Can Attrition Theory Provide Insight for Cyber Warfare?

Stephen Defibaugh and Donna Schaeffer
Marymount University, Arlington Virginia, United States of America
Stephen_Defibaugh@marymount.edu
dschaeff@marymount.edu

Abstract: This paper explores the notion that cyber-adversaries can use classic attrition tactics to cause weakness to address follow-on attacks. We conducted a grounded theory study that reviewed historic literature to identify parallels between past attrition tactics and cyber warfare. From historical examples, we see the possibility of an adversary conducting an asymmetric campaign by flooding the adversary with false-positive attacks in order to have them drain resources. For a modern perspective, we interviewed subject-matter experts from a US military command. Thematic analysis demonstrates a link between attrition and cyber-maneuver warfare. One significant finding is that most subject-matter experts agreed a culture of compliance, which encourages a full resources response to security events given full resources, can reduce the ability to maneuver appropriately and takes away from the focus on critical mission functions that cyber security is actually in place to protect. Other common themes that surfaced include that some interviewees believed their organizations were not prepared for cyber war nor are they resourced adequately to respond to a state of cyber war. Issues that need further study are the need to compare and correlate telemetry and metrics of incident responses and better tracking of the dollar-cost value of incident response and cyber tactics.

Keywords: cyber, attrition, compliance, cyber warfare

1. Introduction

With the emergence of cyber space as a domain of future warfare, it remains a contested territory that has many competitors present maintaining an equal number of independent objectives and goals. As shown through history, with the emergence of each new domain, such as sea, air, and space, we see potential maneuvers for advantage and domination of each unexplored area (Defibaugh, 2021). Often times, these competitions bring diverse groups and individuals into conflict. Accepting this, it is not surprising to see maneuvering extend into the cyber realm (Applegate, 2012). One of the challenges is the popularity in the mentality of deterring or preventing the single attack or multiple attacks aimed from a single actor. In many cases, this is a vague and multi-headed beast even in the best of circumstances. There are often many solutions for the different types of problems, and very few instances of a clear-cut answer that will address a cyber security need. In the face of this particular problem many leaders turn to compliance-based policy and guidance that provide generic steps and mitigations (Defibaugh, 2021). These generic steps and mitigations are often used as the only measurement for success in today's current environment. In this mentality of regulatory or policy compliance, organizations seemingly desire to spend more resources in an attempt to remain compliant in the eyes of regulatory agencies and the media, regardless of impact or defense against the likelihood of adversary engagement. These provide short-term mitigations to specific issues but do not always scale up to consider the longer-term, higher perspective.

Many decisions by cyber security professionals or organizational leadership are often made as responses to intelligence that is gathered regarding threats to an organization's weaknesses. These threats can come from a wide spectrum of possible actors ranging in skill and motivation; from basic scripting and building skills to advanced adversaries looking to establish a near-permanent foothold within systems. The advanced adversaries are more willing to play a long game and may not always use the most sophisticated methods when simpler tactics will achieve the same goal. The advanced use of tactics, techniques, and procedures (TTPs) are often like a fingerprint that are used in their attribution. Increasingly, we see signs that advanced persistent threats (APTs) are provided resources by, or are directly controlled by, nation-states in an effort to either disrupt or gain another nation or organization's resources (Defibaugh, 2021). In 2006, elements of the United States Air Force Cyber Command and the Department of Defense began to incorporate the concept of cyber warfare into their operational doctrines (Butler 2013).

However, as time has progressed, those involved in these seeming cyber warfare campaigns have witnessed a regular increase in threats and attackers with no real definition of what the indicators of compromise (IOCs) or the attributes of a cyber war might even look like. In an environment where the use of advanced TTPs in a cyber war could mean using tactics similar to kinetic warfare, we may begin to see the use of cyber as a means for attrition warfare instead of the highly technical attacks we are used to seeing publicized in the media. Large,

complex organizations may even be exposing themselves to such attacks by attrition by reacting to each individual threat or false attack in a very predictable manner.

2. Examining the Strategic Impact of a Compliance & Response Mentality

Despite increased activity by threat actors and recognition of cyber threats in the global media, studies have not fully explored the concept that reacting to every security incident with full resources could be used as a method to attack an organization, possibly denying or degrading the targeted organization from accomplishing its mission or goals (Defibaugh, 2021). The second topic of concern is that there are no available indicators of compromise that identify when malicious cyber activities go beyond small-scale attacks and into the realm of cyber warfare. The amount of qualitative and quantitative research on a cyber-attack through attrition as a viable attack method has not been fully realized. There are many resources that early on identified cyberspace as the next domain of warfare (Harris 2018). Other works focus on the possibility of future multi-domain warfare where cyber wars will be fought alongside more conventional kinetic combat. There are a surprising number of early works documented from 2006 through 2012 that suggest that there are bridges between kinetic and cyber warfare. Nevertheless, none of the materials identified in the early research has attempted to study any direct use of attrition tactics as viable methods of cyber warfare. Even so, some organizations appear very willing to proceed without any consideration or exploration into the idea of regular drain on resources being weaponized against them. Any thought of exposure to a consistent resource drain, despite long-term impact that might prevent them from adequately responding to a single or multiple adversary attackers, is entirely suppressed.

This article addresses two issues. The first issue is the exploratory examination of classic attrition tactics used by advanced cyber adversaries to exploit the current compliance driven and reactionary posture of United States-based organizations in order to weaken them as a part of a coordinated cyber warfare campaign. Second, qualitative research was conducted to determine if experts in the cyber security field have considered the concept of attrition as a tactic to conduct cyber warfare (Defibaugh, 2021). In order to examine this gap in the research, an exploratory qualitative methodology, using an exploratory grounded-theory approach, examined historical examples of warfare where attrition was used to degrade or deny adversarial advantages. The preconceived notions of attritional conflict leading into World War I will be examined along with literature that reviews maneuvering and relationships between attack and defense costs. This research study focuses on the exploration of the concept where cyber attrition tactics as a component of a cyber war campaign to deny or degrade US-based organizations as it is executed at a nation-state and organizational level.

3. Assumptions, Limitations, and Scope

A limitation of this research is that it is exploratory in nature and will only serve to essentially expose and explore a potential area in cyber security research. It will not be able to provide mitigations or corrections if the research questions are answered. The scope of this research will consist of cyber war and cyber warfare that would be executed at the nation-state level. As stated by Scott Applegate (2012), cyberspace appears to be more of a contested territorial domain that includes competitors from state and non-state domains, organized groups, proxies, and individuals. For the purposes of this research, electronic warfare and cyber terrorism will not be the focus. As this is an exploratory research case, the methodology was utilized from similar exploratory studies (Defibaugh, 2021). An assumption that is present during the course of this research is that cyber security experts that occupy similar positions with similar qualifications are qualified to maintain informed, professional opinions that are grounded in logic and reason.

4. Reviewing Conflicts and Cyber Security

William Philpott (2015) defines attrition as, “the cumulative exhaustion of the enemy’s fighting capacity” (Philpott, 2014). When we consider wars of attrition we often think about a number of different scenarios ranging from a siege of a fortified installation to people in trenches unable to advance or retreat. There are many examples of attrition warfare in human history. However, if we consider a series of events that involves multiple nation-state actors that include warfare beyond simple shooting, and that has been well documented, then the events that take place in the World War I provide an excellent area to examine. During World War I, the German military term for the strategy of attrition under State Siege Law was *Ermattunsstrategie* (Philpott, 2014).

Attritional strategy during conflict is effectively predicated on destroying or annihilating adversarial forces faster than the adversary could effectively replace them (Philpott, 2014). However, in 1915, and even in some cases before that time, a shift in strategic thinking began to take place on both sides of the conflict. Before the war

was started in earnest, the German general staff outlined a plan, which concluded that a protracted fight might end up ruining Germany economically. They faced opposition on multiple fronts, and if one opponent could be annihilated, then a second opponent might be worn down through an attritional struggle (Philpott, 2014). We note that in history, their choice had an impact on post-World War I German economics. Military strategy was decidedly amateurish. The failure of the leaders on both sides was often attributed to the differentiations between tactics, operations, and strategies, while completely ignoring the huge influence of resources and the constraints of logistics (Philpott, 2014). Presently, a worrisome parallel in the field of cyber security and cyber warfare emerges. If decision makers and subject matter experts are unable to take a step away from the immediacy of cyber security decision loops, then we may be resigning ourselves to repeat the same mistake and confuse what we think is strategy with tactical operations. When an adversary is able to invade the decision loop of another and force them, from a strategic level, to operate on a small, tactical scale, then the defending side is fighting a losing battle. This was a concept that Lloyd George, the British Prime Minister from 1916 to 1922, fundamentally failed to grasp. When both sides have millions of men in reserve and an efficient method of communication, most strategic initiatives will result in a stalemate (Lloyd George, 1982). This plays into the cyber realm very well if we consider the Internet as a force multiplier. In a modern sense, we may have numerous enemies that can exist in the cyber realm, as they are easily created and the Internet provides them with a nearly unlimited means of efficient communication. The French strategy, in July 1915, was to overthrow the Germans with simultaneous attacks that would not necessarily annihilate them outright, but would more-so overwhelm them on multiple fronts (Prete, 1915). The principle strategy of Erik von Falkenhayn, the second Chief of the German General Staff, was aimed at breaking the cohesion and will between Germany's adversaries. He planned to do this individually and collectively by destabilizing their united front. The thought process was that by engaging in battles on multiple fronts and inflicting heavy losses, this might encourage capitulation (Philpott, 2014).

5. Strategy During Cyber Maneuvering

We see in the previous section that conventional warfare not only shares a potential complementary relationship, but that cyber warfare is able to incorporate elements of conventional warfare using the Internet and information technology as a force multiplier. Next, we will examine how maneuvering in the physical domains has already begun to translate into maneuvering during cyber operations. According to Scott Applegate (2012), though conventional and cyber warfare differ over the amount of time that activities take place and their relation to varying strategies, the ultimate principle of maneuvering during a conflict, either cyber or conventional, has often been an important, if not deciding factor . If we look at historical examples of new domains and territories, it is unsurprising that cyberspace is a new domain where dominance is sought. Exploration of domains, such as land and sea, became the battlefields where new maneuvers and tactics were developed. Later, the same occurred for air and space (Applegate, 2012). As we consider cyberspace as a war-fighting domain, it is expected that it will become a contested territory vied for by numerous competitors, which may include state and non-state actors, organized groups, and even private individuals (Applegate, 2012).

The US military describes the concept of maneuvering as, "The disposition of forces to conduct operations by securing positional advantages before and or during combat operations" (Joint Publication 3-0, 2011). In historical examples, maneuvering would look like armies attempting to capture or defend strategic locations, governments may attempt to sequester or impinge on another nation's ability to engage in maneuvers or warfare through economic or strategic means, or any method or process that would give one actor an edge over another. In cyber terms, this may more resemble methods or processes employed to attack or defend information, which would constitute as the same since it provides an edge to one side over another (Applegate, 2012). In present conflicts, the targets of value are now focused on the capture of critical computing resources, industry and military secrets, and the infiltration of critical civilian and military infrastructure (Applegate, 2012). These targets, just like the Gallipoli Peninsula and Vimy Ridge in World War I, are critical areas of leverage, and the capture or denial of these would give one actor the edge over the other. This is an example that illustrates a clear parallel between the underpinned paradigms of conventional warfare and cyber warfare.

Colonel John Boyd described maneuvering as, "Operating inside of an adversary's decision loops and penetrating his moral-mental-physical well-being in order to destroy him from inside and remove his will to resist (Boyd, 1986). In this context, we start to see an application of an overall strategy forming. The established goal of attritional warfare is to exhaust the enemy's fighting strength and will to resist. Operating inside an enemies' decision cycle and eroding their will to continue fighting seems to be an effective way of conducting warfare. This type of attack is even more effective than those only in the physical domain, when the attack leverages the Internet as a force multiplier, which is both effective and very inexpensive to conduct. When we frame strategies

in this manner, then we can start to better understand the idea of cyber maneuvering as an application of force. The purpose of this application of force may be to capture, disrupt, deny, degrade, destroy, or manipulate computing and information resources in order to achieve a position of advantage over other competitors (Applegate, 2012). According to Parks and Duggan, from their Principles of Cyber Warfare, "Maneuvering in cyberspace involved the application of force to specify points of attack or defense" (Duggan, 2011). Furthermore, according to Scott Applegate (2012), the idea of cyber maneuvering as an element of warfare has come along far enough for us to identify defining characteristics. Though research is being conducted into types of cyber warfare maneuvering, the extent of which these maneuvers are employed, which might define a clear act of cyber warfare, has not yet been internationally established (Mali, 2018). Willson & Tomhave define a weapon of cyber warfare as an information technology system purpose built to damage the infrastructure or operations of another IT system (2012). This angle does not take into account the possibility of a cyber warfare weapon being used to alter or direct the behavior of an adversary to a desired point or conclusion.

6. The Discovered Link between Attack and Defense Costs

From the literature, we can see that there is a clear link between conventional warfare and cyber warfare. In some circumstances, we even see the integration of cyber war alongside conventional tactics, or as a prelude, in order to soften an adversary prior to a significant strike. Policy makers and executive leaders, although recognizing the value and risk of attritional warfare, have already begun to move away from this and consider different approaches (Defibaugh,2021). Peter Munson (2007) wrote that strategic policy makers and leaders must be able to more accurately assess the available resources and thus set strategies that are appropriate to limited power, without overreaching. From the literature, we can see that there is a clear link between conventional warfare and cyber warfare. In some circumstances, we even see the integration of cyber war alongside conventional tactics, or as a prelude, in order to soften an adversary prior to a significant strike. As far as defining cyber capabilities as weapons, it is often equated that the term weapon implies an offensive connotation, whereas some weapons may actually be a passive force that is used to degrade or eliminate an adversary's will to resist (Mali, 2018). The Tallinn Manual defines a weapon of cyber warfare as something that is capable of causing injury, damage, death, or destruction (Schmitt,2013). However, this representation does not take into account passive weapon systems designed to degrade or interfere with an adversary (Mali, 2018). Though Mali does further define weapons of cyber warfare, he does not apply them to a stratagem. Applegate takes this further by establishing that not only are maneuvers still relevant but, using the Internet as a force multiplier, they are effective and potentially devastating if misinterpreted. However, at present, we lack framing mechanism to understand what tactics and maneuvers are available in order to employ a strategy of cyber attrition against an adversary.

From this, we are not only able to define cyber war as the ability to steal, degrade, interrupt, or otherwise interfere with an adversary's information systems, but also the maneuvering of force in the cyber realm in order to gain a significant advantage. We are also able to better understand the idea of specific maneuvers that would enable these activities and interpret them, not as individual events, but on the greater sum of their activities towards an end game (Defibaugh, 2021). Unlike the definition of cyber warfare and cyber weapons put forth by Rid & McBurney, the cyber attacks themselves may not be effective, but have the ultimate goal of changing an adversary's thought process entirely and thus manipulating their behavior favorably towards the adversary's goals (2012). We also see that not only is it possible to interfere with an adversary and manipulate their decision-making process, but that it has even been executed in several public and well documented international events. Having previously established attritional warfare as a relevant strategy in the modern era, it is a viable strategy in an era of asymmetric conflicts using the Internet as a tremendous force multiplier. We begin to see possible exploitation, positional, and influencing maneuvers that are readily available to attack our more classic mentality and effectively wear us down through resources or will attrition, until we ultimately lose the collective ability to continue resisting. According to the Internet Security Alliance Board of Directors, "An estimated $1 trillion was lost in the US in 2008 through cyber attacks" (Williams, 2009). Even the response required merely to figure out who perpetrated a cyber attack requires expensive resources and talent in the form of specialized teams with specific knowledge and experience. With the sharp increase in frequency of cyber attacks, we also see a proportional increase in spending (Jensen, 2009, 2010). The concern that is becoming evident is that US-based organizations, with their policies of strict compliance, are reacting in proportion to each individual cyber event or incident and bringing the full scope of resources to bear. This is a problem when you start to pull back and look at the larger picture of sustainment in the cyber realm. To secure complex systems, it takes thousands or tens of thousands of trained personnel and billions of dollars involved in monitoring, maintaining, and defensing

complex systems of systems (Lynn, 2010). Members of the United Stated Senate have even stated that the federal government has spent more on cyber security for federal agencies than it has on the gross domestic product (GDP) of North Korea (US Congress Senate Committee on Homeland Security and Governmental Affairs. Subcommittee on Federal Financial Management Government Information Federal Services and International Security, 2010). This is very troubling because if we look at historic examples from William Philpott (2015) and the First World War I, we see that economies of adversary nations were clear and definite targets for attrition style warfare. It can be noted in several cases where the cost of maintaining armed forces, infrastructure, or the inability to adequately respond prevented the defending side from responding in any meaningful. In several historical circumstances, to include Vimy Ridge, it was evident that nations were able to maneuver themselves in ways to exploit their adversary's circumstances to ultimately cripple them and erode their will to resist until they ultimately surrendered. From the perspective of an adversary who is able to cheaply and effectively use the Internet as a force multiplier, it is advantageous for them to allow the US and NATO to continue chasing every single incident without any regard to potential maneuvering or orchestration by an adversary seeking to execute cyber maneuvers in support of a larger intentional campaign (Defibaugh,2021). An adversary seeking to gain an advantage through an influencing maneuvering may be attempting to support an attrition campaign designed for friendly organizations to expend precious resources chasing shadows and threats that were never truly intended to have an impact on their own. Only by looking at the aggregate maneuvers do we start to really see the potential jeopardy that a reactionary posture seeking to blindly enforce compliance, provides.

7. Researching Attrition Theory for Cyber Warfare

In order to examine the modern topic of attrition theory in the context of cyber warfare, the general concept of attrition warfare had to be established as a grounded and accepted fact. In order to achieve this, attrition through history was reviewed using a methodical gathering and analysis of data. The concept of attrition as a strategy and tactic in conventional warfare is well grounded in the historical literature. Using both online and print sources, major wars and conflicts can be found utilizing keywords searches. The grounded theory research supports the research questions by underpinning circumstances where wearing an adversary down through indirect combat, economical, or social means was a more advantageous avenue than outright head-on conflict. Having confirmed that attrition is a viable attack strategy, a comparison of cyber warfare strategies can be undertaken to show distinct circumstances where attritional warfare would have a potential impact utilizing the combat domain of cyber. In order to examine the modern topic of attrition as a strategy in cyber warfare, the general concept of attrition warfare had to be established as a grounded and accepted fact. In order to achieve this, attrition through history was reviewed using a methodical gathering and analysis of data. The concept of attrition as a strategy and tactic in conventional warfare is well grounded in the historical literature. Using both online and print sources, major wars and conflicts can be found utilizing keywords searches. The grounded theory research supports the research questions by underpinning circumstances where wearing an adversary down through indirect combat, economical, or social means was a more advantageous avenue than outright head-on conflict. Having confirmed that attrition is a viable attack strategy, a comparison of cyber warfare strategies can be undertaken to show distinct circumstances where attritional warfare would have a potential impact utilizing the combat domain of cyber.

The interview protocol was developed to support the research method for gathering data to determine if economic factors could potentially be used to engage an organization in attrition warfare. The first component was the number of individuals interviewed in order to gather significant data. Based on expert recommendations from researchers and experts in the same field, the number of interviews was a minimum of seven individuals. The individual interviewees all belonged to the same parent organization, but also belonged to different sub-organizations. In each circumstance, the interviewee was not a direct subordinate, nor were they supervised by the research team. The interview subjects were each of the same pay grades and had the same minimum qualifications as established by the organization. For this study, since all of the subject matter experts were required to have the same qualifications to hold their position and grade, the interviewees' race, gender, and other influencing factors were deemed irrelevant to this area of research.

The interview protocol that was utilized was designed to limit confirmation bias and sample bias. In order to support this, the subject matter expert had to be within a certain organizational grade level and have equivalent cyber security roles and responsibilities. As shown in previous research, cyber security is a relatively new field in comparison with others and, therefore, is still exploratory (Defibaugh, 2021). The interview method was built upon the interview protocol to support the primary research topics, specifically the question of whether financial

and thematic data could demonstrate a relationship to cyber war by visualizing attrition activities against an organization. The first step in the interview method was to develop the questions that would permit a semi-structured format with open-ended questions that would elicit unbiased, clear answers. The desired amount of questions for an hour-long interview was about 11 to 15 questions. (Defibaugh, 2021)

8. Struggling to See Beyond Compliance

According to qualitative interviews conducted at a U.S. based organization, two common themes were brought to light from the data aggregated from the following examples (Defibaugh 2021):

1. Some organizations in this study were not prepared for cyber war.
2. The focus of cyber security is entirely myopically centered on a compliance-based mentality, according to a majority of participants in this study.

According to research performed by Defibaugh, it was established that US-based organizations, using a strict-policy of compliance, are reacting proportionally to individual cyber events and incidents (2021). This becomes a significant problem when the defenders have the perception of having to be right in every encounter with the adversary, whereas they only have to be right once. As the topic of compliance furthered, some participants expressed concern of compliance as the seemingly only benchmark for cyber warfare readiness. One of the interviewees from Defibaugh's study (2021) offered that,

> *As a matter of fact, some of the programs that are being put in place actually decreased performance within our activity. And so then we asked specific questions about, hey, if we have to perform our mission based on the restrictive or based on the configuration that you put in front of us, how do we perform that mission? And the answer is, 'Well, you have to work around that.' So then, we ask when we get interviewed by the people who are chartered to go put this protective measure in place at the top level domain, and we start telling the things we do, it doesn't appear to me that they understand our mission or the technologies we're using* (p. 77).

This is an interesting perspective in that it does not simply mean to be done with compliance audits, moreover, that the total sum effect to include larger impact on strategy must be accounted for. The participant wondered, in the same vein as attrition warfare, if cyber security professionals could audit themselves into submission (Defibaugh, 2021):

> *I think primarily most of our organizations are still focused on compliance. I think they're more concerned with just making sure that they're compliant, that they're meeting the requirement, and they stop at that point. And I think the perspective has to change to where we look at that. That compliance that we're looking at is the baseline, not the end goal. The end goal is to take it beyond that and start looking at how you can actively start making changes that aren't part of that requirement. It's training and perspective, the perspective from management in general has to change to where we're not just looking to be compliant. Compliance is a part of the picture, but it's not the goal. And I think the second part is that the only way people are going to truly start to understand when they see something anomalous and understand and recognize it as a problem, is if they run tests in their own environment (p. 78).*

Another participant felt very strongly that compliance activities had become overblown and,

> *So, what happens when you get compliance-based compliance, then it is validated with an audit and audit comes in? They make sure that all of those compliance pieces are in place. So what happens is you basically shift all of your focus from providing your day-to-day production support to making sure that you're compliant, and somewhere in the middle of that it gets lost. The fact that the really important thing is that you're monitoring the traffic levels and what's happening on your network, so that if you are attacked, you can recognize it (p. 78).*

This is an interesting perspective in that it does not simply mean to be done with compliance audits, moreover, that the total sum effect to include larger impact on strategy must be accounted for. Qualitative research provides contextual information that does not always have readily available quantitative measures with which to perform a completely rounded analysis.

Table 1: Data Collection Categorization developed from (Defibaugh, 2021)

Data Value	Data Type	Expected Value Collected
Typical Number of Events Experienced in 12 months?	Interval	No
Average amount of funding expended per month on Incident Response for 12 months?	Interval	No
Percentage of incidents determined to be false positive across 12 months?	Interval	No
Are organizations focused on spending resources appropriately on cyber attack?	Nominal	Yes
Does a compliance driven mentality weaken an ability to respond to cyber threats?	Nominal	Yes

As seen in Table 1, common themes extracted from the nominal interview data can be used to demonstrate the gap in quantitative data when the metadata is compared (Defibaugh, 2021). Each of the interviewees were able to provide nominal data based on earned experience and tacit knowledge. However, there was a significant lack of available interval data to perform a meaningful quantitative validation on the contextual knowledge that was collected.

9. Conclusions and Future Areas of Research

One of the overarching themes that was identified in the research conducted by Stephen Defibaugh was that in many cases, the blind pursuit of compliance takes away from the focus on things which may truly be more critical. In circumstances where the behaviors of a target are known, then the compliance based approach begins to show weaknesses as an overall strategy. Compliance sets the bare minimum standard and baselines systems in order to provide a basic profile to system security. Yet, when adversaries understand that stimuli can be created to manipulate behaviors and decisions, then we start to see where compulsive behavior and reactions can become very dangerous. Further topics of research would center on further exploration of qualitative themes gathered from cyber security experts that have a unique view of both policy, operational execution, and resource expenditure. The qualitative, exploratory research that was conducted by Defibaugh demonstrates the need for further quantitative and mix-methods studies that examine the possibility of utilizing attritional styles of attack as a strategy for conducting cyber warfare. Understanding the amount that is spend on compliance as well as incident response must be balanced against strategic perspectives and pragmatic worldviews. It is imperative that the cyber security field understand the cost-value impact of its currently adopted methodologies and industry practices by developing the proper metrics and telemetry that can identify patterns at a strategic level.

References

Applegate, S. D. (2012, June). The principle of maneuver in cyber operations. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, (pp. 1-13). Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6243974&isnumber=6243954

Boyd, J. R. (1986). Patterns of Conflict. Project on Government Oversight, Defense, and National Interest - John Boyd Compendium. J. R., 1986. Retrieved from http://dnipogo.org john-r-boyd

Butler, S.C (2013). Refocusing on Cyber Warfare Thought. *Air & Space Power Journal,* 27(1 (Jan/Feb)), 44-57. Retrieved from http://proxymu.wrlc.org/login?url=https://search-proquest-com.proxymu.wrlc.org/docview/1318929576?acountid=27975

Defibaugh, S. J. (2021). *Attrition as a Practical Attack Methodology and Tactic for Cyber Warfare* (Doctoral dissertation, Marymount University).

Harris, M. A. (2018). Preparing for Multidomain Warfare: Lessons from Space/Cyber Operations. *Air & Space Power Journal, 32*(3), 45. Retrieved from http://proxymu.wrlc.org/login?url=https://search-proquest-com.proxymu.wrlc.org/docview/2099884315?accountid=27975

Lloyd George, D. L. (2017). *War Memoirs of David Lloyd George*. Vol. 1 Pickle Partners Publishing.

Mali, P. (2019). Defining Cyber Weapon in Context of Technology and Law. In Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications (pp. 1119-1132). IGI Global.

Munson, P. (2007). *The Return to Attrition: Warfare in the Late Nation-State Era.* NAVAL POSTGRADUATE SCHOOL MONTEREY CA CENTER FOR CONTEMPORARY CONFLICT..

Parks, R. C., & Duggan, D. P. (2011). Joint Publication 3-0 Joint Chiefs of Staff, United States Department of Defense, Washington, D. C., **2011,** pp. 111-27.

Parks, R. C., & Duggan, D. P. (2011). Principles of Cyber Warfare. *IEEE Security & Privacy, 9*(5), 30-35.

Philpott, W. J. (2015). *War of Attrition: Fighting the First World War.* Abrams.

Prete, R. A. (1997). The Franco-British strategic conflict on the Western Front and the Calais conference of July 6, 1915. *World wars and contemporary conflicts*, 17-49.

Rid,T.,&McBurney,P.(2012).Cyber-Weapons.The RUSI Journal,157(1),6–13.doi:10.1080/03 071847.2012.664354

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. CambridgeUniversityPress.doi: 10.1017/CBO9781139169288

Us Congress Senate Committee on Homeland Security and Governmental Affairs. Subcommittee on Federal Financial Management Government Information Federal Services and International Security. (2010). *More Security, Less Waste: What Makes Sense for our Federal Cyber Defense*: *Hearing Before the Federal Financial Management, Government Information, Federal Services, and International Security Subcommittee of the Committee on Homeland Security and Governmental Affairs, United States Senate of the One Hundred Eleventh Congress*, *First Session, October 29, 2009*. US Printing Office.

Williams, M. (2009). Cyberspace May Be Locale of Next War. Federal Times (Dec. 7, 2009).

Willson,D.,&Tomhave,B.(2012).Legal&EthicalConsiderationsofOffensiveCyber-Operations. RSA Conference 2012. Retrieved from https://www.rsaconference.com/writable/presentations/file_upload/star-304.pdf