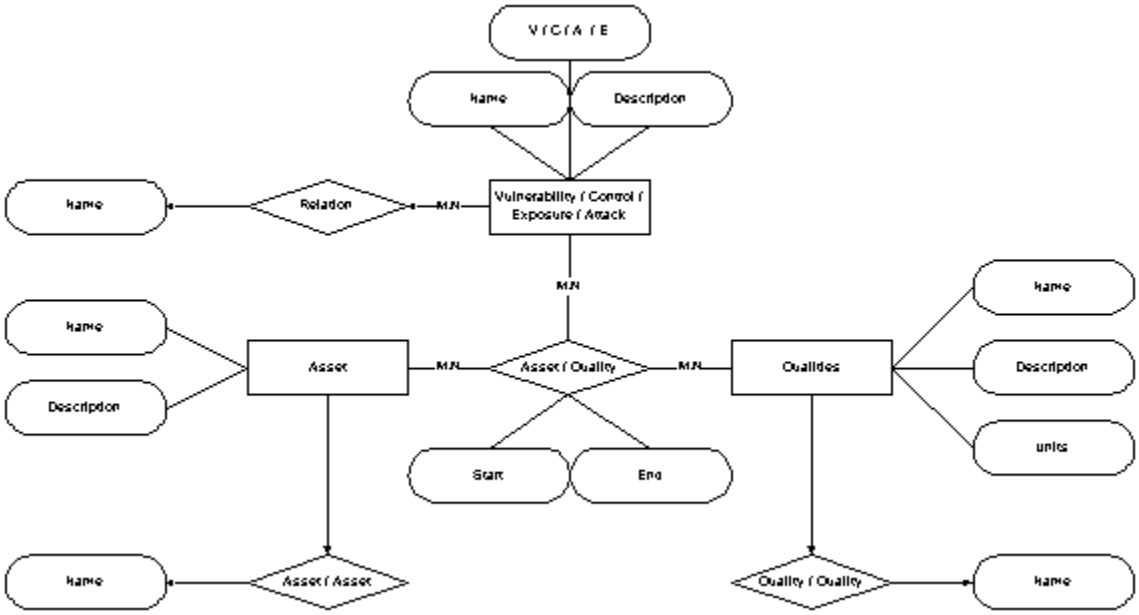

Figure 6. Entity Relationship

8. Summary

Defensive Information Warfare is the protection of our symbolic representations from denial, corruption and exploitation. Using Desert Storm Scud missile attacks as an operational context, this paper defined the data quality concepts of vulnerabilities, attacks, controls and exposures, and the relationship and propagation of data qualities among them. Then a system architecture incorporating these concepts was described. The resulting system would allow information warriors to more precisely understand the immediate and ripple effects of information attacks.