The Calculus of Protecting Interstate Competition from Cyber Attack

Vaughn H. Standley
College of Information and Cyberspace
National Defense University
Washington D.C., U.S.A.
vaughn.standley.civ@ndu.edu

Roxanne B. Everetts
College of Information and Cyberspace
National Defense University
Washington D.C., U.S.A.
roxanne.everetts@ndu.edu

***Abstract* — Lethal conflict may be approximated using power law statistics, which on a log-log plot of exceedance probability (EP) versus severity is characterized by constant slope -q. Values of q<1 violate probability axioms and describe high-risk systems. Consistent with reports that q for war improves after 1950 from 0.41 to 0.75 due to increases in military alliances, q is argued to be a sensitive function of network variables. Low-risk interstate competition is achieved when q>1 and allows for the use of Bayesian hypothesis tests based on q to serve as a decision criteria about when to react to threats, leading to a set of parameters that determine if conflict will escalate and to the conclusion that redundant networks, deterrence, and attack detection stabilize competition against cyber conflict. Examples of the importance of the Bayesian parameters in creating and adapting networks to stabilize competition are provided.**

Keywords –network; likelihood ratio; power law; resiliency; Bayesian

I. INTRODUCTION

This paper describes a first-order analytical model that associates a set of network parameters to the potential for cyber-attacks to escalate a state of peaceful interstate competition to violent conflict.

The *Stability-Instability Paradox* [1], developed by Snyder in 1965 [2], describes an interrelationship between all-out war and lesser forms of conflict where strategic-level peace, achieved through nuclear deterrence, leads to regional armed conflict. Competition is a form of nonviolent conflict that includes political, economic, informational, and military efforts that exceed normal peaceful relations. "During competition, U.S. and Allied forces actively campaign to advance and defend national interests in an environment that is short of armed conflict" [3]. Thus, competition arises in the absence of regional armed conflict in the same way that regional conflict arises in the absence of all-out war.

Deterrence is about "decisively influencing an adversary's decision calculus to prevent attack or the escalation of a conflict" [4]. Thus, deterrence is first and foremost an information and decision process and not simply derived from an assessment of risk from military capabilities. There is no a priori reason to think that interstate competition is different because people decide, nation-states do not.

Because deterrence is within the domains of information and decision theory, "Shannon's Maxim" comes into play. The "father of information theory," Claude Shannon, argued that one ought to design cyber systems under the assumption that the enemy will immediately gain full familiarity with them [5]. While Shannon's Maxim is more widely known as being fundamental to public key infrastructure (PKI) on which all cybersecurity is based today, its parallel in deterrence is that a nation's military capabilities should be assumed to be known by its adversaries. Emerging technologies like Blockchain, extend the level of openness described by Shannon's Maxim and, for this reason, appear to be stronger than PKI. While it seems certain there will always be a role for encryption, "policy and political push for more transparency could prove to be the deciding factor" in selecting open technology over traditional cybersecurity methods [6]. In the same way that encryption methods evolved from "security through obscurity" to those based on a presumption of being known, information assurance seems set to evolve to be more open and networked, rather than more closed. The extreme importance of information methods and systems to deterrence suggests they too are better served by more open and more networked systems. Similarly, if we apply the *Stability-Instability Paradox*, then this assumption would apply to regional armed conflict and nonviolent interstate competition as well.

II. THE POWER LAW, WAR, AND STRATEGIC COMPETITION

The power law of statistics is used to describe the relationship between two values when a change in one results in a change of proportional size in the other. Power laws have been defined across numerous disciplines, including science, statistics, physics, engineering, etc. [7]. A common application of power laws is the use in defining a probability distribution. Unpredictable and catastrophic failures in networked systems are often observed to follow a power law relationship, meaning that the probability of a severity S that exceeds a severity level s is equal to s raised to a negative constant q and multiplied by a constant C. Intuitively, the power law means that smaller consequence events happen exponentially more often than larger events. Formally, it is described by the following formula:

$$P(S > s) = Cs^{-q} \tag{1}$$

In 1960, Lewis Fry Richardson was the first to fit armed conflict with power law constants in his famous *Statistics of*

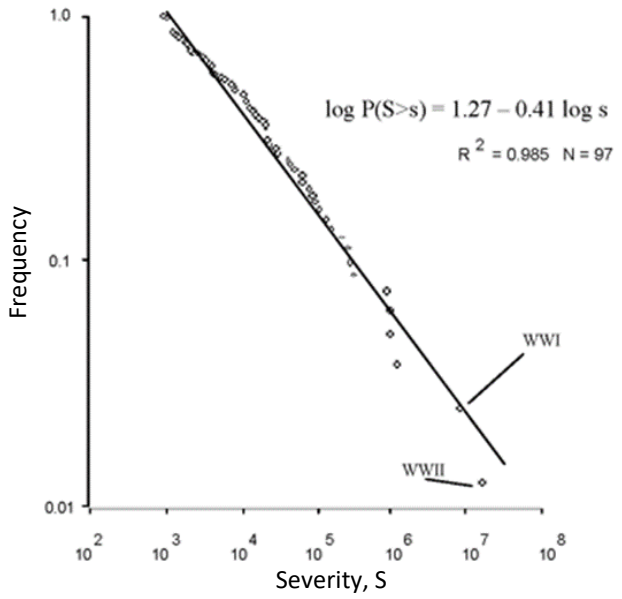

Figure 1. Dots indicate wars. The solid line is a Power law fit to the data. Data Source: Correlates of War Project [8].

Deadly Quarrels. This work was later confirmed by Cederman [8]. On a plot of $logP(S > s)$ versus $log(s)$, Cederman's fit to the data describes a straight line with slope equal to -0.41 and a y-intercept equal to 1.27. See Figure 1. When not written in log-log form, the power law fit to this data may be written as Eq. (2):

$$P(S > s) = 18.6s^{-0.41} \quad (2)$$

Power law phenomena are identified as "low-risk" if $q > 1$ because the rate of increasing severity is outpaced by decreasing likelihood. Conversely, phenomena are "high-risk" if $q < 1$ because severity increases faster than the likelihood decreases. Accordingly, q for war is a high-risk phenomenon. However, the power law violates the axioms of probability if $q < 1$ and is, therefore, untrustworthy beyond what is indicated directly by data.

Rational decisions are based on risk, not just likelihood. Risk is equal to likelihood multiplied by severity. In the case of Figure 1, severity is the number of persons killed. Figure 2 illustrates how extremely severe wars cannot be discounted even though their likelihood is small. For example, the war line (red) in Figure 2 increases as severity s increases. Believing that the fit to the data in Figure 1 holds until $s = 10^8$, a hypothetical nuclear war killing a 100 people (8 on the x-axis) is more risky than a war killing a thousand (3 on the x-axis). This agrees with our observation that nations build and maintain military defenses for extremely unlikely wars. For systems having a q value greater than one, risk decreases with increasing consequences. The decreasing green line that we call "Competition" in Figure 2 is derived from q=1.10. The consequences of increasingly improbable conflicts may be ignored. That is, it's low-risk.

Reflecting on the *Stability-Instability Paradox*, it seems that it is simply evidence of the power law nature of war. The power law requires that smaller conflicts are likely in the absence of larger ones, and vice-versa, even if the underlying mechanisms are not clear.

III. War and Competition Networks

The underlying mechanisms for war have been proposed and debated for centuries. One idea is that war is a network phenomenon [9]. In this theory, nations seeking to expand their network eventually seek to absorb nodes of other nations' networks, analogous to the natural process that often leads larger companies to acquire smaller ones. The first forty years of Durant's acquisition of various automobile companies (Oldsmobile, Cadillac, etc,), that eventually lead to the formation of General Motors, is a notable example. This process is often referred to as 'preferential attachment.' "Species distribution and many other phenomena are observed empirically to follow power laws where preferential attachment process is a leading candidate mechanism to explain this behavior" [10]. It is called Competitive Exclusion in different contexts.

A parametric model of this network process is obtained through the exceedance probability used in traditional quantitative risk management. Failures start and propagate in a network according to the vulnerability of nodes in terms of probability γ, and the network spectral radius, ρ. Spectral radius embodies the main characteristics of a bidirectional network, which are the density of links and size of heavily connected hubs. The measure of network resilience, z, is proportional to both the inherent fractal dimension of the network, q, and to $\gamma\rho$, where $z < 1$ indicates low-risk, $z > 1$ is high-risk, and $z >> 1$ indicates the potential for catastrophe. The spectral radius can be seen as a measure of "reachability" from any one node to any other node along a chain of network hops. As reachability increases, vulnerability to cascading failure increases. The product $\gamma\rho$ will determine the degree to which failures propagate. Survivability of a network can be

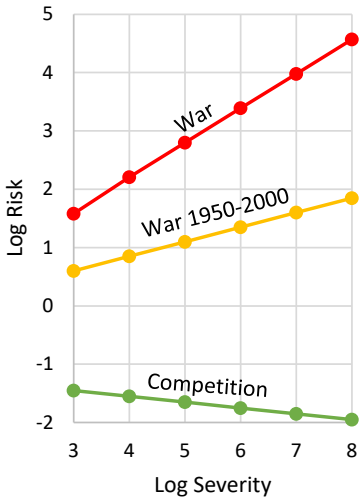

Figure 2. Log risk versus log severity s for three q values.

achieved by hardening or isolating nodes from the network as soon as the nodes have been compromised. For example, in a network model for the communicability of a human disease, nodes in the network represent humans who may receive preventive treatment to reduce infectiousness, decreasing γ. Or, links in the infection network are cut by enforcing a quarantine to reduce ρ. Lewis [11] reports that networked critical infrastructure sectors (e.g., communication, transportation, electricity, etc.) obey a *Fundamental Resilience Equation*, the log-linear relationship in Eq. (3), where b and k are constants:

$$log(q) = b + k\gamma\rho \tag{3}$$

This equation, where k is negative, indicates that vulnerable and/or large networks subject to cascading failure lessen q. Raising severity s to the value on both sides of Eq. (3) reveals that q changes exponentially with linear changes to $b + k\gamma\rho$ as in Eq. (4):

$$q = s^{b+k\gamma\rho} \tag{4}$$

Based on extensive simulation work, Lewis reports that the average b, k, and ρ are 0.5, -0.42, and 8, respectively. What this means is that there is only a narrow band, between 0 and 0.14, where the product $\gamma\rho$ results in $q>1$. Greater values result in $q < 1$, leading to estimates of exceedance probability that can't be trusted. Within the narrow range, however, q will be extremely sensitive to the product $\gamma\rho$ if war is a network phenomenon.

Jackson and Nei [12] report that political, military, and economic alliances increase resistance to cascading failure. In other words, war is a network phenomenon. Their findings allow us to estimate a larger value of q for war between the years of 1950 and 2000 that is apparently due to increased network redundancy and hardness that decreases the exponent:

> *"The number of wars per pair of countries per year from 1950 to 2000 was roughly a 10th as high as it was from 1820 to 1949. This significant decrease in the frequency of wars correlates with a substantial increase in the number of military alliances per country and the stability of those alliances."* [12]

Though there has been no employment of nuclear weapons since 1945, their presence and proliferation bears some comment, since the possibility of nuclear warfare has, in some way, affected all subsequent wars involving nuclear states and their surrogates. The consequences of war changed when the U.S. and USSR gained nuclear capabilities. The effects of nuclear arsenals—particularly those delivered by ICBMs—on whether or not states go to war may not be an easy thing to measure but surely exist. In addition, the number of countries over the last two centuries varied considerably due to the rise and fall of European colonialism. In short, it may not be an "apples-to-apples comparison". For the moment, however, we simply accept the assertion by Jackson and Nei [12].

The q in Eq. (2) was adjusted until $P(10^3>s)$ becomes one-tenth the value as for for q=0.41. The value q=0.75 was obtained. Since the year 2000, the Internet and GPS-enabled smart phone technologies, to name a few, have further extended interstate networks, decreasing the negativity of the network term and increasing the overall exponent (i.e., increasing q). Note that the values -0.41 and -0.75 are typical according to Lewis [11] but outside the band where q is a valid parameter of a probability distribution. Figure 3 illustrates decreasing $P(S > s)$ as a function of s for war (q=0.41), war from 1950 to 2000 (q=0.75), and Competition (q=1.1).

IV. Attack Calculus During War and Compeitition

To have operational significance, the power law data must be incorporated into a decision-making formula. A Bayes' hypothesis test provides a means for making decisions based on probabilities and evidence and serves as a simple quantitative model of how friendly and hostile nations would react to threats rationally under different circumstances.

A Bayesian hypothesis test may be derived from a dichotomous form of Bayes' Theorem. Let A be an event, such as a military attack or cyber operations that have comparable consequences; i.e., deaths. Participants don't know if A will happen, only that it may happen. The probability of A happening is $P(A)$ and the probability of A not happening is $P(\bar{A})$. The consequences, or cost, of inaction are C if A is true. The cost of unnecessary action when A is not true is $\bar{C}$. Let d be some data that is a probabilistic indication of A. Knowledge of d helps decide if an action should be taken to avoid A. The probability of observing d given A is $P(d|A)$ and the probability of observing d given $\bar{A}$ is $P(d|\bar{A})$. These definitions of cost may be thought of as the consequences of deciding contrary to the truth. One chooses to act on the belief that A is true if the following is true:

$$P(d|A)CP(S > s|A)P(A) > P(d|\bar{A})\bar{C}P(\bar{A}) \tag{5}$$

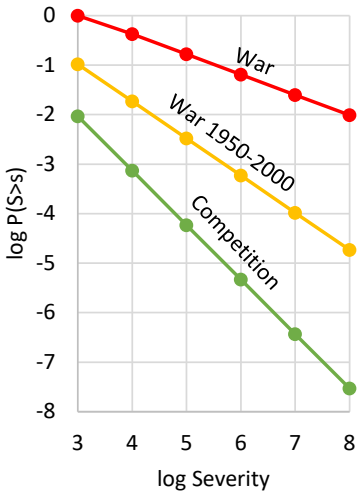

Figure 3. Log exceedance probability P(S>s) versus log severity s for three q values.

This particular dichotomous formulation of Bayes' theorem includes the costs for mistakes because rational decisions can't be made without taking into account risk; i.e., cost multiplied by probability. Note: for the purposes of calculating risk, we rewrite $P(S > s)$ in Eq. (1) in the conditional form as $P(S > s|A)$ to indicate that the severity of an attack depends on if an attack occurs. Thus, the risk of A is $CP(S > s|A)P(A)$ and the risk of $\bar{A}$ is $\bar{C}P(\bar{A})$. Intuitively, when the consequences of inaction (the left-hand side of Eq. (5) exceed the cost of incorrect action (the right-hand side of Eq. (5), then one chooses to act.

Eq. (5) may be written with both conditionals on the left-hand side as the ratio of the true-positive over the false-positive, and the right side the ratio of the risks of both choices:

$$\frac{P(d|A)}{P(d|\bar{A})} > \frac{\bar{C}P(\bar{A})}{CP(S > s|A)P(A)} \tag{6}$$

The left-hand side of Eq. (6) is referred to as the *likelihood ratio*, L (also called a Bayes factor), while the right-hand side is referred to as the *critical likelihood ratio*, L^*, weighted with consequences. To make a rational decision favoring a belief in A, L must be greater than L^*. If L is not greater than L^*, then the decision should be to do nothing:

$$L > L^* \tag{7}$$

Note that this is a simplified construct. Probabilities are more accurately defined by density functions. And other considerations, such as morality, ethics, economy, etc. would need to be weighed separately. However, this formulation will serve to demonstrate some of the characteristics of conflict during competition and war.

The math should be indifferent to whether a conflict is conventional or nuclear, so consider a hypothetical example of the critical likelihood ratio (L^*) where two nations, X and Y, have equivalent nuclear weapon capabilities. Both arsenals have the ability to destroy the other's population unless the nation under attack sends its population to hardened bunkers within 30 minutes, the amount of time it takes for the first missiles to arrive. However, every time such an emergency is declared, many people will die in the panicked rush to get to safety. Event A is where nation Y intends a surprise nuclear first strike against X, using all of its nuclear forces. Nation X has a launch warning system that provides data (d) indicating that Y's attack is underway. C is the consequences of deciding $\bar{A}$ when A is true and $\bar{C}$ is the consequences of deciding A when $\bar{A}$ is true.

The probability of an attack $P(A)$ against the U.S. can be estimated based on historic data. Using the Correlates of War (COW) Project data, we do that now. Between years 1816 and 2007, inclusive, the years covered by the COW project, there were 239 Intra- and Inter-State wars. Thus, on average, there is approximately 1.25 wars per year. Assuming a Poisson distribution ('a statistical distribution showing the likely number of times that an event will occur within a specified period of time'), this yearly average of wars leads to a probability of 0.71 that there will be at least one war in the world in any given year. Of the 239 wars, the U.S. was involved in 13. Therefore, $P(A) = 0.71 \times 0.054 = 0.038$. Conversely, $P(\bar{A}) = 0.96$.

Following the 2018 missile attack false-alarm in Hawaii, Fisher [13] argued that the Soviet downing of Korean Airlines Flight (KAL) 007 in 1983 could be considered as an example of a nuclear war false-alarm. Reportedly, the Soviet Union mistook KAL 007 for an American spy plane conducting pre-nuclear war operations. All 269 passengers and crew onboard were killed. For illustration, this number is rounded to two significant digits and used as the value of $\bar{C}$ such that $\bar{C}/C$=270/s, where s is severity in deaths. Therefore, the critical likelihood ratio for war is given by Eq. (8). It is shown as the red line of Figure 4:

$$L^*(War) = \left(\frac{270}{s18.6s^{-0.41}}\right)\left(\frac{0.96}{0.038}\right) \tag{8}$$

On the right-side of Eq. (8), the left bracketed ratio is the ratio of the false-alarm consequence in deaths over the inaction consequences in deaths. We call this "the deterrence ratio." The right-most bracketed ratio is the ratio of the probability the U.S. will not be attacked in any given year over the probability that it will be attacked in the same year. Another way to interpret Eq. (8) is to regard the numerator as the risk of incorrect action and the denominator as the risk of inaction. Even though this form of the equation can be simplified, we choose not to do so to retain some clarity.

To decide that an attack is underway, a likelihood ratio $P(d|A)/P(d|\bar{A})$ should exceed the critical likelihood ratio, L^*, in Figure 4. L^* should be greater than one, zero on the log scale. But this is not the case for war above 10,000 deaths, or 4 on the log scale, meaning the hypothesis test is useless because no indication of an attack is enough to send citizens to bunkers. If this result seems non-intuitive, consider that L^* is dominated by the severity s in the denominator of Eq. (8), which is consistent with our understanding of a high-risk phenomenon. The only way for L^* to become greater is to

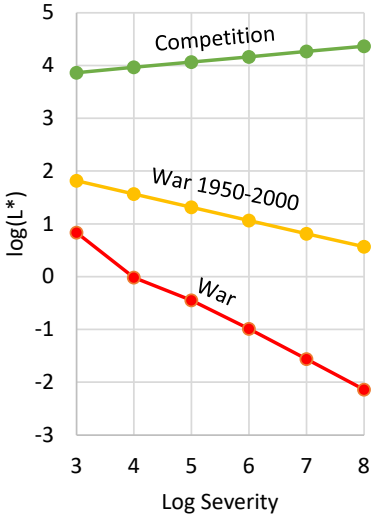

Figure 4. Log critical likelihood ratio L versus log severity s for three q values and where* $\bar{C}/C = 270/(s \times 18.6s^{-q})$.

increase $\bar{C}/C$, which serves as a deterrent for attack. A different result is obtained for war for the years 1950 to 2000. The detection ratio stays above one, starting near 100 for 1000 deaths, lowering to about 3.7 for 100 million deaths. See the orange line in Figure 4. The significance is that there is a high threshold for deciding that an attack is underway even though the exponent q has changed only slightly. The orange line is given by Eq. (9) below:

$$L^*(War\ 1950-2000) = \left(\frac{270}{s18.6s^{-0.75}}\right)\left(\frac{0.96}{0.038}\right) \qquad (9)$$

Low-risk interstate competition is achieved when q>1. The smallest increase above one involving two-significant digits finds the exponent equal to 1.1. Although arbitrarily chosen to be greater than one, our confidence in this assumption is bolstered by the works of Overill and Jantje who report that cyber-crime may be fitted to a power law with a q of 1.6 [14], suggesting that an overall q of between 1.0 and 2.0 is realistic. The equation for L^* in this case is Eq. (10) below:

$$L^*(Competition) = \left(\frac{270}{s18.6s^{-1.1}}\right)\left(\frac{0.96}{0.038}\right) \qquad (10)$$

To decide that an attack is underway during competition, a likelihood ratio $P(d|A)/P(d|\bar{A})$ should exceed the critical likelihood ratio, L^*, following Eq. (10). It is shown as a blue line in Figure 4. It indicates that the positive likelihood ratio must be greater than 10,000, 4 on log scale, to choose in favor of A. The significance is that the evidence for attack during competition must be very high, whereas for war it is small.

V. Conflict Esclalation Parameters

The forgoing analysis suggests that cyber-attacks, or any kind of conflict, could escalate if there are significant impacts to any one of the following sets of parameters: the fractal dimension q, the likelihood ratio $P(d|A)/P(d|\bar{A})$, or the deterrence ratio, $\bar{C}/C$. These are discussed in turn.

A. The Fractal Dimension

The network term $k\gamma\rho$, which is related to the fractal dimension q by double exponential (i.e., an exponent raised to an exponent), impacts the Bayesian hypothesis tests in an extreme way. It is comprised of the spectral radius, ρ, which may increase without bound with the number of nodes. Nodes may represent nations. Segments connecting nodes may represent alliances between nations. But nodes could just as easily represent Internet server farms in different nations and the segments be fiber optic transmission lines between them. For an n-by-n connection matrix, ρ ranges from $\sqrt{n-1}$ to n. The vulnerability, γ, is associated with forces that diminish or nullify the network specified by ρ. For example, the network term may be the target of information and cyber operations, reducing its contribution to the negative exponent and making the system more risky. The fractal dimension will normally be measured or obtained through simulation where the underlying mechanism need not be immediately evident. Such is the case for the q-value for war. However, in terms of network parameters k, γ, and ρ, the effect of a cyber-attack on the exponent of Eq. (4) should be calculable.

The theory that war is a network phenomenon posits that networks help prevent or mitigate war. While this seems counter to the *Fundamental Resiliency Equation*, Eq. (3), which attributes cascading failure to the network itself, the two ideas are not incompatible. The addition of network components, such as the alliances described by Jackson and Nei [12], can overlay an existing network. The cascading failure of one such network thus will be mitigated by the redundant network leading to larger q.

B. Likelihood Ratio

The parameter representing attack detection is the likelihood ratio (L). Obtaining $P(d|A)$ or $P(d|\bar{A})$ separately or together as a ratio depends on performance of real information systems or processes. Ideally, the performance of a detection system is assembled into what is called a Receiver Operator Characteristics (ROC) graph. Detection systems face many technical challenges and are a natural target of hostile information or cyber operations. Manipulating or interfering with a target nation's detection network could facilitate a surprise attack by decreasing L *or* decreasing L^*, suppressing the target's reaction time.

C. The False-Negative/False-Positive "Deterrence Ratio"

The "false-alarm" consequence will depend on what specific action is taken, whether it is sending people to shelters, launching a counterstrike, or some other action that intends to mitigate the impact of an attack. The value of $\bar{C}$ is a vexing question, more so than the value for C. The cost of a false-alarm is not easy to justify without real data. Furthermore, unnecessary action in response to a false-alarm can lead to a series of counter-actions that may escalate out of control. That is, a false-alarm could result in the same consequences as a true-positive: war. The deterrence ratio must be increased in order to prevent war. Figure 5 shows the

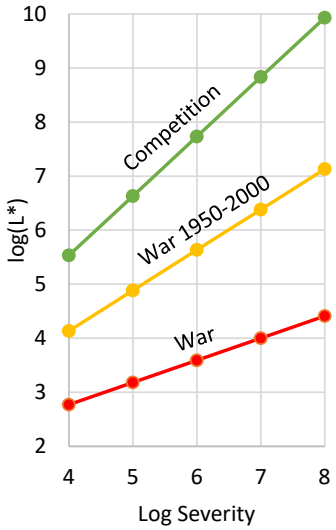

Figure 5. Log L^* vs *log severity s for three q values and* $\bar{C}/C = 1$.

critical likelihood ratios for war and competition if $\bar{C}/C$ is equal to 1.0. This is the case where the cost of unnecessary action is war itself and might be considered the extreme case. All three lines in Figure 5 indicate that $P(d|A)/P(d|\bar{A})$ must be dramatically higher to choose in favor of an attack, A. For the case of strategic war, the red line, L^* exceeds 100. Similarly, L^* for competition starts high and increases even more dramatically.

VI. Example Adaptations that Protect Competition

In this section we discuss specific examples of adaptations involving redundant networks, deterrence, and attack detection to illustrate how they protect peaceful competition from escalating as a result of cyber conflict.

A. Trade & Diplomatic Alliances Incorporating Detection

Larger L^* means a greater threshold for conflict escalation. Figure 6 shows how L^* increases exponentially with linear changes in q, indicating increase robustness against attack false-alarm provided that $\gamma\rho$ decreases. Redundant networks compensate for effects that would otherwise cause cascading failure. Extending or strengthening the alliances of the type cited by Jackson and Nei [12] should help stabilize competition, beyond that for war between 1950 and 2000.

Adding to an alliance a method for detecting attacks is an adaptation that amplifies an existing or redundant network. Bi- and multi-lateral treaties may include verification provisions. The Nuclear Nonproliferation Treaty (NPT), for example, is a long-lived diplomatic network started as part of the Atoms for Peace program in 1953 that has been maintained by the International Atomic Energy Agency since 1970. It has provisions for continuous verification of nuclear materials and technologies by a cadre of nuclear safeguards inspectors. Under the NPT, sharing of nuclear technology is encouraged for the use of civilian power, but not allowed if the technology is used for military applications. Thus, not only does this network increase stability of competition through the network parameters, it increases the true-detect/false-alarm ratio to improve rational choices about potential escalation of conflict.

B. Open Technologic Networks

Returning to Shannon's Maxim, there is an increasing abundance of evidence that open electronic networks and software contribute to the stability of interstate dynamics. Open systems are computer systems that provide a combination of interoperability, portability, and open software standards. They allow for increased communication, negotiation, and vetting of cybersecurity processes. Examples include the Internet, the Unix operating system, and the Firefox web browser. The top reasons individuals or organizations choose open source software are: lower cost, security, no vendor lock in, and better quality [15]. For these reasons, open systems comprise the bulk of computer technology in the world. These technologies increase the spectral radius, ρ, and decrease node vulnerability, γ.

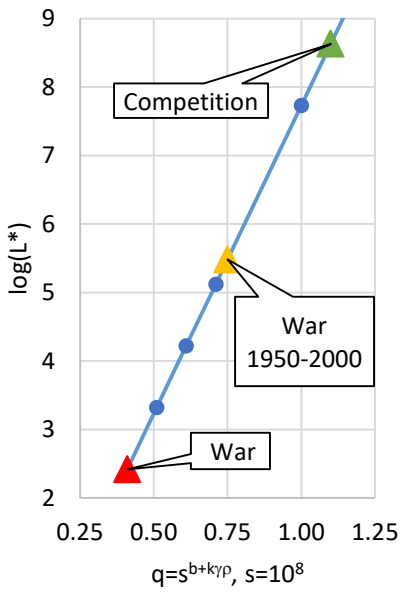

Figure 6. Log L versus q.*

Some open technologic networks were originally closed national security systems. The Internet is the most famous example of a national security technology that was made open to the public. Despite the difficulties it creates, its net effect is to help keep peace within and between nations. There are other examples. Many people don't know that GPS navigation signals were originally classified. It wasn't until the Soviet downing of Korean Airlines Flight 007 that it was decided the benefits of declassifying these signals outweighed the disadvantages [16]. Once GPS was made publically available, the private sector miniaturized the electronics which enabled the receiver to be added to cell phones. Despite navigation telemetry being broadcast only (i.e., unidirectional), GPS public availability increases network infrastructure by making information globally available via a small spectral radius while being simultaneously less vulnerable to cyber-attacks due to its unidirectionality [17]. An adaption that decreases vulnerability and spectral radius while maintaining global availability diminishes the loss of network resilience resulting from cascading failure.

C. Deterrence of Cyber Crimes

By way of the Bayesian likelihood ratio weighted with consequences, we've shown that a rational enemy will attack unless there is a deterrent. One reason that cyber-crime is so rampant is that there is little deterrent. There's a low probability of the offending individual or nation facing punishment or sanctions, so attacks are likely to continue. An adaptation of cyberspace that clarifies what constitutes national and international offenses and ensures commensurate responses with a high probability will help prevent attacks and help stabilize interstate competition. Goldman and McCoy argue that, "imposition of financial sanctions, public/private partnerships to disrupt tools of cybercrime, and activities to disrupt payment networks run by criminals who sell

fraudulent goods over the Internet" [18] decrease cybercrime. Their recommendations emphasize that it is as important to punish criminals if convicted as it is to lessen the chances that they will benefit from their crime.

Schwartz contends that deterrence of cyber-crime is a myth due to the unique nature of the medium and attackers [19]. Thus, detection of cyber-crime or -attacks appears as important as dispensing punishment or denying benefit. The Bayesian attack formula shows how detection is intertwined with prior probability, conditional probability, and consequences, suggesting that another adaptation be the automation of detection based on techniques such as the Bayesian hypothesis test.

VII. Conclusion

The power law of statistics, Shannon's Maxim, network failure theory, and Bayes' theorem were brought together in this study to create a parametric model of war and nonviolent interstate competition to enable a study of the tendency of cyber and other forms of attack to escalate conflict from competition to war and, conversely, how to lessen this tendency by modifying network parameters.

We manipulated the *Fundamental Resiliency Equation* to show that conflict, as represented by q, is in theory related to network variables b, k, γ and ρ by double exponential. The significance of this is that the exceedance probability will be extremely sensitive to network variables over the domain of their validity; i.e., $q > 1$. Our investigation relies on the researched conclusion that war has a q value reported by Cederman of less than one. Other q values have been reported [20].

Examples of creating and adapting networks to stabilize and protect competition were provided. Open networks, standards, and software continue to create technologic interstate alliances that further stabilize competition. Further stability can be achieved by making military information systems publically available, like what was done with GPS in the 1980s. Trade and diplomatic networks that build-in systems for detecting conflict should be expanded. Finally, deterrence and detection of attack seem to be inseparable for the case of cybercrime.

The method described in this paper for estimating an attack detection threshold is built on a rigorous mathematical framework on which to conduct further research. Preliminary results reported by Standley, Nuño, and Sharpe indicate that the severity of war follows log-normal statistics with a mean of 7900 deaths, standard deviation of 10, validity between one and 15 million deaths, obeys probability axioms in all cases, and is equally applicable to the Bayesian hypothesis test method [21]. These findings suggest that the power law is an approximation that is valid only for a narrow range of deaths and is not indicative of the underlying phenomena; e.g., preferential attachment.

The opinions, conclusions, and recommendations expressed or implied are the authors' and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government, or any other organization.

References

[1] Rauchhaus, R., Evaluating the Nuclear Peace Hypothesis:A Quantitative Approach, Journal of Conflict Resolution, Vol. 53, Issue 2, January 27, 2009.

[2] Snyder, G., 1965. The balance of power and the balance of terror. In Balance of power, ed. Paul Seabury. San Francisco: Chandler.

[3] 2018 Nuclar Posture Review, U.S. Department of Defense, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-Nuclear-Posture-Review-Final-Report.PDF.

[4] *Ibid*.

[5] Shannon, C. E., "Communication Thoery of Secrecy Systems", Bell systems Technical Journal, Vol 28-4, page 656 – 715, Oct. 1949.

[6] Gabison, G., "Policy Considerations for the Bockchain Technology Pulbic and private Applications," Science and Technology Law Review, Vol 19, 327 – 350, 2016.

[7] Andriani, P.; McKelvey, B. (2007). "Beyond Gaussian averages: redirecting international business and management research toward extreme events and power laws". Journal of International Business Studies. 38 (7): 1212–1230. doi:10.1057/palgrave.jibs.8400324.

[8] Cederman, L.E., "Modeling the Size of Wars: From Billiard Balls to Sandpiles." The American Political Science Review 97.1 (2003): 135-50. JSTOR. Web. 27 Apr. 2015.

[9] Duffield, M., War as a Network Enterprise, Cultural Values: The Journal for Cultural Research, Jan-April 2002, 6 (1&2):

[10] Simon, H. A. (1955). "On a class of skew distribution functions". Biometrika. 42 (3–4): 425–440. doi:10.1093/biomet/42.3-4.425.

[11] T.G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, 2e. Wiley, 2015.Gause, Georgii Frantsevich (1934). The Struggle For Existence (1st ed.). Baltimore: Williams & Wilkins.

[12] Networks of military alliances, wars, and international trade, Matthew O. Jackson and Stephen Nei, PNAS December 15, 2015. 112 (50) 15277-15284

[13] Fisher, M., Hawaii False Alarm Hints at Thin Line Between Mishap and Nuclear War, the New York Times, Jan. 14, 2018, https://www.nytimes.com/2018/01/14/world/asia/hawaii-false-alarm-north-korea-nuclear.html

[14] Overill, R.E. and J.A.M Silomon, Single and Double Power Laws for Cyber-Crimes, Department of Informatics, King's College London, Strand, London WC2R 2LS, UK, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.225.6194&rep=rep1&type=pdf.

[15] Guseva, I., "Bad Economy Is Good for Open Source". Cmswire.com. 2009-03-26.

[16] Pace, S. and G.P. Frost, Irving Lachow, David R. Frelinger, Donna Fossum, Don Wassem, and Monica M. Pinto, The Global Positioning System: Assessing National Policies. Santa Monica, CA: RAND Corporation, 1995.

[17] Standley, V. and E. Boucheron, Space-based Unidirectional Networks and Resiliency, (Accepted), QRS 2018.

[18] Goldman, Z.K. and D. McCoy, "Economic Espionage: Deterring Financially Motivated Cybercrime," 8 J. Nat'l Sec. L.& Pol'y 595 (2015- 2016).

[19] Schwartz, M.J., "The Myth of Cybercrime Deterrence," Bank Info Security, June 1, 2015. Online. Available at: https://www.bankinfosecurity.com/blogs/myth-cybercrime-deterrence-p-1867.

[20] Clauset, A., Trends and fluctuations in the severity of interstate wars, Science Advances 21 Feb 2018, Vol. 4, no. 2, http://advances.sciencemag.org/content/4/2/eaao3580.full

[21] Standley, V.H., F.G. Nuno, J.W. Sharpe, "The Validity of Log-Normal Statistics for the Severity for High Magnitude War," 2018, abstract submitted to NATO Science & Technology Organization, Systems Analysis and Studies Panel.