December 2006

Cyber-Emergencies: What Managers Can Learn From Complex Systems and Chaos Theory

Carlos Dorantes
The University of Texas at San Antonio

Alexander McLeod
The University of Texas at San Antonio

Glenn Dietrich
The University of Texas at San Antonio

Cyber-Emergencies: What Managers Can Learn From Complex Systems and Chaos Theory

Carlos Alberto Dorantes
The University of Texas at San Antonio
carlos.dorantes@utsa.edu

Alexander J. McLeod
The University of Texas at San Antonio
alexander.mcleod@utsa.edu

Glenn B. Dietrich
The University of Texas at San Antonio
glenn.dietrich@utsa.edu

ABSTRACT

Traditional analysis of events has used linear methods. This paper employs chaos theory to analyze cyber security events. It demonstrates that there might be an underlying pattern to seemingly random events. Determining this pattern can lead to a better understanding of what and when an event will occur.

Keywords

Cyber security, chaos theory, complexity theory, emergency management, managers

INTRODUCTION

Historically, linear principles popularized by Newtonian physics and Cartesian mathematics have directed the field of management. In addition, scientific problem solving strategies have been largely based on reductionism. Systems were viewed as linear, regardless of their level of complexity. These approaches to analyzing a situation worked well for static environments exhibiting little change. However, the modern competitive environment is anything but static and linear. Today's complex, non-linear systems can be studied using chaos and complexity theories, which focus on discovering order, structure, and patterns from chaotic behavior in complex systems. In this paper, we use Chaos Theory to shed some light on the potential of cyber disasters.

Chaos Theory is the study of unstable non-periodic behavior in deterministic non-linear dynamic systems. A dynamic system is a system in which the elements affect each other reciprocally and with time lags. Complexity Theory studies how complex systems can generate simple outcomes. For example, a human being can be considered a complex system composed of billions of cells working together in such a way that the body functions as a single unit performing simple as well as complex actions. Intensity in the interactions among the units is a characteristic of complex systems. Some authors consider Chaos Theory as an extension of Systems Theory while others consider Chaos Theory as part of Complexity Theory. Chaos Theory focuses more on finding an underlying order in the apparent disordered behavior of deterministic dynamic systems, while Complexity Theory covers a wider perspective involving the conception of the system, its elements, its complex interactions, and possible variety of behavior types.

Complexity Theory is comprised of four phases: stability, order, complexity and chaos(Battram, 1998). In the stability phase, inactivity reigns. In the order phase, predictable behavior exists. The complexity phase provides the greatest opportunity for affecting change. During this phase, systems may be nudged in certain directions, and chaos may potentially be averted. In

the final phase, chaotic behavior, there is no structure to support stability or order (Goulielmos, 2002). Cyber-disaster behaviors are chaotic states where management has difficulty dealing with the volume of requests for resources and existing policies and procedures do not support return to stability and order.

A cyber-emergency is defined as an acute event in which a significant infrastructure failure or reduction in service involving multiple complex interrelated systems affects people negatively (Dunlevy, 2003). Cyber-emergencies of such great disruption are typically reported to national level security agencies.

The U.S. Defense Advanced Research Projects Agency established the Computer Emergency Response Team Coordination Center (CERT/CC) to assist organizations in improving security. The CERT/CC provides alerts, advisories, and summaries of critical incidents, along with fixes and workarounds to serious security problems. Unfortunately, the occurrence of serious incidents appears unpredictable and chaotic in distribution (CERT/CC, 2003).

While cyber disasters have a low probability of occurring, when they do happen, they can have devastating consequences. This can be illustrated by looking at the financial services sector of the international economy. Wire transfer systems handle the majority of monetary exchanges using the Internet to accomplish these transactions. The sheer number of transfers is staggering. For example, in the U.S. the Fedwire Payment System moved $1.857 trillion dollars in 114.9 million transfers in 2004 (FRB, 2003). Imagine the impact of losing this vital function for an extended period. Even a reduction in capability, as the consequence of an Internet attack, would affect a large number of people throughout the world. Therefore, it is important to understand how and when cyber disasters might occur over time before preparing to effectively respond to such crisis.

If we accept that cyber disasters are erratic, unstable, and unpredictable then we assume that the systems are non-linear (Mainzer, 1994). Non-linear systems theory provides new insight into complex system behaviors previously thought to be chaotic (Priesmeyer and Cole, 1995). The non-linearity of cyber-crises makes them difficult to foresee, adding to managerial complexity.

Chaos theory delivers alternative frameworks for understanding interrelated elements in disastrous situations. These theories appear in a variety of areas including; disaster response management (Goulielmos and Giziakis, 2002; Koehler, 1995), strategic decision making (Richards, 1990), stock market behavior (Nawrocki, 1995). How management responds during disaster events may critically modify outcomes. Traditionally, policies and procedures establish standards for action. However, emergency response often requires action beyond tradition. The idea of matching "unstable" strategies to resolve instability in the environment stems from Complexity Theory (Kiel, 1995). The value found in application of complexity theory may be the generation of alternate views of difficult situations.

One of the characteristics of Chaos Theory is that small, seemingly unimportant changes or errors can alter the environment and lead to big changes or consequences. For example, a small amount of code in a web browser can lead to a significant exploitation of the network that can spread worldwide in a matter of days. All actions are interdependent within the system and therefore any action may affect the future of the system(Battram, 1998). Given the complex nature of cyber disasters, it can be assumed that their occurrence is not predictable using traditional methods.

The purpose of this paper is to examine cyber-disasters to determine if Chaos Theory would aid in understanding the occurrence of crises, and to attempt simulation of such events. Cyber disaster data from the CERT will be analyzed using the following several methods.

Two methods will be used for to diagnosis the data using Chaos Theory. The first method is called Rescaled Range (R/S) Analysis. This method is used to evaluate whether the time series data follows a totally random behavior, a persistent behavior or an anti-persistent behavior. These behaviors could be governed by underlying rules. The second chaos diagnostic method is called Lyapunov exponent. This method calculates a parameter that conveys information about the level of sensitivity of the system to initial conditions. Finally, a simple dynamic deterministic function will be used in an attempt to simulate the occurrence of cyber disasters over time.

METHODOLOGY

Data was collected from the online site of the 'United States Computer Emergency Readiness Team' (US-CERT, 2006). US-CERT is a partnership established in 2003 between the Department of Homeland Security and the public and private sectors. The purpose of this partnership is to protect the nation's Internet infrastructure from cyber attacks. Due to the sensitivity of the cyber attack data, only vulnerability reports were accessible. Although this data might or might not represent the behavior of cyber attacks, it can be argued that vulnerability reports convey information about the types of cyber attacks along with recommendations to minimize the probability of attacks against such weaknesses. Vulnerabilities reported by CERT are the best indicator we have regarding the types of cyber attacks launched on the Internet. These vulnerability reports are the result

of carefully analyzing different cyber incidents reported daily by organizations and individuals in the US. The cyber incidents are classified and organized by vulnerability type and recommendations to protect against possible attacks are issued. Therefore, it is assumed that vulnerabilities are signals of the persistency of cyber incidents such as virus, worms, intrusions, and other types of cyber attacks. The data below covers vulnerability reports from January 1997 to January 2006. Table 1 shows the frequency of reports by year.

Year	Number of Reports Published
1997	7
1998	10
1999	30
2000	90
2001	327
2002	304
2003	225
2004	345
2005	261
Total	1599

Table 1. Vulnerability Reports by Year

CERT information is updated daily, and the data can be collected by day of report. Reports for January 2006 were added to the 1599. A total of 1627 vulnerability reports were download and aggregated by month. Then a time series by month was used for the analysis. Figure 1 shows the number of reports by month.

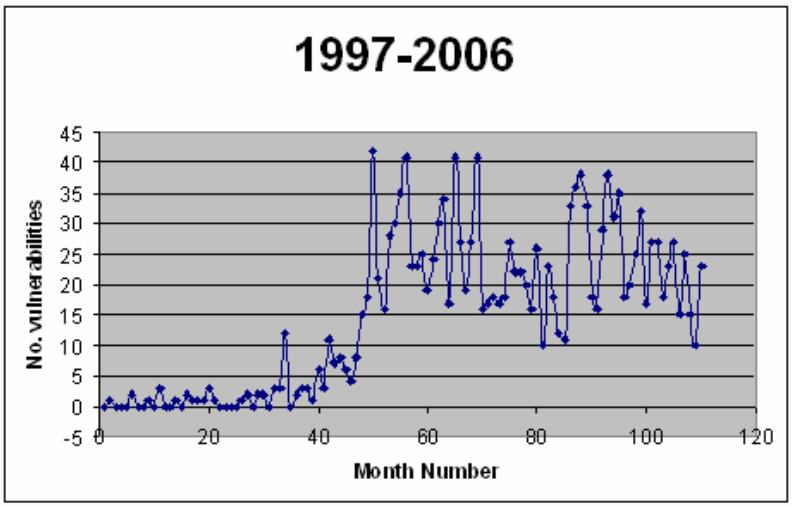

Figure 1. Number of Vulnerabilities Per Month (1997-1/2006)

ANALYSIS

In order to understand and shed some light on the behavior of cyber incident occurrences, first, a diagnosis of chaotic behavior was performed, followed by a simulation using a deterministic non-linear function. The chaos diagnostic tests determined if the frequency of the incidents follows a chaotic, random, or deterministic behavior over time. After testing for the level of chaotic behavior, a deterministic non-linear function was used in order to simulate the cyber incidents over time.

Chaos Diagnostic

One of the objectives of this paper is to determine if the frequency of cyber incidents over time is random, follows a certain pattern, or follows a deterministic chaotic order. Even though there is no single direct measure or test for chaotic behavior, several tests provide information about time series data that include randomness, autocorrelation or dependence, and long memory. Two popular measures used frequently in several fields are the Hurst exponent (Hurst, 1951)or Rescaled Range (R/S) method (Mandelbrot and Taqqu, 1979), and the Lyapunov exponent (Oseledec, 1968). According to Lo (1991), the Rescaled Range analysis demonstrates superiority to more conventional methods of determining long-range dependence.

Rescaled Range

The Rescaled Range method was initially developed in the field of hydrology by Hurst (1951) and further extended in the field of fractal mathematics (Mandelbrot and Taqqu, 1979; Mandelbrot and Van Ness, 1968). Hurst discovered that a large number of natural phenomena such as river discharges, mud sediments, and tree rings are dynamic systems that follow a biased stochastic behavior over time (Sprott, 2003). Later Mandelbrot and Van Ness (1968) labeled this behavior as Fractional Brownian Motion (FBM) that is a generalization of the random walk. Any time series data may be seen as the graph of a Brownian motion over time. The Hurst exponent provides a measure of whether the time series is a pure random walk or has underlying trends with long memory such as a FBM. The method to estimate this exponent is called Rescaled Range analysis (R/S).

Considering one-dimension motion, an object follows a random walk, also called Brownian motion, when the object randomly moves one-step at a time either going forward or backward depending on a random variable. An FBM is a biased stochastic behavior that follows certain trends or underlying order over time, while a random walk follows just a stochastic behavior without any specific systematic order. A random walk is said to have short memory since every step is independent of the previous step. It has short memory since the position of the object at time $t+1$ depends on the previous position t, but the movement from time t to time $t+1$ is totally independent. On the other hand, an FBM is considered either persistent (positive correlation) or anti-persistent (negative correlation) with long memory since no step is totally independent to the previous step. A system with FBM carries over some information from previous steps in order to determine the following step. An FBM can be persistent or anti-persistent. A persistent FBM is characterized by large periods with similar trend, while an anti-persistent FBM is characterized by very short periods with the same trend and more radical changes. In other words, the surface of an anti-persistent FBM time series will be rougher than that of a persistent FBM. A random walk will be something in the middle, not too jagged, but not too smooth.

The value range of the Hurst exponent is $0 \le H \le 1$ (Mandelbrot, 1975). The value of H is a degree of persistency of the FBM.

FBM with persistent behavior: $0 \le H < 0.5$

Standard Brownian motion or random walk: $H = 0.5$

FBM with anti-persistent behavior: $0.5 < H \le 1$

Using Monte Carlo simulations, the following behaviors were simulated to show the difference between these three types of behavior:

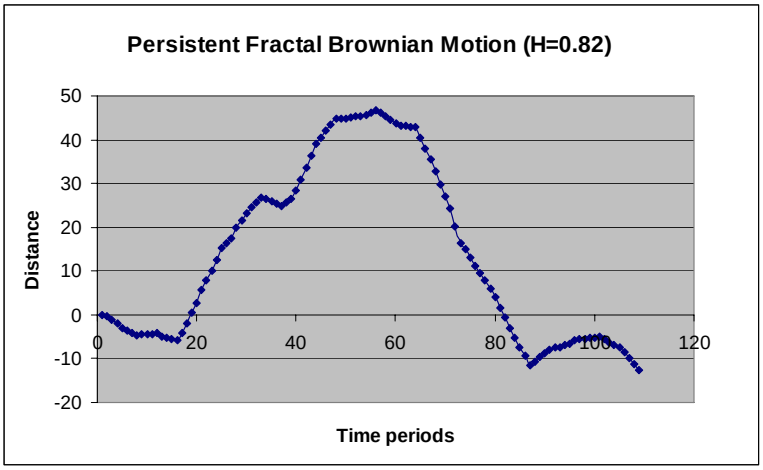

Figure 2. Persistent Fractal Brownian Motion

In the persistent FBM seen in Figure 2, the behavior of the system at time t is not totally independent of behaviors before t and the system is characterized by long periods with similar and consistent tendency –either decreasing or increasing

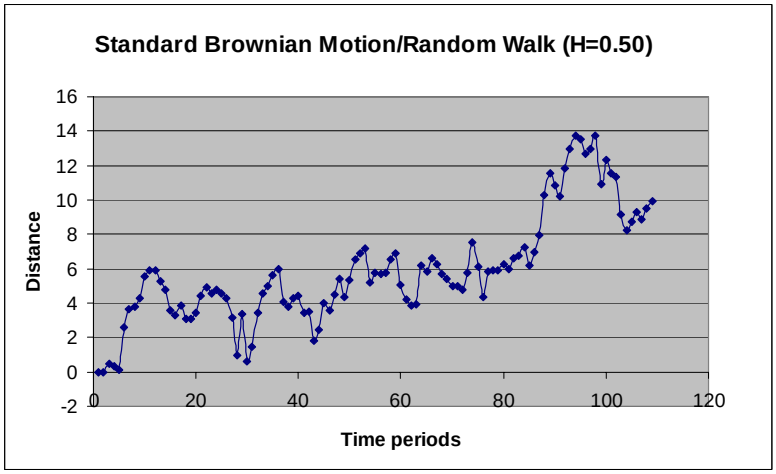

Figure 3. Standard Brownian Motion/Random Walk

In the standard Brownian motion or random walk in Figure 3, every step is independent of previous steps, so there is no correlation between the movements. In the antipersistent FBM, the movements of the system are negatively related to previous movements, so the system presents radical movements usually in opposite direction to the previous movement.

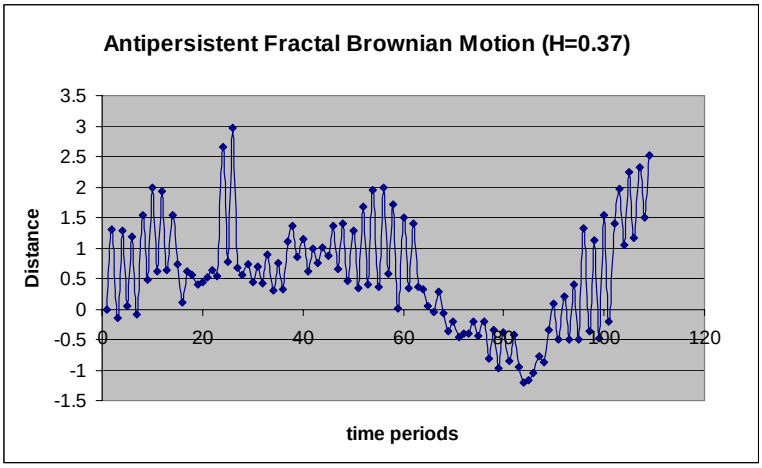

Figure 4. Anti-Persistent Fractal Brownian Motion

Another way to understand the differences in these types of behavior is through the concept of fractal dimension of the curves. For a flat line, the dimension is one. The dimension of the curve increase as the curve departs from a line and become a jagged surface. For example, a curve with a dimension of a fraction close to 2 should be a very jagged curve that should resemble a coarse surface since the curve should move up and down in every period of time.

The Hurst exponent is related to the fractal dimension of the time series curve by $D = 2 - H$. A time series without changes over time (flat curve) has a dimension of 1 where $(H = 1)$. As the curve moves toward a rough surface, H will decrease and D will increase. A random walk has a dimension of 1.5 where $(H = 0.5)$.

Method to Estimate the Hurst Exponent

Rescaled range analysis (R/S) is used to estimate the Hurst exponent. This analysis is based on the asymptotic value of the maximum standardized distance that an object can move in a random walk or an FBM over a very large period of time (toward infinity). Feller (1951) proved that for a pure random walk the number of standard deviations that an object moves is almost equal to the square root of the time periods the object was randomly moving. For an FBM this relationship is similar, but the difference is that, instead of using an exponent of 0.5 (square root), the time period is raised to the H value. This is shown by the following expression:

$$R/S \sim (t)^H, \; R/S = a(t)^H$$

Where:

R = Range of cumulative sums given by the difference between the maximum and minimum value of:

$$Y_j = Y_0 + \sum_{i=1}^{j} (X_i - \mu_X) \text{ For } 1 \le j \le t$$

In other words, $R = \max(Y_1, Y_2, ...Y_t) - \min(Y_1, Y_2, ...Y_t)$ and Y_j is the actual Y value of the time series curve at time j.

Y_0 is the initial value of Y at time $t = 0$.

X_i represents the stochastic movement at time or period i.

At time $i+1$, the new value of $Y_{i+1} = Y_i + X_i$ where $Y_{i+1} = Y_i + (X_i - \mu_x)$.

$S = std(X)$ standard deviation of the stochastic movements or change from every time period.

t = number of time periods

a = constant.

Therefore, $H = \log_n(R/S)$, that mathematically is equivalent to $H = \ln(R/S)/\ln(n)$.

A better estimation of H has been proposed by (Mandelbrot and Taqqu, 1979) using several combinations of subsets of the time series to calculate several R/S ratios. A traditional way to create the subsets is to divide the initial set of time series data in two halves and then divide each half into two halves continuing until the sub-samples are no smaller than 4. Then for the step i there will be 2^i parts or sub-samples of time series data. For each sub-sample in each step, an R/S is computed and then all the R/S for that step are averaged. There will be i different averaged R/S s. To get the Hurst exponent the natural logarithm of the number of periods for each step is regressed on the averaged R/S s of the corresponding step. Then the Hurst exponent will be the coefficient of regressing $\ln(t_i)$ on $\ln(R/S)_i$. The regression model is a transformation of the original equation by applying a natural log to each part of the equation:

We have different sets of R/S for each iteration or step described above:

$$R/S_i = at_i^H$$

Transforming the equation by logarithms:

$$\ln(R/S)_i = a + H\ln(t_i) + \varepsilon$$

H is the actual regression coefficient of this model.

The specific steps to calculate the different R/S_i and the actual H are detailed in (Corazza, Malliaris and Nardelli, 1997). This method was used in this paper.

Estimation of the Hurst Exponent

In our case, the sample size is 110 months. Using 31 sub-samples and following the method proposed by (Corazza et al., 1997), the Hurst exponent was estimated at 0.3629. Table 2 shows some relevant estimates of this computation.

Range of the whole sample	42
Standard deviation of the monthly changes	8.3966
Average of changes per month	-0.00909

Table 2. Estimates of Hurst Computation

A correlation can be calculated by $C = 2H - 1$, so the autocorrelation is approximately -0.27. This estimate suggests anti-persistence behavior of the vulnerability reports. This means that after an increase in the number of incidents in one month, it is more likely that the following month will decrease in a stochastic magnitude with a standard deviation of 8.39. This is a sign of a not totally chaotic behavior, however, it is not sufficient to provide a convincing conclusion. The Lyapunov exponent provides a more direct test for chaotic behavior. The following section will describe the method and results of this method.

Lyapunov Exponent Test

Most experts in Chaos theory would agree that a system is chaotic if its behavior is aperiodic, bounded long-term, and deterministic exhibiting sensitive dependence to initial conditions (Sprott, 2003). The difficulty in providing evidence of chaotic behavior is to show sensitivity to initial conditions. The Lyapunov exponent provides evidence of a possible chaotic behavior and the level of predictability of the system. The Lyapunov exponent is a measure of the sensitive dependence of initial conditions and conveys the average rate of divergence or convergence of two neighboring trajectories in the time series data (Pigliucci, 2000). If the exponent is negative, the system converges to a certain point. If the exponent is close to zero the

system behaves with periodic regularity. If the exponent is positive, the system can be either chaotic with an underlying order or random. A large positive exponent is a sign of pure randomness, while a small positive exponent is a sign of chaos (Pigliucci, 2000).

It is assumed that that the value for $Y(t+1)$ can be calculated deterministically with a function of $Y(t)$. The exponent can be calculated from experimental data or by a specific formula if the deterministic dynamical function is known. A Lyapunov local exponent has to be calculated for each $Y(t)$ of the time series. This local exponent is the number to which the e constant (2.71…) has to be raised to get the absolute value of the slope (derivative) of the time series function at the time period t. The Lyapunov exponent is given by the average of all of these local exponents (Sprott, 2003). Symbolically, this can be represented as:

$$\Delta Y_1 = f(Y_0 + \Delta Y_0) - f(Y_0) = \Delta Y_0 * f'(Y_0)$$

Where

X_0 = Initial value of the random or stochastic part of the random walk with $f' = df / dY$.

The local Lyapunov exponent λ is defined at X_0 such that $e^{\lambda 1} = \left|(\Delta Y_1 / \Delta Y_0)\right|$, or $\lambda^1 = \ln\left|(\Delta Y_1 / \Delta Y_0)\right| = \ln\left|f'(Y_0)\right|$

The global Lyapunov exponent is computed over many operations:

$$\lambda = (1/N) * \sum \ln\left|f'(Y_i)\right|$$

Y_i is the actual value of the time series curve at each point i. For the computation of the Lyapunov exponent, we are focusing on the derivative of the logistic map, which is the graph resulting from using $Y_{(t+1)}$ as dependent variable and $Y_{(t)}$ as independent variable. It is possible to use the local Lyapunov exponents to identify possible attractors. For the present analysis, we only focused on the estimation and interpretation of the Lyapunov exponent. As we have mentioned, if the Lyapunov exponent is positive and small, then it is a sign of chaotic behavior. The value of the exponent conveys how chaotic the data is. This exponent also provides information about the rate of predictability of the time series since it gives information about how sensitive the time series is to initial conditions. The bigger the largest positive Lyapunov exponent is, the more rapid the loss of predictive "power" and the less the prediction time for the time series.

Estimation of the Lyapunov Exponent

Simply stated, it is not possible to detect a deterministic dynamic function that relates $Y_{(t+1)}$ with $Y_{(t)}$. Using the method suggested by (Sprott, 2003), we computed the Lyapunov exponent. See Figure 5. Since we do not have a deterministic function of $Y_{(t+1)}$ a deterministic function was defined according to the data. The data was sorted by the number of incidents $Y_{(i)}$. In those cases where there was no intermediate value between $Y_{(i)}$ and $Y_{(i+1)}$, a value was estimated using the previous and following data available. The value was computed as an extrapolation of these values according to the number of intermediate values to compute. By doing this, we have a specific value of $Y_{(i+1)}$ for each $Y_{(i)}$. Then, we could calculate the differences in $Y_{(i)}$ and $Y_{(i+1)}$ to compute the slope for each point $Y_{(i)}$, and average them to get the global Lyapunov exponent. After this procedure, we got a Lyapunov exponent of 1.2611. Since the exponent is small and positive, it is a sign of chaotic behavior, not totally random. This can suggest certain amount of underlying order in the chaotic behavior. This is consistent with the estimation of the H exponent since that result suggested some level of negative correlation in the data, or what is also named short memory. It is not possible to describe the structure behind the chaotic order, but it is possible to see that after an increasing trajectory, it is very likely that a decreasing value will appear, suggesting that a short term prediction would be possible.

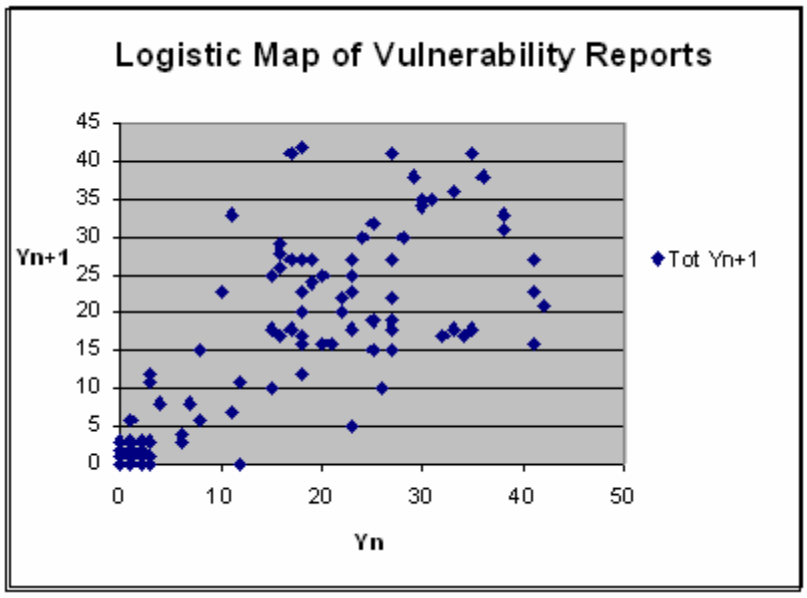

Figure 5. Logistic Map

Simulation

Finally, we simulated the behavior of the data in order to see if we could find a deterministic behavior underlying the apparent semi-chaotic behavior. We used the simple dynamic deterministic function proposed by May (1976). The function is:

$$Y_{(i+1)} = A * Y_{(i)} * (1 - Y_{(i)})$$

Where

$Y_{(i+1)}$ is the value of the time series curve at time $(i+1)$

$Y_{(i)}$ is the value of the time series curve at time i

A is a constant with possible values $[0..4]$

The possible values of any $Y_{(i)}$ are $0 \le Y_{(i)} \le 1$.

This function can be used to simulate population of species in which the population in a period $t+1$ depends on the population at t and this population is regulated by limited natural resources (in this case, the term $1 - Y_{(i)}$ is the regulator). This simple equation can generate equilibrium, cyclical order, or chaotic behavior. For certain values of the parameter A, the system can respond with any of these types of behavior. For example, if A is between 0 and 3, the system becomes to equilibrium to a certain point depending on the initial value. From 3 to 3.5, no matter what initial value the system starts, the system ends up oscillating in two points. As the parameter A increases from 3.5, the system behaves more chaotic until 4. After 4, the system diverges and goes to the minus infinite. This function has also been used to simulate dynamic economic models (Stutzer, 1980).

After manipulating this function, modifying the initial condition and the constant A, the following time series emerged. The purpose was to find a behavior similar to that of our real data. Figure 6 shows this simulation of non-linear deterministic function of vulnerability reports by month.

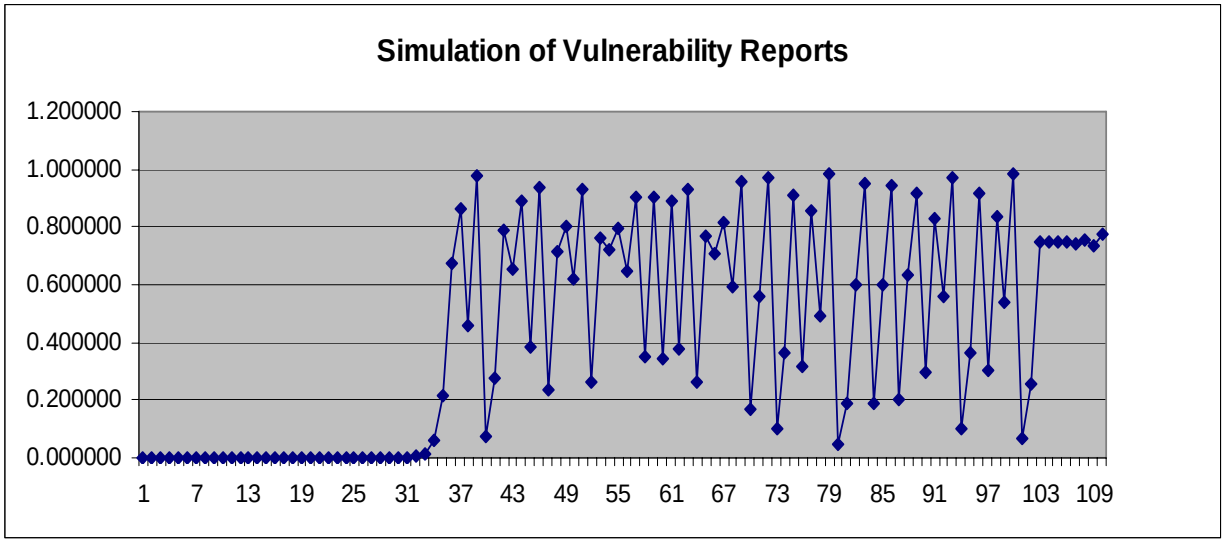

Figure 5. Simulation of Non-Linear Deterministic Function

The constant used was 3.95, while the initial condition was 1.233221×10^{-21}. It has been shown that this function shows chaotic behavior after a value of 3.58. It was not possible to get a similar time series compared with the real data. However, they are similar in the level of persistency of the time series and in the period where the number of reports increased. It is important to note that an apparent stability appeared at the end of the period. However, the actual behavior beyond this apparent stability is also chaotic. This is a sign that complex systems can apparently go to stability and suddenly move to the edge of chaos again.

Conclusions and Discussion

The present paper provides a new perspective based on Chaos theories to understand how the cyber incidents might behave over time. More specifically, the study questions and analyzes the underlying order of the apparent chaotic behavior based on the number of vulnerabilities reported to CERT. Understanding cyber incidents is an important issue since there has been an increase in the number of incidents worldwide. In addition, the negative impact of these incidents has grown dramatically since the mid 1990's. The increase in frequency and type of cyber attacks for the last five years does not follow an apparent pattern (Gordon, Loeb, Lucyshyn and Richardson, 2005).

Vulnerabilities reported by CERT are currently the best indicator we can have regarding the types of cyber attacks launched on the Internet in the US every day. Even though the study does not pretend to predict the number of cyber attacks, it sheds light on the dynamics of cyber attack vulnerabilities occurring every month. Results suggest that the behavior of these reports is not purely random providing some evidence of short system memory. According to our results, the vulnerability time series data was anti-persistent and negatively correlated. The data present signs of non-totally random behavior. Some authors have argued that a chaotic system could be predicted only over very few periods of time that are multiples of the Lyapunov exponent. According to our estimation of this exponent, it could be possible to predict the number of vulnerabilities for a period of 20 days (1.2^{-1} number of months, which is less than one time period used in the analysis). According to the Hurst exponent estimation, the data is negatively correlated over time, meaning that after a decreasing number of vulnerability reports over some period of time, it is more likely that the following period there will be a radical increase in the number of vulnerability reports. This might suggest that in vulnerable complex IT systems –like most modern corporate IT infrastructures – managers should pay attention when the system is experiencing continuous decrease in number of incidents or periods of stability. In this situation, most managers might continue using their planned emergency response strategy instead of being aware and prepared for a very likely radical change in the system that could cause a crisis. In crisis time, managers might be prepared to respond organically more than systematically.

The main contribution of the present paper is the new approach to identifying underlying patterns in the frequency of incidents over time that could provide important information for predicting in the short-term. This methodology can be used in further research to analyze more detailed data of cyber attacks. Further research is needed to understand the dynamics of

cyber attacks by considering specific types of attacks and having access to data related cyber attacks reports. Variables such as severity of the attack, the propagation time, and the nature of the attack need to be considered in future work.

REFERENCES

1. Battram, A. (1998) *Navigating Complexity*, Industrial Society, London, UK.

2. CERT/CC "Cert Coordination Center Alerts," 2003.

3. Corazza, M., Malliaris, A.G., and Nardelli, C. (1997) Searching for Fractal Structure in Agricultural Future Markets, *The Journal of Future Markets*, 17, 4, 433-463.

4. Dunlevy, C.J. "Protection of Critical Infrastructures: A New Perspective," CERT Analysis Center, 2003.

5. Feller, W. (1951) The Asymptotic Distribution of the Range of Sums of Independent Random Variables, *Annals of Mathematical Statistics*, 22, 427-469.

6. FRB "Fedwire and National Settlement Services - Annual Data," Federal Reserve Board, 2003.

7. Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R. "Csi/Fbi Computer Crime and Security Survey," Computer Security Institute and Federal Bureau of Investigation.

8. Goulielmos, A.M. (2002) Complexity Theory Applied to Management of Shipping Companies, *Maritime Policy and Management*, 29, 4, 375-391.

9. Goulielmos, A.M. and Giziakis, C.B. (2002) Marine Accident Prevention: An Evaluation of the Ism Code by the Fundamentals of Complexity Theory, *Disaster Prevention and Management*, 11, 1, 18-32.

10. Hurst, H.E. (1951) Long-Term Storage of Reservoirs, *Transactions of the American society of civil engineers*, 116,

11. Kiel, L.D. (1995) Chaos Theory and Disaster Response Management: Lessons for Managing Periods of Extreme Instability, What Disaster Response Managment Can Learn From Chaos Theory, California Research Bureau, 1-20.

12. Koehler, G.A. (1995) Disaster Characteristics That Disorder Organizations, What Disaster Response Managment Can Learn From Chaos Theory, California Research Bureau, 1-26.

13. Lo, A.W. (1991) Long-Term Memory in Stock Market Prices, *Econometrica*, 59, 5, 1279-1313.

14. Mainzer, K. (1994) *Thinking in Complexity: The Complex Dynamics of Matter, Mind, and Mankind*, Springer-Velag, New York, NY.

15. Mandelbrot, B.B. (1975) Stochastic Models for the Earth's Relief, the Shape and Fractal Dimension of the Coastlines, and the Number-Area Rule for Islands, 72, 3825-3833.

16. Mandelbrot, B.B. and Taqqu, M. (1979) Robust R/S Analysis of Long-Run Serial Correlation, *Bulletin of the International Statistical Institute*, 48, Book 2, 59-104.

17. Mandelbrot, B.B. and Van Ness, J. (1968) Fractional Brownian Motion, Fractional Noises and Applications, *SIAM Review*, 10, 422-437.

18. May, R.M. (1976) Simple Mathematical Models with Very Complicated Dynamics, *Nature*, 261, 10, 459-467.

19. Nawrocki, D. (1995) R/S Analysis and Long Term Dependence in Stock Market Indices, *Managerial Finance*, 21, 7, 78-91.

20. Oseledec, V.I. (1968) A Multiplicative Ergodic Theorem: Lyapunov Characteristic Numbers for Dynamical Systems, *Transactions of the Moscow Mathematical Society*, 19, 197-221.

21. Pigliucci, M. (2000) Chaos and Complexity, *Skeptic*, 8, 3, 62-70.

22. Priesmeyer, H.R. and Cole, E.G. (1995) Nonlinear Analysis of Disaster Response Data, What Disaster Response Managment Can Learn From Chaos Theory, California Research Bureau, 1-26.

23. Richards, D. (1990) Is Strategic Decision Making Chaotic?, *Behavioral Science*, 35, 3, 219-232.

24. Sprott, J.C. (2003) *Chaos and Time Series Analysis*, Oxford University Press, Oxford, UK.

25. Stutzer, M. (1980) Chaotic Dynamics and Bifurcation in a Macro Model, *Journal of Economic Dynamics and Control*, 2, 4,

26. US-CERT "Vulnerability Notes Database," US Department of Homeland Security, 2006.