Applying Mathematics and Engineering Techniques to Cyber Security

Chuck Easttom
chuck@chuckeasttom.com / https://orcid.org/0000-0002-6744-6731
Georgetown University
Plano, TX, Estados Unidos de América

Recibido: 19/8/2021 Aceptado: 26/9/2021
doi: https://doi.org/10.26439/ciis2021.5575

ABSTRACT. While there are many approaches to cybersecurity, it is common for those approaches to be somewhat ad hoc or subjective. Cybersecurity needs a rigorous mathematical and engineering approach, which can be applied to address security issues, evaluate security controls, and investigating security breaches. The current paper maps the use of engineering and mathematical tools for cybersecurity purposes.

KEYWORDS: cybersecurity engineering / cyberthreat analysis / cyberthreat modelling / mathematical modelling

APLICACIÓN DE TÉCNICAS MATEMÁTICAS E INGENIERÍA A LA CIBERSEGURIDAD

RESUMEN. Si bien existen muchos enfoques de la ciberseguridad, es común que esos enfoques sean al menos algo *ad hoc* o subjetivos. La ciberseguridad necesita un riguroso enfoque matemático y de ingeniería. Esto se puede aplicar para abordar problemas de seguridad, evaluar controles de seguridad e investigar brechas de seguridad. El documento actual mapea el uso de herramientas de ingeniería y matemáticas con fines de ciberseguridad.

PALABRAS CLAVE: ingeniería en ciberseguridad / análisis de ciberamenazas / modelado de ciberamenazas / modelado matemático

1. INTRODUCTION

Cyber-attacks are a reality of modern life. There has been a wide assortment of techniques proposed to catalog and analyze various attacks. What is conspicuously absent from the literature is the application of engineering practices and mathematical tools to analyze cyber-attacks. The current approach presented in this paper is to apply various engineering techniques to cybersecurity processes. Cybersecurity analysis would be enhanced and improved by integrating these methods into cybersecurity analysis. This paper proposes a general methodology for doing that, along with a specific case study.

This is concurrent with a more general problem of lack of engineering rigor in cybersecurity. While the term engineering is widely used in cybersecurity, there is a noticeable lack of actual engineering techniques in practice, and even in academic programs (Easttom, 2019).

2. REVIEW OF LITERATURE

In order to fully appreciate the currently proposed methodology, it is required that one first examine two different subtopics in this review of the literature. The first is an examination of existing cybersecurity modeling techniques. This provides an understanding of the current state of cybersecurity. The second domain reviews engineering techniques for failure analysis and mathematical tools that will later be applied to cybersecurity. As many cybersecurity professionals will not be familiar with the engineering and mathematical techniques described in this paper, it is necessary to provide a general overview of these methods to describe integrating said techniques into cybersecurity.

Most efforts to quantify data in cybersecurity relate to quantifying the economic impact of breaches (Dongre *et al.*, 2019; Gandal *et al*., 2020). Studies also quantify risk (van den Hooven, 2020) and ancillary topics such as the trade-off between security and privacy (Suo *et al*., 2021). Despite these narrowly focused efforts cybersecurity is generally approached without the benefit of quantifiable techniques and engineering rigor.

There have been attempts to apply mathematics to cybersecurity issues. As one example, Ahmadian *et al.* (2019) applied non-Bayesian methods to evaluating cyber-attacks on power systems. Their study, while applicable, was very narrowly focused on specific attacks executed against specific targets. Their study did not provide a generalized method for analyzing cyber-attacks, nor was it intended to. Furthermore, their modeling method focused on a very narrow use of mathematics. Among the techniques they did not explore were predator-prey dynamics. Their method did, however, illustrate the need for mathematical modeling in cyber-attack analysis.

The current method that provides the most quantifiable data regarding cyber vulnerabilities is the CVSS. The typical vulnerability scoring system (CVSS) is commonly utilized to

categorize vulnerabilities. CVSS is an open industry standard that allows for scoring vulnerabilities based on severity (Allodi & Massacci, 2014). When using CVSS, there are three groups of metrics: base, temporal, and environmental. The base group describes the basic characteristics of the vulnerability that are not determined by time (temporal) or environment. The metrics in this group are Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality Impact, Integrity Impact, and Availability Impact (Feutrill *et al.*, 2018).

The Attack Vector Metric can be in the following categories: Network (N), Adjacent (A), Local (L), Physical (P). Attack Complexity can be: None (N), Low (L), and High (H). User Interaction can be: None (N) or Required (R). The Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope. Its values can be: Unchanged (U) or Changed (C). The Impact Metrics (Confidentiality, Availability, or Integrity) are all rated: High (H), Low (L), or None (N) (Holm & Afridi, 2015). This method is effective, but it is incomplete.

Ultimately CVSS will produce a cumulative score, a number. The first issue with CVSS is that the scoring is still based on subjective assessments. It is up to the analyst to assign a numerical value for items like confidentiality. This introduces a substantially subjective aspect to this quantitative methodology. There have been efforts to revise CVSS (Singh & Joshi, 2016) to integrate Bayesian statistics with CVSS (Frigault *et al.*, 2017). However, these attempts still leave the basic CVSS process as being at least partially arbitrary.

CVSS is also narrowly applied to quantifying vulnerabilities. It does not provide a mechanism for quantifying cybersecurity failures. Nor does it provide a means to analyze attacks objectively. CVSS is a valuable tool, but it has a narrow application, which shows the need for a more broad-based, engineering approach to cybersecurity.

Another approach to modeling network attacks is STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (Khan *et al.*, 2017). Microsoft developed STRIDE for describing security threats in six separate categories. The threats are the letters in the acronym. The concept of using this tool is to ensure that all of the enumerated threats are modeled.

STRIDE was designed as a means of analyzing potential threats to the network. However, it can be used to categorize a network incident (Sanfilippo *et al.*, 2018). Much like CVSS, STRIDE provides ancillary benefits to network forensics. It can aid in describing the initial breach, but that is the limit of STRIDE's efficacy in facilitating network forensic analysis.

A model used to describe the impact of threats is the DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability) model. DREAD is a mnemonic for risk rating using five categories (Naagas & Palaoag, 2018). This modeling technique assesses the likelihood of an attack is and the damage it would cause. DREAD is an

effective model for considering where to allocate resources for network defense. DREAD can apply to a network forensics investigation to aid in evaluating the damage of a given incident (Yaqoob *et al*., 2019). Much like STRIDE and CVSS, DREAD provides a narrowly focused ancillary tool for network forensics.

There have also been studies analyzing cybersecurity as an ecology. Dupont (2019) viewed cybercrime from the perspective of the ecological system, both technology and human, within which the cybercrime occurred. Mazurczyk *et al.* (2016) defined several related terms such as attacker-defender ecology (ADE), cybersecurity ecology (CSE), and defenders' ecology (DE). Their work did provide a broad view of cyber-attacks and even incorporated Lotka-Volterra equations, something the current study also does.

While each of the threat analysis techniques examined in this section does provide valuable tools for cybersecurity, they all have a substantial gap. There are numerous engineering and mathemathical tools that can and should be brought to bear on cybersecurity problmes. There are numerous engineering and mathematical tools that can and should be brought to bear on cybersecurity problems.

3. CURRENT METHODOLOGY

3.1 Engineering Failure Analysis

One possibility for improving the quantitative analysis in cybersecurity is to utilize existing metrics from other engineering disciplines. There are specific metrics utilized in engineering for failure analysis and reliability engineering. This failure analysis is typical in mechanical, aerospace, and electrical engineering. For cybersecurity to indeed be an engineering discipline, it should also incorporate such failure analysis. Any breach should be considered a failure of the security controls. Whether those are technical controls or procedural/policy controls, it is still a failure of controls. If a virus outbreak in a network, there was a failure of one or more anti-virus controls. By quantifying the level of failure, one can quantify the efficacy of controls and track improvement in such controls. A nascent treatment of failure analysis for cyber security was outlined in a previous paper (Easttom, 2020) and is expanded upon here.

One of the first issues in failure mode analysis is to determine the severity of the incident. US Army MIL-STD-882 provides some guidance in classifying the severity of incidents (Fernald, 2020). There are four categories of severity that are listed and described in Table 1.

Table 1
MIL-STD-882 Severity Categories

Category	Description	Criteria
I	Catastrophic	Possible death, permanent total disability, financial loss exceeding $1M, or irreversible severe environmental damage.
II	Critical	Possible permanent partial disability, injuries, or occupational illness that may result in hospitalization of at least three personnel, financial loss between $200K and $1M, or reversible environmental damage.
III	Marginal	Possible injury or occupational illness resulting in one or more lost workday(s), financial loss between $10K and$200K, or mitigatable environmental damage.
IV	Negligible	Possible injury or illness not resulting in a lost workday, financial loss between $2K and $10K, or minimal environmental.

Own elaboration

These may not apply to all cyber incidents; however, they provide a guideline for quantifying the severity of an incident. One aspect of bringing engineering rigor to the field of cybersecurity is quantifiable data. Incidents must be ranked in a quantifiable manner.

A standard method of identifying reliability in systems engineering is the Mean Squared Deviation. The Mean Squared Deviation formula is relatively simple and provides insight into how any system deviates from expectations (Engel, 2010). It essentially takes the square of the errors, or deviations from the expected/desired outcomesThis is sometimes referred to as the mean squared error (Engel, 2010; Wasson, 2015). The MSD formula is shown in equation 1.

$$MSD = \frac{1}{n} \sum_{i=2}^{n} (y_i - T)^2 \qquad (1)$$

In equation 1

yi is the actual value

T is the target value

The MSD provides a positive integer value that demonstrates how far the system has deviated from its expected performance. This is commonly used in many engineering disciplines (Modarres *et al*., 2016). The MSD can readily be applied to any cybersecurity control. The smaller the MSD, the closer the systems function is to its intended purpose. This is

commonly used in many engineering disciplines. This provides the cybersecurity team with quantifiable objectives: reducing the MSD for cybersecurity controls.

Related to the MPD is the Mean Percentage Error (MPE) formula. The MPE is the arithmetic mean of modeling, testing, or actual usage (Beynon-Davies, 2016). This metric compares expected values to actual values and calculates mean error. An error is defined as any deviation from the planned or expected value. This is critical in modeling as it can be used to evaluate the efficacy of the model itself. The MPE formula is shown in equation 2.

$$\mathrm{MPE} = \frac{100\%}{n} \sum_{t=1}^{n} \frac{a_t - f_t}{a_t} \tag{2}$$

Where:

n = is the number of different times for which the variable is forecast.

at is the actual value of the quantity being forecast

ft is the forecast.

Essentially this metric describes the difference between expected values and the actual value. This is an excellent metric for evaluating the efficacy of any security control. It can be applied to IDS/IPS, anti-virus, and even computer security policies.

Other failure metrics can be utilized to test the efficacy of any cyber defense technology. Statistical tools can be handy in this regard. On such test is the Kruskal-Wallis test. The Kruskal-Wallis test is a non-parametric test that compares two or more independent samples. The Kruskal-Wallis test is essentially a non-parametric version of the ANOVA test. Unlike the ANOVA, the Kruskal-Wallis test does not assume a normal distribution of the data set. This test is often used to test the correlation between two or more data sets that may not even have the same number of elements. The formula is shown in equation 3.

$$H = (N-1)\frac{\sum_{i=1}^{g} n_i(\bar{r}_{i\cdot} - \bar{r})^2}{\sum_{i=1}^{g}\sum_{j=1}^{n_i}(r_{ij} - \bar{r})^2} \tag{3}$$

N {\displaystyle N}N is the total number of observations across all groups

g is the number of groups

n_i is the number of observations in group i.

r_{ij} is the rank (among all observations) of observation j from group i.

$$\bar{r}_{i\cdot} = \frac{\sum_{j=1}^{n_i} r_{ij}}{n_i} \text{ is the average rank of all observations in group } i$$

$$\bar{r} = \tfrac{1}{2}(N+1) \text{ is the average of all the } r_{ij}.$$

Each of the three preceding mathematical tools (i.e., MSD, MPE, and Kruskal-Wallis) provides a means of quantifying the efficacy of cybersecurity measures. These tools provide a means of evaluating defensive modalities that has a mathematical rigor currently not frequently seen in cybersecurity.

Failure mode analysis is another tool from engineering that can be applied to cybersecurity. Any given breach either is a failure or causes failures. For example, a virus outbreak might cause network failure or operating system failure. The concept in traditional failure analysis is to examine as many components and subsystems as are practical in order to identify failure modes (Franklin, et al., 2012). Then the causes and effects of these failure modes can be analyzed. There are subtypes of Failure Mode and Effects Analysis (FMEA), such as functional failure mode and effects analysis or process failure mode and effects analysis. Failure Mode and Effects Analysis has several critical terms (Modarres et al., 2016):

- Failure Cause: This is what you are seeking, the ultimate cause of the failure. Why did the system fail? This may not always be the proximate cause or the apparent cause.
- Failure Mode: This is a description of what failed. In every engineering discipline, a complete description of the failure is critical to understanding why it failed.
- Failure Effect: This is the most apparent part of FMEA; what is the effect of the failure. For example, failure of coolant in a Nuclear Reactor could lead to more severe effects.
- Failure Severity: This is tightly coordinated with the failure effect. What is the severity of the failure, or put more simply, how bad was the failure?

Irrespective of the particular FMEA approach taken, the preceding four terms/concepts will substantially be important. Ishikawa diagrams (Chokkalingam, et al., 2016) are a commonly used engineering tool in FMEA. These are sometimes called fish diagrams because the defect is the fish's head, and the issues leading to the defect are branches or fish bones (Liliana, 2016). A generic example of how to create an Ishikawa diagram is shown in figure 1.

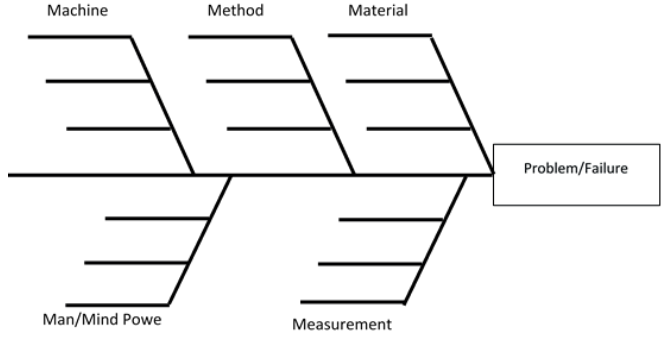

Figure 1. Ishikawa Diagram
Own elaboration

The Ishikawa diagram is a standard tool in root cause analysis. The major problem is traced back through a series of contributing factors that facilitated the problem. Some of these may be necessary components of the system or processes. However, the key is to identify those issues that can be eliminated or remediated. This can only be accomplished with root cause analysis.

FMEA is closely related to Failure Mode Effects and Criticality Analysis (FMECA). FMECA extends FMEA by including criticality analysis. How severe are the effects of failure modes? Types of failures include complete systems failures, degraded operation, and no immediate effect. Severity is divided into categories such as I Catastrophic; II Critical; III Marginal; IV Negligible. Failures are also ranked by probability. They can be A Frequent; B Probable; C Occasional; D Remote; E Improbable.

Related to root cause analysis with Ishikawa diagrams is the use of the issues tree. This is a breakdown of questions that are used to dissect the failure. The questions should follow four rules:

1. Each question will answer a "how" or a 'why" question.
2. The process begins with a critical question and progresses left to right.
3. Any branches should be mutually exclusive and collectively exhaustive (MECE)
4. The breakdown should be insightful.

Consider applying this process to a virus outbreak. One would have a series of questions starting with what is shown in Table 2:

Table 2
Failure Analysis and Virus Outbreaks

How did the virus get into the network	Answer downloaded	Was this in violation of policy	Answer Yes	Is there a lack of policy education?
			Answer No	Why is there no policy against this?
	Answer email attachment	Was this in violation of policy	Answer Yes	Is there a lack of policy education?
			Answer No	Why is there no policy against this?
	Answer USB drive	Was this in violation of policy	Answer Yes	Is there a lack of policy education?
			Answer No	Why is there no policy against this?

Own elaboration

As can be seen, each question provides an answer which leads to the next question. This provides a rigorous process of proceeding from one question to the next to determine the root cause of a specific issue. Root cause analysis facilitates more effective remediation of cybersecurity issues.

3.2 Lotka-Volterra Equations

In addition to applying engineering failure methods, mathematical techniques from biology can be applied to cybersecurity. Biologists frequently analyze predator-prey relationships, population changes, and similar issues. It is quite natural to consider applying these robust mathematical tools to cybersecurity. The Lotka–Volterra equations describe predator-prey dynamics in biological systems (Momeni et al., 2017). Cybercrime is also a predator-prey relationship. Whether the issue is phishing scams, malware distribution, or online child predators, the situation is similar to what is found in biology. A particular predatory is seeking a specific prey. Mazurczyk et al. (2016) applied Lotka-Volterra equations to understanding cyber criminals' operations within the cyber ecosystem. The application of Lotka-Volterra to online predators was briefly introduced in a previous paper and is expanded upon here (Easttom, 2021). The Lotka-Volterra equations are first-order, nonlinear differential equations. Thus, they should be understandable to most engineering students, even at the undergraduate level. The basic formula is shown in equation 4.

$$\frac{dx}{dt} = \propto x - \beta xy, \qquad (4)$$
$$\frac{dy}{dt} = \delta xy - \gamma y,$$

In equation 4, the x is the number of prey, the I is the number of a particular predator, t represents time, and α, β, γ, δ are positive real parameters describing the interaction of the two species (Elsadany & Matouk, 2015). The differentials represent the instantaneous growth rates of the two populations. The Lotka-Volterra equations have been expounded upon leading to competitive Lotka-Volterra equations and Generalized Lotka-Volterra equations (Vaidyanathan, 2015). Competitive Lotka–Volterra equations are used to study two or more species competing for a shared resource (Nguyen & Yin, 2017). This model begins with the logical population model often used in ecology. This model is shown in equation 5.

$$\frac{dx}{dt} = rx\left(1 - \frac{x}{K}\right) \qquad (5)$$

In equation 5, *x* is the size of the population at a particular time, *r* is inherent per-capita growth rate, and *K* is the carrying capacity. Given two populations labelled *x1* and *x2*, the competitive Lotka Volterra model is depicted in equation 6.

$$\frac{dx_1}{dt} = r_1 x_1 \left(1 - \left(\frac{x_1 + \alpha_{12} x_2}{K_1}\right)\right)$$
$$\frac{dx_2}{dt} = r_2 x_2 \left(1 - \left(\frac{x_2 + \alpha_{21} x_1}{K_2}\right)\right) \quad (6)$$

In equation 6, *α12* represents the effect species two has on the population of species one and *α21* represents the effect species one has on the population of species two.

The Lotka-Volterra equations, and their variations, lead naturally to the concept of mutualism (Tang, 2021). In biology, Holland *et al.* (2015) explain that mutualism describes the interaction between two or more species wherein each species derives some benefit. An obvious example is a relationship between bees and the flowers they pollinate. However, mutualism must not be conflated with cooperation (Epstein, 2018). Mutualism need not be intentional, nor something both species engage in voluntarily (Klipp *et al.*, 2016). In a predatory-prey dynamic, the prey certainly does not willingly engage in the relationship. However, while the prey species provides sustenance for the predator, the predator provides population control for the prey species (Holland *et al.*, 2002).

3.3 Lanchester's Laws

Lanchester's laws are related to the previously described Lotka-Volterra equations. However, rather than describing predator-prey relationships, these equations describe calculating the relative strengths of military forces (Kress, 2020). In addition to human military combat, it has been shown that these laws are applicable to animal combat (Clifton, 2020).

The basic mathematics is not particularly difficult. Lanchester's square law is shown in equation 7.

$$\frac{dA}{dt} = -\beta B$$
$$\frac{dB}{d_t} = -\propto^A \quad (7)$$

If α=β, meaning the two sides have equal firepower, the side with more soldiers at the beginning of the battle will win.

If A=B, meaning the two sides have equal numbers of soldiers, the side with greater firepower will win.

If A>B and α>β, then Red will win, while if A<B and α<β, Blue will win.

If A>B but $\alpha<\beta$, or A<B but $\alpha>\beta$, the winning side will depend on whether the ratio of β/α is greater or less than the square of the ratio of A/B.

These laws have been validated by applying them to historical battles. Hyeon & Aurelia (2020) applied these laws to the use cloud computing by militaries. It should be a relatively obvious application to use these equations to describe the 'battle' between cyber attackers and cyber defenders. This is particularly applicable to nation state cyber conflicts. More importantly, the Lanchester's laws illustrate another modality of the application of mathematics to cybersecurity.

3.4 Nicholson–Bailey model

The Nicholson–Bailey model was developed for studying population dynamics in parasite-host systems (Sarif Hassan et al., 2018). This model utilizes differential equations to understand the population growth in a host-parasite population (Jamieson & Reis, 2018). This is particularly applicable to cybercrime, as the cybercriminal can accurately be viewed as a parasite on the host population of legitimate internet users. The model is often expressed concerning to discrete-time as follows in equation 8.

$$\begin{aligned} H_{t+1} &= kH_t e^{-aP_t} \\ P_{t+1} &= cH_t\left(1-e^{-aP_t}\right) \end{aligned} \tag{8}$$

The value *H* represents the host population, and *P* represents the parasite population. The *k* value is the rate of reproduction for the host, and a is the efficiency of searching by the parasite. Finally, *c* is the average number of viable eggs the parasite lays in a given host. The value is the probability that the host will survive *Pt* predators. Conversely, 1- is the probability the host will not survive. Clearly, this model requires some modification to be applicable to cybercrimes. The parasite in a cybercrime does not 'lay eggs' in the host. However with some minor modifications, the concept is still applicable to at least some cybercrimes.

4. CONCLUSIONS

This paper introduces engineering failure analysis along with population biology dynamics to cybersecurity. While other engineering and mathematical tools that could be ported to cybersecurity, the tools presented in this paper are relatively easy to implement and derive immediate use from them. As the profession of cybersecurity matures, it will be imperative to incorporate rigorous engineering techniques and mathematical tools. This will allow the field of cybersecurity to progress from a subjective art to an objective engineering discipline.

REFERENCIAS

Ahmadian, S., Tang, X., Malki, H. A., & Han, Z. (2019). Modelling cyber attacks on electricity market using mathematical programming with equilibrium constraints. *IEEE Access*, *7*, 27376-27388. https://doi.org/10.1109/ACCESS.2019.2899293

Allodi, L., & Massacci, F. (2013). How CVSS is DOSsing your patching policy (and wasting your money). *BlackHat USA*.

Beynon-Davies, P. (2016). *Information Systems Development: an introduction to information systems engineering*. Macmillan International Higher Education.

Bollobás, B. (2013). *Graduate Texts in Mathematics: Modern graph theory*. Springer Science & Business Media.

Chokkalingam, B., Raja, V., Anburaj, J., Immanual, R., & Dhineshkumar, M. (2017). Investigation of Shrinkage Defect in Castings by Quantitative Ishikawa Diagram. *Archives of Foundry Engineering*, *17*(1), 174-178. https://doi.org/10.1515/afe-2017-0032

Clifton, E. (2020). A Brief Review on the Application of Lanchester's Models of Combat in Nonhuman Animals. *Ecological Psychology*, *32*(4), 181-191. https://doi.org/10.1080/10407413.2020.1846456

Dongre, S., Mishra, S., Romanowski, C., & Buddhadev, M. (2019). Quantifying the Costs of Data Breaches. In J. Staggs & S. Shenoi (Eds.), *Critical Infrastructure Protection XIII* (pp. 3-16). Springer, Cham. https://doi.org/10.1007/978-3-030-34647-8_1

Dupont, B. (2019). The ecology of cybercrime. In R. Leukfeldt & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 389-407). Routledge.

Easttom, C. (2018). A Systems Approach to Indicators of Compromise Utilizing Graph Theory. *2018 IEEE International Symposium on Technologies for Homeland Security,* 1-6. doi.org/10.1109/THS.2018.8574187

Easttom, C. (2019). *Incorporating Cybersecurity Engineering within the Discipline of Systems Engineering* [Master's thesis, University of Texas at El Paso]. Open Access Theses & Dissertations. Retrieved from https://scholarworks.utep.edu/open_etd/62/

Easttom, C. (2020). Mathematically Modeling Cyber-Attacks Utilizing Engineering Techniques. *15th International Conference on Cyber Warfare and Security (ICCWS).*

Easttom, C. (2021). Mathematically Modeling Victim Selection in Cybercrimes. *16th International Conference on Cyber Warfare and Security (ICCW)*.

Elsadany, A.A., Matouk, A.E. Dynamical Behaviors of Fractional-Order Lotka–Volterra Predator-Prey Model and its Discretization. *J. Appl. Math. Comput*. 49, 269–283 (2015). https://doi.org/10.1007/s12190-014-0838-6

Engel, A. (2010). *Verification, validation and testing of engineered systems*. John Wiley & Sons.

Fernald, D. G. (2020, January). US Army Software System Safety Process, Case-Study, and Success Stories. *2020 Annual Reliability and Maintainability Symposium (RAMS)*, 1-6. https://doi.org/10.1109/RAMS48030.2020.9153623

Feutrill, A., Ranathunga, D., Yarom, Y., & Roughan, M. (2018). The Effect of Common Vulnerability Scoring System Metrics on Vulnerability Exploit Delay. *2018 Sixth International Symposium on Computing and Networking (CANDAR)*, 1-10. https://doi.org/10.1109/CANDAR.2018.00009

Franklin, B. D., Shebl, N. A., & Barber, N. (2012). Failure Mode and Effects Analysis: too Little for too Much? *BMJ Quality Safety*, *21*(7), 607-611. https://doi.org/10.1136/bmjqs-2011-000723

Frigault, M., Wang, L., Jajodia, S., & Singhal, A. (2017). Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks. In L. Wang, S. Jajodia & A. Singhal (Eds.), *Network Security Metrics* (pp. 1-23). Springer, Cham. https://doi.org/10.1007/978-3-319-66505-4_1

Gandal, N., Riordan, M. H., & Bublil, S. (2020). A New Approach to Quantifying, Reducing and Insuring Cyber Risk: Preliminary Analysis and Proposal for Further Research. *Centre for Economic Policy Research*. https://doi.org/10.2139/ssrn.3548380

Jamieson, W. T., & Reis, J. (2018). Global Behaviour for the Classical Nicholson–Bailey Model. *Journal of Mathematical Analysis and Applications*, *461*(1), 492-499. https://doi.org/10.1016/j.jmaa.2017.12.071

Sarif Hassan, Sk., Ahluwalia, D., Maddali, R. K., & Manglik, M. (2018). Computational Dynamics of the Nicholson-Bailey models. *The European Physical Journal Plus*, 133(9), 349. https://doi.org/10.1140/epjp/i2018-12164-1

Holland, J. N., DeAngelis, D. L., & Bronstein, J. L. (2002). Population Dynamics and Mutualism: Functional Responses of Benefits and Costs. *The American Naturalist*, *159*(3), 231-244. https://doi.org/10.1086/338510

Holm, H., & Afridi, K. K. (2015). An Expert-Based Investigation of the Common Vulnerability Scoring System. *Computers & Security*, *53*, 18-30. https://doi.org/10.1016/j.cose.2015.04.012

Hyeon, C., & Aurelia, S. (2020, October). Enhancement of Efficiency of Military Cloud Computing using Lanchester Model. *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 960-964. https://doi.org/10.1109/I-SMAC49090.2020.9243515

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017). STRIDE-Based Threat Modeling for CyberPphysical *Systems. 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 1-6. https://doi.org/10.1109/ISGTEurope.2017.8260283

Klipp, E., Liebermeister, W., Wierling, C., & Kowald, A. (2016). *Systems Biology: a Textbook* (2nd ed.). Wiley.

Kress, M. (2020). *Lanchester Models for Irregular Warfare. Mathematics*, *8*(5), 737. https://doi.org/10.3390/math8050737

Liliana, L. (2016). A New Model of Ishikawa Diagram for Quality Assessment. *IOP Conference Series: Materials Science and Engineering*, 161. https://doi.org/10.1088/1757-899x/161/1/012099

Mazurczyk, W., Drobniak, S., & Moore, S. (2016). Towards a Systematic View on Cybersecurity Ecology. In B. Akhgar & B. Brewster (Eds.), *Combatting Cybercrime and Cyberterrorism* (pp. 17-37). Springer, Cham. https://doi.org/10.1007/978-3-319-38930-1_2

Naagas, M. A., & Palaoag, T. D. (2018). A Threat-Driven Approach to Modeling a Campus Network Security. *Proceedings of the 6th International Conference on Communications and Broadband Networking*, 6-12. https://doi.org/10.1145/3193092.3193096

Modarres, M., Kaminskiy, M. P., & Krivtsov, V. (2016). *Reliability Engineering and Risk Analysis: a Practical Guide* (3rd ed.). CRC press. https://doi.org/10.1201/9781315382425

Momeni, B., Xie, L., & Shou, W. (2017). Lotka-Volterra Pairwise Modeling Fails to Capture Diverse Pairwise Microbial Interactions. *ELife*, *6*. https://doi.org/10.7554/elife.25051

Nguyen, D. H., & Yin, G. (2017). Coexistence and Exclusion of Stochastic Competitive Lotka–Volterra Models. *Journal of Differential Equations*, *262*(3), 1192-1225. https://doi.org/10.1016/j.jde.2016.10.005

Sanfilippo, J., Abegaz, T., Payne, B., & Salimi, A. (2019). STRIDE-Based Threat Modeling for MySQL Databases. *Proceedings of the Future Technologies Conference,* 368-378. https://doi.org/10.1007/978-3-030-32523-7_25

Singh, U. K., & Joshi, C. (2016). Quantitative Security Risk Evaluation Using CVSS Metrics by Estimation of Frequency and Maturity of Exploit. *Proceedings of the World Congress on Engineering and Computer Science*, 1, 170-175.

Suo, D., Renda, M. E., & Zhao, J. (2021). *Quantifying the Tradeoff Between Cybersecurity and Location Privacy.* arXiv. https://arxiv.org/abs/2105.01262

Vaidyanathan, S. (2015). Adaptive Biological Control of Generalized Lotka-Volterra Three-Species Biological System. *International Journal of PharmTech Research*, *8*(4), 622-631.

van den Hooven, C. (2020). Quantitative Risk Calculation in Cybersecurity: The Value of Quantifying Risk. *ISSA Journal*, *18*(10).

Wang, W., Yang, D., & Luo, Y. (2013). The Laplacian Polynomial and Kirchhoff Index of Graphs Derived from Regular Graphs. *Discrete Applied Mathematics*, *161*(18), 3063-3071. https://doi.org/10.1016/j.dam.2013.06.010

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of Things Forensics: Recent Advances, Taxonomy, Requirements, and Open Challenges. *Future Generation Computer Systems*, *92*, 265-275. https://doi.org/10.1016/j.future.2018.09.058

Wasson, C. S. (2015). *System Engineering Analysis,Design, and Development: Concepts, Principles, and Practices* (2nd ed.). John Wiley & Sons.

BIBLIOGRAPHY

Babarinsa, O., & Kamarulhaili, H. (2017). On Determinant of Laplacian Matrix and Signless Laplacian Matrix of a Simple Graph. In S. Arumugam, J. Bagga, L. Beineke, B. Panda (Eds.), *Theoretical Computer Science and Discrete Mathematic*s (pp. 212-217). Springer. https://doi.org/10.1007/978-3-319-64419-6_28

Birolini, A. (2017). *Reliability engineering: Theory and Practice* (8th ed.). Springer.

Deo, N. (2017). *Graph Theory with Applications to Engineering and Computer Science*. Dover Publications.

Fu, L., Song, W., Lv, W., & Lo, S. (2014). Simulation of Emotional Contagion Using Modified SIR Model: A Cellular Automaton Approach. *Physica A: Statistical Mechanics and its Applications*, *405*, 380-391. https://doi.org/10.1016/j.physa.2014.03.043

Godsil, C., & Royle, G. F. (2013). *Graduate Texts in Mathematics: Algebraic Graph Theory*. Springer Science & Business Media.

Gross, J. L., & Yellen, J. (2005). *Graph Theory and its Applications* (2nd ed.). CRC press.

Harko, T., Lobo, F. S., & Mak, M. K. (2014). Exact Analytical Solutions of the Susceptible-Infected-Recovered (SIR) Epidemic Model and of the SIR Model with Equal Death and Birth Rates. *Applied Mathematics and Computation*, *236*, 184-194. https://doi.org/10.1016/j.amc.2014.03.030

Kuddus, A., Rahman, A., Talukder, M. R., & Hoque, A. (2014). A Modified SIR Model to Study on Physical Behaviour among Smallpox Infective Population in Bangladesh. American Journal of Mathematics and Statistics, *4*(5), 231-239.

Latino, M. A., Latino, R. J., & Latino, K. (2016). *Root Cause Analysis: Improving Performance for Bottom-Line Results* (4th ed.). CRC Press

Motzek, A., Möller, R., Lange, M., & Dubus, S. (2015). Probabilistic Mission Impact Assessment Based on Widespread Local Events. *Proceedings of the NATO IST-128 Workshop: Assessing Mission Impact of Cyberattacks*, 16-22.

Noel, S., Harley, E., Tam, K. H., Limiero, M., & Share, M. (2016). CyGraph: Graph-Based Analytics and Visualization for Cybersecurity. In V. N. Gudivada, V. V. Raghavan, V. Govindaraju & C.R. Rao (Eds.), *Handbook of Statistics* (Vol. 35, pp. 117-167). Elsevier. https://doi.org/10.1016/bs.host.2016.07.001

Sahu, M. K., Ahirwar, M., & Shukla, P. K. (2015). Improved Malware Detection Technique Using Ensemble-Based Classifier and Graph Theory. *2015 IEEE International Conference on Computational Intelligence & Communication Technology*, 150-154. https://doi.org/10.1109/CICT.2015.147