Journal of Strategic Security

Volume 8
Number 4 *Volume 8, No. 4: Winter 2015*

Article 3

How Power-Laws Re-Write The Rules Of Cyber Warfare

David L. Bibighaus
Booz Allen Hamilton, bibighaus@acm.org

Follow this and additional works at: https://scholarcommons.usf.edu/jss

pp. 39-52

Recommended Citation
Bibighaus, David L.. "How Power-Laws Re-Write The Rules Of Cyber Warfare." *Journal of Strategic Security* 8, no. 4 (2015) : 39-52.
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1439
Available at: https://scholarcommons.usf.edu/jss/vol8/iss4/3

This Article is brought to you for free and open access by the Open Access Journals at Scholar Commons. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

Introduction

This article deals with the unique uncertainty encountered in the cyber domain. Uncertainty in warfare is nothing new. Clausewitz once famously wrote that:

> "War is the province of uncertainty; three quarters of the factors on which action in war is based are wrapped in a cloud of greater or lesser uncertainty. Here, then, above all a fine and penetrating mind is called for, to search out the truth by the tact of its judgment."[1]

Good officers make plans knowing full well that the unexpected will happen and that they will have to adapt and change in the face of this uncertainty. As von Moltke said, "No plan survives contact with the enemy."[2] But good officers try to account for this uncertainty and figure out both what is possible and what is likely. This article will argue that assumptions about randomness in physical warfare do not apply to the cyber domain. Within information systems, the randomness encountered is different than the randomness normally encountered in the physical world. This creates the situation that, without a deliberate mental effort, an officer in the cyber domain will be inclined to make assumptions that are ill-suited to the battlefield on which he fights. Finally, this article will explore assumptions based on the physical world that should be re-examined for the cyber domain.

Two Kinds of Randomness

"The Die is Cast"

– *Julius Caesar, as he led his army across the Ruibcon*

Since ancient times, generals have linked warfare with the roll of a dice. By the mid-1800s, some of the first war games included dice to simulate the element of randomness in war.[3] This choice worked because it mimicked the kind of randomness we frequently encounter on the battlefield. Throw a large number of dice, add up their values and plot the result and you will get a bell curve. Gaussian randomness describes the variations in physical strength, speed, and agility our ancestors would have encountered in the African savannah and later on the battlefield. Intuitively, people know that there is a

[1] Clausewitz, Carl von, and Frederic N. Maude, *On War* (London: Kegan Paul, Trench, Trübner & Co LTD, 1908), 48.

[2] Barnett, Correlli, *The Swordbearers* (London: Eyre & Spottiswoode, 1963), 35.

[3] Ewalt, David M, *Of Dice and Men* (New York: Simon and Schuster, 2013), 97.

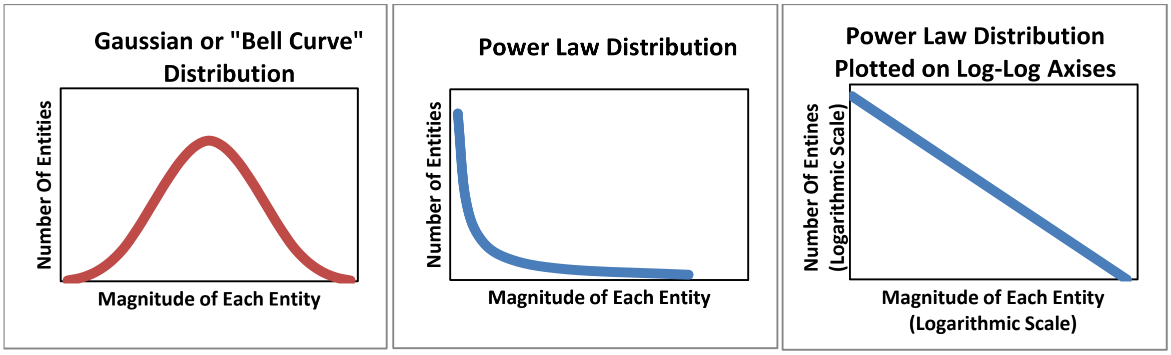
typical height, weight, strength, and speed for the humans, predators, and prey we find in our environment. Of course, we encounter deviations from this norm, but our brains know how to accept and understand these realities. Sometimes we see a large deviation from the norm, but as both generals and casino operators know, under Gaussian randomness with enough rolls of the dice things tend to "average out."

Recently however, many scientists have begun to observe a different kind of randomness that governs many of the phenomena in our high-tech world: the Power-Law.[4] The Power-Law can also be demonstrated by rolling dice, but we have to play a different game. Roll a dice. If the result is odd, the game is over and you score no points. If the result is even, you earn one point and can roll again. Every time from then on that you roll an even number, double your points and roll again. The game ends once you roll an odd number. In this game, half of the people will end up with nothing and a few very lucky people will finish with a large score. To understand a bell curve you must discover where the bell is centered (the average) and the width of the bell (the standard deviation). To understand a Power-Law, you must note what is happening on the extremes. Power-Law distributions are a general case of the "80-20" rule, where 80 percent of the impact comes from 20 percent of a population. One of the signatures of a Power-Law distribution is that if you plot it on a Log-Log scale, the result should be a straight line. Figure 1 shows a Power-Law versus a normal distribution.

[4] Barabási, Albert-László, and Jennifer Frangos. *Linked* (New York: Basic Books, 2002);, Albert-László Barabási, *Bursts* (New York: Penguin, 2010); Nassim Nicholas Taleb, *The Black Swan* (New York: Random House LLC, 2007); Steven Pinker, *The Better Angels of Our Nature* (New York: Penguin, 2011).

DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1439

Figure 1: Comparison of Random Distributions



Music sales, monetary wealth and book sales are all common areas of everyday life that follow a Power-Law distribution.[5] Most professionals in the music industry ignore what is happening with the "average" artist and instead concentrate on what is happening at the top of the charts. Select a professional musician at random and the odds are that the artist has only managed to sell a few copies of his/her works. However, within the pool of professional musicians are a few who are able to sell millions of albums. Despite thousands of artist working in the industry, only a small handful truly shape it. This is not the case with a plumber, dentist or carpenter. In these professions, the income distribution looks more like a bell curve. The reason that musicians, authors, and artists have such a variable income, whereas dentists, plumbers, and carpenters do not, is that the former work primarily with information whereas the later work primarily with physical entities.

There are three other important differences that set the Power-Law distribution apart from Gaussian randomness. The first is the difference in magnitude between an outlier and the average. Under a bell curve distribution, an outlier can only deviate so far from the norm. Out of roughly seven billion people, Sultan Kosen is currently the world's tallest living man.[6] While being 8'3" is enormous, his height is only a factor of 1.5 times taller than an average sized adult male. Under a bell curve, there comes a point where anything beyond that is astronomically rare. In contrast, under a Power-Law distribution, it is common to see events that deviate from the norm by a factor of more than a thousand. If, instead, people's height (governed by a bell curve) were to correspond with their income (governed by a Power-Law), the earth would be populated with billions of midgets and a

[5] Taleb, *The Black Swan*, 33.
[6] Guinness World Records. "Tallest man - living" February 9, 2011, available at: *http://www.guinnessworldrecords.com/world-records/tallest-man-living*. accessed: June 24, 2014.

handful of giant colossuses such as Bill Gates. The presence of extreme variations from the norm is the first key to understanding a Power-Law distribution.

The second key to understanding Power-Laws is that they arise from two factors: Growth and preferential attachment.[7] Power-Laws occur on systems that are allowed to grow and change in a way that reinforces success. Indeed, Power-Laws are a mathematical signature of evolution.[8] Bill Gates' fortune did not spring into being all at once. Rather it grew with the success of Microsoft as more and more PC users chose the Microsoft operating systems and productivity tools.

The third and final key to understanding Power-Laws is the difficulty in identifying which small advantages will become enormously consequential. In the popular television show American Idol, talented singers compete for a single record contract. The show is a vivid example of a Power-Law distribution at work. Thousands compete, but most receive nothing. A few receive a trip to Hollywood and fewer still receive a small measure of fame. For one winner however, the rewards are enormous. The entertainment of the show is derived in large part from the unpredictability of the outcome. Consider a record producer. Even for a well-trained professional, accurately differentiating between singers who are in the 67.8th and 67.9th percentiles is very difficult. Fortunately that task matters little. However differentiating between who is in the 99.8th and 99.9th percentile (just as difficult) is extremely important because of the enormous differences in sales outcomes.

For a more serious example, Stephen Pinker has noted that the casualty counts in war follow a Power-Law distribution.[9] Most conflicts are relatively bloodless, but a few are absolutely devastating. We shake our heads in disbelief at the picnickers who came to watch the first battles of the US Civil War, because they believed the rebels would be quickly crushed. Likewise, all of the generals in the early days of World War I assumed that the conflict would end quickly. But we miss the key point that under a Power-Law system, it is reasonable to assume that most wars are short and relatively bloodless. The tragedy is that when events fall in just the right way, the outcome is very different. Even worse, few will recognize it until it's too late.

[7] Barabási, *Linked, 87.*
[8] Ibid, 208.
[9] Pinker, *The Better Angels of Our Nature, 218.*

Multiple authors have shown that Cyberspace is full of Power-Laws. The physical topology of links and nodes on the Internet follows a Power-Law distribution.[10] The distribution of web page links also follows a Power-Law distribution.[11] The propagation patterns of computer viruses are explained by Power-Law distributions.[12]

This article argues that there is a deep and hidden assumption of Gaussian randomness that underlies much of our strategic thought. However, within the cyber domain, a different kind of randomness dominates. This observation demands that military professionals challenge some common assumptions as they prepare for and conduct war.

Randomness and the Differences Between Cyber and Physical Weapons

Imagine the best soldier living in the Roman Empire. His superior strength, speed and agility place him six standard deviations above the norm: literally a one-in-a-million soldier. Being mortal, his strength, speed, and agility are superior to his opponents, but as was discussed in the previous section, not astronomically so. By himself the soldier could make a difference in the outcome of a small battle, but not a large campaign. This is because his physical variations are governed a bellcurve distribution. The Tofflers observed that we evaluate weapons by their range, speed, and lethality.[13] Technology can improve the range of a bullet or the lethal radius of a bomb, but even today, variances in these characteristics are still described with a bellcurve.

Now imagine the impact that a one-in-a-million cyber warrior could have in a cyber conflict. The impacts of cyber weapons (and by extension those who create them) seem to be governed by a Power-Law distribution. In other words, most weapons will have little impact, but a few will be extremely consequential.

Defining a Cyber Weapon

In this article, a cyber weapon refers to a unique exploit or technique, but does not account for the number of copies in existence. In the physical world,

[10] Faloutsos, Michalis, Petros Faloutsos, and Christos Faloutsos. “On Power-Law Relationships of the Internet Topology,” *SIGCOMM Computer Communications* 29:4 (1999): 251–62.
[11] Barabási, *Linked,* 66.
[12] Ibid, 133.
[13] Toffler, Alvin, *War and Anti-War* (New York: Little Brown & Company, 1993).

having ten identical copies of an aircraft carrier is roughly ten times better than having only one.[14] But having ten identical copies of the same exploit would not be appreciably different that possessing a single copy.

For purposes of this definition, a unique weapon may only be a small evolutionary change from an existing exploit. Researchers have noted that the frequency of calls made to different software libraries follow a Power-Law distribution.[15] What is striking is that the same pattern appears when biologists examine the distribution of known proteins to biological processes. In other words, software bears the same mathematical signature of evolution. This shouldn't surprise anyone who has actually worked with software. Experience would suggest that exploits, just like other software, evolve as well.

Cyber Weapon Effectiveness

If the effectiveness of cyber weapons operated under a Power-Law distribution, we would expect that most weapons would impact only a small number of systems, but a few could exploit many hosts.[16] Further, we would expect that small environmental factors, such as the structure of the network or the configuration of the target, would result in very different outcomes for similar exploits. In addition, we expect that a small variation in the design of one cyber weapon might make a large but unexpected impact in its effectiveness.

What we experience on the Internet squares with our expectations. One example of the Power-Law phenomena in cyber warfare is computer viruses. Consider that on 18 June 2014, an "average" day, the Wild List[17] reported only 1,820 variations of malicious logic that have been observed "in the wild," meaning they are actively propagating on real systems. Yet an anti-virus scanner has signatures against hundreds of thousands of unique exploits. McAfee's website reported discovering 30 new instances of malicious logic in a single day (June 23, 2014). All of the instances were rated as a low threat.

[14] Toffler, Alvin, and Heidi Toffler, *Revolutionary Wealth* (New York: Random House LLC, 2006), 100.
[15] Sergi Valverde, Ramon Ferrer Cancho, and Ricard V.Solé, "Scale-free Networks from Optimal Design," *SFI Working Paper: 2002-04-019* (Santa Fe, NM: Santa Fe Institute, 2002): 512-517, available at *http://www.santafe.edu/media/workingpapers/02-04-019.pdf*.
[16] Taleb, *The Black Swan*, 206.
[17] WildList Organization International, "The Wildlist," available at: *http://www.wildlist.org/CurrentList.txt*.

DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1439

This is consistent with a Power-Law distribution. Thousands of new viruses are constantly created every year. Most are only seen once. Only a few are ever observed in the wild and most of those cause little damage.

Yet on the other extreme, consider the Conficker worms. SAIC estimated that by March of 2009, Conficker.A had infected 4.7 million IP Addresses and Conficker.B had infected 6.4 million systems. Confiker was an example of a piece of malicious logic that was serious enough to warrant an Infocon Yellow[18] on the Internet Storm Center (Internet Storm Center, 2014). According to their history, an Infocon Yellow event occurs a little more than once a year. An Infocon Orange[19] event is even more rare, occurring briefly from the Code Red worm in 2001 and again from the Slammer worm in 2003. An Infocon Red event has never occurred since the Storm Center's creation.

The point of these examples is to show that malicious logic strongly exhibits the characteristics one would expect under a Power-Law distribution. Most new cyber weapons do next to nothing, while a few have an enormous impact. This might create a tempting target for budget cutters except for one small problem: We cannot predict the effectiveness of cyber weapons.

Predicting the effectiveness of cyber weapons

Because the effectiveness of a cyber weapon is contingent on so many variables, it is virtually impossible to predict the effectiveness a-priori. When Robert Morris created the Morris Worm in 1988,[20] he had no idea that it would impact the Internet as severely as it did. Likewise when David L. Smith created the Melissa virus he had no idea it would cause a global impact.[21] In both cases, the authors had placed controls to limit the spread of their attacks, and in both cases the exploits unexpectedly overwhelmed their control systems.

The phenomenon of unpredictability is a feature of Power-Law distributions. At the extreme, a tiny variation can have a huge difference in outcomes.[22] But

[18] Infocon Yellow is an event where "impact is either unknown or expected to be minor to the infrastructure. However, local impact could be significant."

[19] Infocon Orange is as "a major disruption in connectivity is imminent or in progress."

[20] Eugene H. Spafford, "The Internet Worm Program: an Analysis," *Purdue Technical Report CSD-TR-823* (West Lafayette: Purdue University, November 2, 1988), available at: *http://spaf.cerias.purdue.edu/tech-reps/823.pdf*.

[21] Ronald B. Standler, "Examples of Malicious Computer Programs," October 5, 2002, available at: *http://www.rbs2.com/cvirus.ht*m.

[22] Taleb, *The Black Swan*, 232.

observing tiny variations is, by definition, difficult. The Power-Law randomness of a cyber weapon arises in part because its performance is dependent on its "fitness" to the environment at the time. Since the cyber environment is complex and constantly changing, cyber warriors cannot know for sure how it will perform with certainty until they actually use it.

Thus the mindset of employing cyber weapons must be radically different than the mindset of a soldier employing weapons in the physical world. The soldier takes it for granted that the way a bullet interacts with armor or flesh is consistent and predictable. Of course, sometimes that soldier might encounter a lucky shot or a dud. But these considerations do not affect how a soldier employs his weapon. On the other hand, a cyber warrior must constantly be aware that the environment is in flux. Systems are constantly being patched and upgraded and users are constantly adding and removing systems and applications from their network. What was an effective attack today could be rendered useless tomorrow.

The Challenges of Randomness in Cyberspace To Strategic Thought

Consider once again the one-in-a-million super soldier. In the world of the bell curve, even great soldiers must exist within the realm of human abilities. A wise general may be thankful to possess such a gifted soldier, but he understands that the success of his army ultimately rests on the collective efforts of a host of average soldiers. The Red Baron may be useful as a source of propaganda, but the overall progress of the air campaign will be determined in the end by the total effort of average pilots.

With Power-Law weapons, it is the extremes that make the greatest contributions. A one-in-a-million cyber warrior could create a cyber weapon more impacting than the efforts of a small army of "average" cyber warriors. The problem that faces us today is that our military and law-enforcement structures are designed specifically for a world of averages. The following examples show some of the ways that "bell curve thinking" has shaped well-established military assumptions.

Cyberspace's Challenge to Sun Tzu

Consider Sun Tzu's most famous dictum:

> “If you know the enemy and know yourself, you need not fear the result of a hundred battles.”[23]

How do cyber warriors know their adversary in cyberspace? For that matter, how do they know themselves? We have already argued that in a Power-Law system, the extremes have a significant impact, but identifying who is in the extremes ahead of time is virtually impossible. Thus, perhaps the most consequential question in cyber warfare is: “How do we measure the power of a cyber army?” Notice the hidden assumption Sun Tzu makes when he offered the following counsel:

> “It is the rule in war, if our forces are ten to the enemy's one, to surround him; if five to one, to attack him; if twice as numerous, to divide our army into two. If equally matched, we can offer battle; if slightly inferior in numbers, we can avoid the enemy; if quite unequal in every way, we can flee from him.”[24]

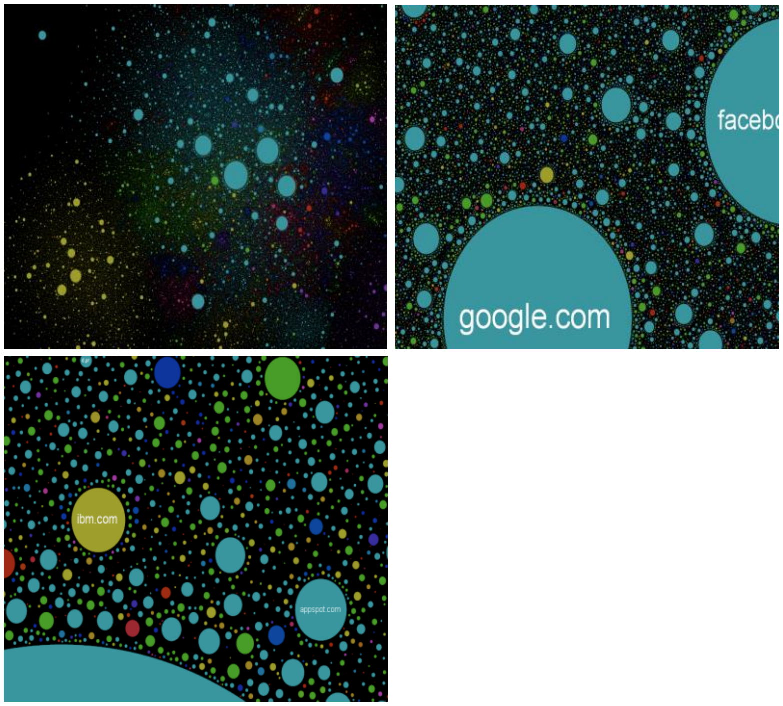
For Sun Tzu, measuring power is achieved simply be counting average bodies. This works in the world of the bell curve where the extremes average out. In the world of the Power-Law, it falls apart. For example, consider one publishing company with 1,000 randomly chosen authors and another publishing company with just one: J.K. Rowling. Who will sell more books? In cyberspace, as in all Power-Law systems, you cannot accurately estimate power with a simple census. You could make a quality assessment about the cyber forces you possess. However, as stated before, differentiating between the top .1% and top .001% is nearly impossible, but in a Power-Law system extremely consequential.

Cyberspace’s Challenge to Understanding the Terrain

No rational commander would go into battle without an understanding of the terrain. Yet in cyberspace, a usable map is hard to come by. Figure 2 is a map of the Internet produced in 2011.[25]

Figure 2: Map of the Internet. Each view focuses on a narrower portion of the Internet, but the Power-Law nature is evident throughout.

[23] Sun, Tzu, *The Art of War* trans. Lionel Giles (Singapore: Graham Brash (Pte) Ltd., 1993), Section 3.18.
[24] Ibid. Sec 3.8-9.
[25] Enikeev, Ruslan, "The Internet Map" 2011, available at: *http://internet-map.net*.



The map looks like a collection of fireworks and at first glance does not appear very useful. Yet those fireworks are a visual representation of a Power-Law Distribution. The centers of the bursts are the extreme ends of the distribution, and the edges of the bursts are the more common nodes. A wise commander should recognize that the centers of the bursts are the key landmarks of the battlefield. There is no escaping this reality. As noted earlier, this pattern appears at various levels of abstraction (such as the interconnection of the physical systems that comprise the internet and the networks of hyperlinks that comprise the world-wide web). In addition, a Power-Law distribution is sometimes referred to as a Scale-Free distribution. Whether one is looking at a map of the entire Internet, or the network of a country or even a single military base, the firework pattern will appear over and over again. A wise commander will understand this feature of the cyber battle space.

Cyberspace's Challenge To The Law of Armed Conflict

There are three governing principles in the Law of Armed Conflict: Military Necessity, Distinction, and Proportionality. Of these, Proportionality is the most at risk. Proportionality requires a commander to "refrain from deciding to launch any attack… which would be excessive in relation to the concrete and direct military advantage anticipated".[26] If the effectiveness of a cyber weapon can vary greatly and cannot be known a-priori, then Proportionality is almost impossible to reliably achieve with a cyber weapon. Nations might attempt to place controls that would limit the effectiveness of a cyber weapon. However, both the previously mentioned Morris worm and Melissa virus contained such limiting controls. The reality is that these weapons are often created in secret and tested on small, isolated ranges. Once employed in the real world, there is a small chance that the weapon could become significantly more impacting than anticipated. Would the international community judge such an event by the attempt at control or the result?

Cyberspace's Challenge to Recruiting

In the physical world, governments can reliably convert tax revenues into quantities of well-equipped police officers and soldiers. The greater the disparity between the resources a government invests and a potential adversary, the greater the likelihood the government will prevail. This works because the government only needs to find an average soldier or police officer. Spending more money on an army can result in proportionately more power. With cyberspace, the challenge is to focus on quality more than quantity. Simply recruiting more bodies will be wasteful compared to recruiting and retain the right bodies.

Cyberspace's Challenge to the Peace of Westphalia

The Peace of Westphalia established the principle that nations were sovereign within their own borders. Other nations are prohibited from interference with another nation's domestic affairs. Under this system, a government has the obligation to suppress non-state actors from impacting the security of other nations. To comply with the treaty, a functioning government has to raise a force that is more powerful than any potential rival within its borders. As noted above, governments today simply convert tax dollars into power armies.

Unfortunately in cyberspace, a larger force of average cyber warriors may not be more effective than a few exceptional cyber warriors. The problem is most acute for a small nation. Even though a small country may be able to enforce law and order on the street, it is perfectly conceivable that a small number of

[26] International Committee of the Red Cross (ICRC), "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)", 8 June 1977, 1125 UNTS 3, available at: *http://www.refworld.org/docid/3ae6b36b4.html*.

exceptional hackers could effectively out-compete a number of average government security officers in cyberspace. If a nation cannot establish a monopoly of violence within its borders, we label it as a "failed state." The problem for the world order is how to handle a smaller nation that is a responsible member of the world order and yet a "failed state" in cyberspace. It is likely that many smaller nations may join forces to combat cyber warriors. But what about the nations that both refuse to surrender their sovereignty and cannot control what occurs within their physical borders?

Recommendations

If cyber weapons do exhibit Power-Law randomness, then what are the actionable items? Here are three possible initiatives:

Recognize Military Structures Built on "Bell Curve" Assumptions

The first step of change is to admit the existence of a problem. How power is measured, how officers plan, and what is acceptable in warfare have all evolved from assumptions about an "average" soldier. In cyberspace if these models only consider the average case, they will miss the most important features of the domain. Understanding the Power-Law distributions and how frequently they occur in cyberspace should be an essential part of professional military education.

Rethink How We Recruit, Reward, and Retain Cyber Forces

The Power-Law randomness of cyber warfare puts the government in a similar position to a large publishing house. As noted earlier, a publishing house cannot guarantee a larger market share by simply signing a larger number of average authors. For a publishing house to stay profitable, it must do two things: effectively identify top performers and keep them happy. Currently recruiting in the military is primarily focused on numbers. In cyberspace, the talent scout may be a more appropriate model.

Currently, the American military uses an "up or out policy" with its existing personnel. This is perfectly reasonable because keeping even the most talented operators in the weapon systems does not make a significant difference to the effectiveness of the force. However, in cyberspace this policy is indefensible. Moving or promoting the most gifted cyber warriors out of their job will mathematically make noticeable impact to the force. Likewise, a rational compensation policy for cyber warriors will likely have the result of a commander making less than an exceptionally gifted operator.

DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1439

The reader may be tempted to draw a comparison between the small number of Special Forces operators and the elite cyber forces. The difference is that, in a physical conflict, the regular forces do the bulk of the combat. In Cyberspace, the elite forces will have a much greater impact on the battlefield relative to their numbers.

Design Strategies to Take Advantages of Power-Law Randomness

The U.S. Air Force Standard Desktop Configuration is a classic example of a failure to understand the challenges of Power-Law randomness in cyberspace. The logic is to create and manage a single configuration that represents the most secure known way to build an average office machine. This program may have saved costs, but it also created an enormous vulnerability. This configuration may be highly resistant to a typical attack. But by making the network so homogenous, if a weapon can work against one system, it is likely effective against all. The challenge for the commander in the cyber world is to be prepared for the extreme attack. The standard desktop may provide excellent resistance to the average weapon, but it is uniquely vulnerable to the exceptional. Losses in the cyber world will occur in a more abrupt manner. A wise commander will recognize that no amount of cost savings is worth creating a critical vulnerability that could fail at exactly the wrong moment. In a similar manner, successes will be more abrupt in the cyber world. A successful commander will be prepared to capitalize on wild successes and take steps to limit wild failures.

Conclusion

Military commanders are trained to expect uncertainty. When they commit to a course of action, they are taking a calculated risk. This article has attempted to argue that a commander who brings assumptions from the physical world into cyber warfare is playing the wrong game. Cyberspace is a land of extreme events. Strategies that might be considered safe in physical warfare can be exceptionally dangerous in the cyber domain. This is extremely counter-intuitive. Cyberspace is the first war-fighting domain that is a wholly man-made creation. As such, an observer might be tempted to think that it was designed. In truth, cyberspace evolved. The physical topology, the organizational topology, and the internal structures, all bear the signatures of countless small evolutionary changes. This evolution is constant, rapid, and unforgiving. As a result, entities in cyberspace display behaviors that are far from those to which military professionals are accustomed.

This article has argued that if the effectiveness of weapons in cyberspace follows a Power-Law distribution then there must be a change to cyber strategies. If cyber weapons exhibit such a radically different behavior, the way militaries plan, recruit, and train their forces must necessarily change. Success on these battlefields will depend on people who can distinguish between those principles that have worked in the past and will still apply to cyberspace and those that will not.

DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1439