THE CYBERTHEORY INSTITUTE PRESENTS

USING MANEUVER WARFARE TO CONDUCT ZERO TRUST CYBER WARFARE

CYBER THEORY INSTITUTE

INTRODUCTION

IT'S TIME TO IMPLEMENT MANEUVER WARFARE INTO YOUR APPROACH TO CYBERSECURITY

The means of warfighting – development of weapons that do not involve or require conventional war – has an infinite array of options. Thus, choosing a means of warfare that is limited to the use of arms and military power has become a lower priority.

The method of Military Operations Other Than War (MOOTW) is a means and method growing in use. It enables human beings to use every conceivable means to achieve their goals. "The civilization of war will be an important characteristic of 21st century war."[i]

The successful conduct of a cyberwar campaign requires a leader skilled in the art of maneuver warfare. Maneuver warfare involves the foundational principles on which you can build a strategy to defeat your opponent. This concept enables leaders to deploy information, security controls, physical assets, and people in a manner that provides the best opportunity to break the adversary's will and cause him to cease the attack.

Cybercrime is the greatest economic threat confronting every organization in the world. Fighting an economic war requires a military hue. A defeat on the economic front precipitates a near collapse of the social and political order. The casualties of such a collapse exceed the injury inflicted by a regional war. To date, there has been a reluctance to accept the reality that a war is being fought whose loss could have such ramifications. That reluctance provides a strategic advantage to the cybercriminal as it results, most often, in the target failing to prepare for and respond accordingly to an attack. Cyberwarfare is not for the meek.

[i] Colonel Shoichi Takama, "What the Revolution in Military Affairs is Bringing – The Form War Will Take in 2020"

"The essential thing is action. Action has three stages: the decision born of thought, the order or preparation for execution, and the execution itself. All three stages are governed by the will. The will is rooted in character, and for the man of action character is of more critical importance than intellect. Intellect without will is worthless, will without intellect is dangerous."[ii]

Much like conventional warfare, cybersecurity warfare is a resource-based conflict affected by human and environmental factors. As is often the case in conventional war, the ability to maneuver is critical to positioning resources in a manner that provides the attacked organization with the best opportunity for victory.

In all forms of conflict, the continuous process of move/countermove between the opponents continues until the will to continue, by one of the opponents, is broken. In order to break your opponent's will, the cybersecurity team must be guided by a warrior mindset based on mental toughness and founded on deliberate practice. In the context of cybersecurity, the pressure to make sound and timely decisions increases regularly.

Successful cybersecurity breaches are often attributed to human error or negligence. However, environmental factors such as changing regulations and laws, increased digitization of data and interoperability requirements, the expanding internet of things, and the expanding attack surface, due to remote workers, offer the adversary a growing number of tactics, techniques, and processes to exploit vulnerabilities in an organization's cyber defense posture.

The operational environment of organizations with respect to information security consists of:

- Blurred battle lines among those with varying levels of responsibilities,
- An increased flow of information within the unique operational environment of each organization and business partners,
- Susceptibility to multinational coalition warfare which is becoming a common threat and promises to continue to increase as the requirements for interoperability increase,
- Identities of amorphous enemies which are becoming increasingly difficult to distinguish, and
- Heightened liability due to collateral damage.

[ii] Hans von Seekt, Thoughts of a Soldier, trans G. Waterhouse (London: Ernest Benn Ltd., 1930) p.123
[iii] US Marine Corps "Warfighting" p 7, MCDP Copyright 1989

The ability of security leaders to assess the complex risk environment as it threatens their security position; to make effective decisions on necessary changes, frequently in real time; to communicate their decisions to executive management and the distributed operational environment; and to formulate tactically superior plans in support of the strategy to implement these decisions will determine a successful defense outcome or failure resulting in a breach and subsequent loss in revenue, costs associated with remediation, and diminished brand reputation.

The four human and environmental factors that shape a conflict, and which must be considered if the organization is to successfully defend against an attack on the critical digital assets they are tasked with protecting, are:

DISORDER

In an environment of Friction, Uncertainty and Fluidity, it is common for mistakes to occur as a result of plans going awry, communications failing, or instructions and information that is unclear or misinterpreted. Consequently, the situation will deteriorate, as time progresses, toward Disorder. As the situation continuously changes, the ability of the leader to improvise in an ever-changing environment is critical for success. Disorder is an integral characteristic of any type of conflict and is a perfect description of what can occur for an organization responding to a successful infiltration by a threat actor. In such a state of Disorder, it is human nature for people to behave according to habits they have developed as a product of training and preparation.

FLUIDITY

Fluidity describes the environment (i.e., battlefield situation) in which each event "merges with those that precede and follow it – shaped by the former and shaping the conditions of the latter – creating a continuous, fluctuating fabric of activity replete with fleeting opportunities and unforeseen events"[iv]. It is this factor that drives the requirement for "Continuous Oversight"[v] by the information security team. Continuous Oversight enables an organization to quickly adapt to changing threat conditions and actively seek to shape emerging events in the breach attack. Fluidity will be a factor in how a defender works to prepare for a potential threat or respond to an actual attack. As adversaries are using more attack vectors that are malware-free or zero-day attacks that target a blind spot identified by preceding effort, each individual organization will have challenges regarding Fluidity because of the unique operating environment of its business.

[iii] US Marine Corps "Warfighting" p 7, MCDP Copyright 1989

[iv] Ibid, 9

[v] At the core of continuous oversight are people regularly reviewing the dynamic threat landscape of the organization and applying their current knowledge with that threat intelligence to measure the effectiveness, relative to security (i.e., security assessments) against policies and procedures, physical safeguards, network and server security, and application security

FRICTION

This is what makes the simple difficult and the difficult seem impossible. Friction in conventional warfare can be both mental and physical. The most obvious physical source of Friction is the adversary, but in cyberwarfare, the independent nature of employees, business functions, and business partners, frequently governed by an immature cyber model within the enterprise culture, can contribute to physical Friction. Indecision over a course of action, might be the dominant source of mental Friction, in addition to the lack of a clearly defined goal for the organization's enterprise security program, the lack of tactical planning in support of the cyber defense strategy, or the lack of operational coordination due to unclear or overly complicated plans.

UNCERTAINTY

This is the atmosphere in which "all actions in war take place and is often called the Fog of War"[iii]. The most common cause of Uncertainty is the lack of knowledge regarding the adversary's intentions and capabilities. While knowledge of the adversary's intentions and capabilities continues to improve, it remains a primary source of Uncertainty. What doesn't appear to be improving as rapidly as necessary is the lack of understanding of threats by executive management, the strategy and tactics necessary to mitigate the risk of compromise of critical data and the resulting liability, and the negative impact regarding the tempo of decision making required in a cyber conflict.

A successful information security leader must have a strategy for developing the flexibility to use these four factors to his or her advantage and maneuver a response that limits the potential negative impact of these factors, while creating a situation in which the adversary's will to continue is broken.

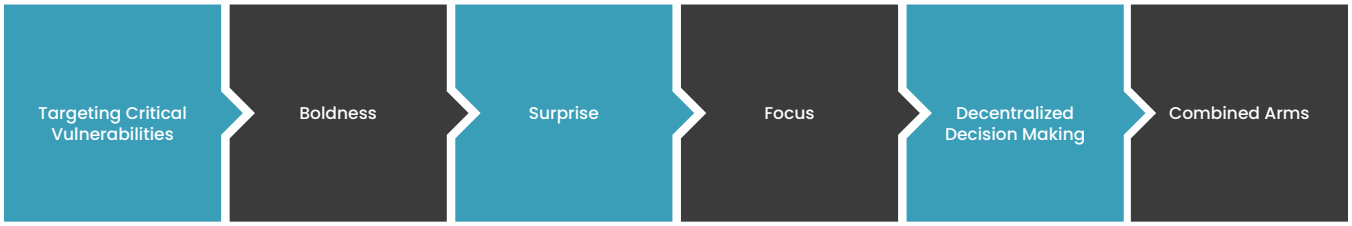
Strategy teaches that the most meaningful success is taking resources away from opponents. With respect to cybersecurity, a vital resource to take from the criminal adversary is available attack surfaces. This logic should be a primary motivation for implementing the Zero Trust strategy of protected surfaces. Zero Trust reduces the attack surface and limits the blast radius—that is, the impact and severity—of a cyberattack, which reduces the time and cost of responding to and cleaning up after a data breach.

The goal of such a strategy is the creation of a cybersecurity posture that enables the collection of people, process, and technology to proactively act in concert in the effort to protect an enterprise's crucial assets. It also enables a team to continually train and prepare to respond to current and new threats and maintain the mental toughness to resist the tendency to become complacent while performing the mundane tasks associated with good cyber hygiene.

But, a strategy is only as good as the principles and tactics used to support it. The Doctrine of Maneuver Warfare provides seven principles to successfully execute the strategy to achieve a mature cyber model for planning, preparation, and training.

THE PRINCIPLES OF THE DOCTRINE OF MANEUVER WARFARE

The purpose of this eBook is to develop a greater understanding of how these principles could be used in the execution of a strategy for building a more active cybersecurity plan. We will begin by discussing each principle of the doctrine, provide insight regarding the Zero Trust strategy model, and present thoughts regarding how the doctrine's principles serve as tactics in this strategy.



1. Targeting Critical Vulnerabilities

In conventional warfare, the primary focus is on targeting the critical vulnerabilities which, "If exploited will do the most significant damage to the competitor's ability to resist."

In cybersecurity warfare, the vulnerabilities of the adversary as well as the attack method being used can be addressed through threat intelligence. The more significant vulnerabilities to address are those within the unique operational environment of the individual organization. Such an effort requires forward looking planning and rigorous self-examination.

Rigorous self-examination requires more than an annual vulnerability scan or penetration test which is too often the norm just to meet compliance requirements. The traditional layered (defense-in-depth) security model, employed by most security teams, has a number of gaps between controls that create blind spots.

As many recent breaches have demonstrated, cybercriminals have altered their tactics to exploit vulnerabilities within applications, devices and widely implemented security controls. Many organizations deploy new technologies absent an understanding of the vulnerabilities being introduced and, therefore, fail to implement appropriate levels of data security.

The speed at which an adversary can act to exploit a vulnerability is dependent upon how quickly an organization identifies and removes it. Minimizing the lag time between identification of a critical weakness and implementation of appropriate security controls maximizes the effectiveness of the resources deployed.

For an organization to identify such a vulnerability and make a decision on the appropriate action to take regarding

[vi] Harell, Yehuda, Follow Me: The Story of Moshe Dayan

its removal is a function of the level of situational awareness within the organization's security team and senior leadership. Such situational awareness is built on its effort to observe the threat activity within its respective industry and orient its defenses to defend against such an attack.

Testing various possible threat scenarios will significantly improve the current level of situational awareness and, more importantly, create new mental models within the security mindset of decision-makers. The new perspective created by this more informed mindset can bring about an increased willingness to be innovative in security strategies and tactics employed to counter the cybercriminal's tactics, techniques and processes as they continuously evolve.

SCENARIO PLANNING

Scenario planning starts by examining a set of strategic uncertainties, and then ranking them in terms of the level of likelihood and severity. The Enterprise Risk Analysis in concert with the most current threat intelligence could be used to determine values such as liability associated with the scenario should an actual attack occur. High and medium risk-ranked scenarios should be explored with respect to the impact on the operational environment, followed by the development of a response plan. The response plan should be practiced and documented for each scenario.

In planning testing scenarios, too many organizations are motivated by meeting compliance requirements rather than improving performance in their ability to respond to attacks targeting vulnerabilities. The result, in many instances, is that the organization and the security team remain in their Comfort Zone. Practicing in this zone does nothing to improve performance. While it may seem harsh, experiencing failure when risk is not a concern can be a learning tool leading to the development of confidence that will serve the individual and the team well in the chaos of an actual attack.

Remaining in your Comfort Zone can create a false confidence regarding your ability to perform and, more importantly, never positions the individual or team in the Learning Zone where all security teams should regularly operate.

By continually operating in the Comfort Zone, an attack thrusts the organization into the Panic Zone causing them to learn on the fly as they attempt to stop the breach. Having to "practice" in the Panic Zone most often

leaves the organization paralyzed because the activities required for a successful response are too difficult and the team frequently doesn't know where to start. "A confused army leads to another's victory."[vii] The Panic Zone is a place where, for the most part, the organization's focus is lost and the response behavior can best be described as frantic.

Both the Comfort Zone and the Panic Zone can be mistaken for the Learning Zone which is the zone an organization should be in at all times. The only way to make progress is to operate in the Learning Zone. This is where the skills and abilities that are just out of reach reside. They are neither so far that we panic nor close enough where they're too easy.

Scenario planning is to be conducted in the Learning Zone and should be done based on the concept of Deliberate Practice with the goal of improved performance. To best serve the purpose of improved performance, the scenario should be designed to identify the organization's "Achilles's heel" and structured such that failure, in achieving the desired performance, is experienced 20% - 50% of the time the exercise is conducted. Effective scenarios that test the response to critical vulnerabilities require significant human involvement in their design if the desired "failure" learning objective is to be achieved.

In order to overcome the emotion of fear when threatened, a person must, through training, come to understand that failure is nothing to fear. Instead, they must develop the mindset that "success is not final, failure is not fatal: it is the courage to continue that counts."

[vii] Sun Tzu, The Art of War

Deliberate Practice requires the person to be operating in the Learning Zone and regularly reusing knowledge and the use of current skills while receiving feedback.

Desired behavior is a learned skill. Training, testing and review of results sharpens this skill, builds confidence in its use, and competence in the execution of the behavior. The frequency of conducting deliberate practice scenarios must be greater than the compliance driven quarterly, semi-annual, annual frequency that is so common. As the Latin saying goes, "Repetitio est mater studiorum" (Repetition is the mother of learning).

In order to maximize the improvement in performance, the repetition should occur in different scenarios presenting different conditions and situations but require the use of current knowledge and skills.

The three zones are constantly changing; as a result, remaining in the Learning Zone is a hard task that must be continuously monitored. Tasks that were once in the Panic Zone will move into the Learning Zone and the cycle will continue.

Be aware that projects beyond your current Learning Zone can put you in the Panic Zone. In such a situation, step back into the Learning Zone; research, read, and talk to an expert. Eventually, this behavior leads to taking on new skills that become habits of behavior, enabling transitioning from the Panic Zone to the Learning Zone and, after Deliberate Practice, into the Comfort Zone.

SCENARIO ANALYSIS

Scenario analysis uses intuition, experience, introspection, and current threat intelligence to limit the range of things that might happen in the rapidly changing and disorderly reality of a cyberattack.

A characteristic of the able commander (leader) is that he/she is active rather than reactive. She/he takes the offense and controls the situation. This is true even when a defensive action is taken. It is an offensive action to consistently seek an improved defensive posture and be able to more efficiently and effectively execute the plan to achieve that posture.

A Top-down, Bottom-up approach to targeting vulnerabilities in the organization should be adopted.

- Top-down
  - Think like the adversary;
  - Never lose sight of your ultimate objective (i.e., Enterprise Security Vision);
  - Make extreme demands on resources at the right time for the right reason.
- Bottom-up
  - Rely on subordinates;
  - Reinforce and reward ingenuity, action, and willingness to take a chance;
  - Encourage team members to speak up during the formation of the Action Plan, scenarios, and potential courses of action.

> "If everybody is thinking alike, then somebody isn't thinking."
>
> General George S. Patton

Discretion in decision making is always important. Having the conviction to take the advice of team members and make a decision based on that advice requires the conviction to stand behind that decision in the face of considerable resistance. Test the decision by encouraging team members to disagree and present alternatives that have the potential for a better outcome.

Reinforcement and training in speaking up can be accomplished by devising creative ways to put people in controlled situations of uncertainty, forcing them to make decisions. A perfect opportunity for this exists when performing "Table Top" exercises, testing the organization's Incident Response Plan, as recommended by the National Institute of Standards and Technology and included in OCR Guidance.[viii]

[viii] NIST: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act

SCENARIO EXECUTION

In order to recognize the greatest value from this principle, the security leader must first step outside the organization and examine every aspect of the people, processes, and technology of the business from the perspective of the potential adversary. "To know the enemy, you must become the enemy"[ix] . This exercise will aid in the discovery of what the adversary may be doing to identify how they can significantly damage the organization.

Communications systems must be flexible and reliable to meet the task at hand. Disaster recovery and backup plans must be documented, practiced, and continuously improved.

- Use all available threat intelligence to rehearse the cybersecurity plan and refine the plan in light of potential outcomes that were not anticipated prior to rehearsals and
- Live and operate by the philosophy of: "A good plan, violently executed now, is better than a perfect plan next week."[x]

Finally, acknowledge the reality that the adversary is performing a similar reconnaissance of the organizations critical vulnerabilities.

With this understanding, the leader should be visible to the organization. Lead from the front and get information from firsthand observations. Quiz the staff on their responsibilities. Actively seek opinions on decisions from people in the business units regarding their ability to maintain productivity during recovery.

[ix] Sun Tzu, The Art of War
[x] General George S Patton

2. Boldness

This principle requires the use of a risk/reward trade-off framework to increase the organization's inclination to make bold decisions, train people to evaluate choices and make decisions, and act in the absence of complete information. In tandem with the calculated risk/reward trade-off of the bold action, there must be a plan for exploiting the opportunity created should the action be successful.

Boldness requires the daring to commit resources to endeavors with uncertain to highly uncertain outcomes entailing considerable risk. Boldness requires:

- Conviction to stand behind a decision in the face of considerable resistance,
- Identification of a breakthrough opportunity and acting decisively to take advantage, and
- Exhaustive planning to mitigate calculated risks associated with the opportunity to create a more favorable risk/reward profile.

While Boldness is most often associated with taking action, it also includes inaction, abstaining from an uncertain and potentially undesirable situation, keeping in mind that being aggressive may prove to be an unsafe strategy as well. Therein lies the paradox. It is imperative that the leader ask the question, "What is the best strategy to defeat the adversary's strategy for circumventing the controls I have employed in this situation?"

> **"Boldness requires calculated risk taking: appropriately weighing risk and reward so that reckless behavior is avoided in the pursuit of breakthrough results."**[xiii]
>
> This relationship formula will serve in calculating risk and reward
>
> (Probability of Sucess x Potential Results from Sucess) - (Probability of Failure x Potential Cost of Failure) = Expected Value of Outcome
>
> The Marine Corp Way

The 80% Rule can be applicable in situations that require Boldness in the decision-making process. This rule states that "delaying any decision so that it can be made with more than 80% of the necessary information is hesitation." In such situations, when the tempo of the situation will not permit the exhaustive, meticulous planning and information gathering to mitigate the risks associated with a bold decision, the leader must rely on intuition. The training of leaders in preparation and planning during Scenario Analyses can help develop keen and quick insight (i.e., intuition) in the face of limited information, thus enabling the exercising of initiative with confidence. Reinforcing ingenuity, action, and willingness to take a chance should be encouraged and rewarded by the security team leader.

[xiii] The Marine Corps Way; McGraw Hill Books, Copyright 2004; p. 57

The inputs require considerable thought and will most often be determined by estimates based on the team's experience. If lacking in that experience, an outside party might be commissioned to assist in determining the input estimates. It's important to weigh the risk and reward, be patient and disciplined in committing resources to a decision, and always consider the question, "What's the downside?"

A final action involves documenting the details of past successful and failed risk/reward decisions in order to accelerate development as a calculated risk taker. This action applies to both preparation and testing scenarios as well as actual attack outcomes.

Boldness will play a key role in reorienting the focus of information security from compliance, as is often the primary motivator in highly regulated industries, to a Strategic Information Security Program of which compliance is but one component.

3. Surprise

"Those who strategize, use the Tao[xiv] of paradox… and use confusion to take control."[xv] Any organization is strong only when it has a core of strongly shared values.

The ability to project to the opponent a contradictory view of your position or plan is known as tactical paradox. The purpose of Surprise in maneuver warfare is to proactively take steps to degrade the quality of information available to the adversary and create a tactical paradox. The result is the adversary is forced to make decisions that may result in exposing his presence earlier than planned. "It is not essential that we take the enemy unaware, but only that he becomes aware too late to react effectively."[xvi]

An organization is composed of both normal and extraordinary forces. The most successful maneuvering comes through the mastery of direct (normal) and indirect (extraordinary) tactics – especially the ability to achieve direct effect through indirect means. The direct force that confronts the adversary is the normal force (i.e., security controls – the Chinese term is "cheng") and the extraordinary force (the Chinese term is "chi") goes to the flanks. "Chi" is the surprise component of maneuver warfare.

There are three approaches that can be used to achieve Surprise in the Doctrine of Maneuver Warfare. They are stealth, ambiguity and deception.

Stealth denies the adversary any knowledge of an impending action. The tactic of threat hunting can be effective in covertly detecting the presence of an adversary which can then be followed by the development and deployment of a response strategy that catches them completely off guard and prohibits an effective reaction.

The normal response to the detection of an adversary's presence is to immediately shut down the affected systems. However, the better response might be the use of stealth to conceal your intentions or coordinate your efforts with members of your Incident Response team. Through this coordinated effort, your first move does not announce the timing or direction of your initial response. Through the use of stealth, the security team is better able to understand the pervasiveness of the threat without alerting the adversary ahead of your response and, consequently, restrict the adversary's ability to change the strategy of the attack.

The cybercriminal conducts reconnaissance of a target organization for the purpose of better understanding the daily operation of the target in order to better plan both the strategy and timing of their attack. **Ambiguity** is "acting in such a way that the enemy does not know what to expect." Creating ambiguity for the adversary can be accomplished by staggering activities such as vulnerability scans, penetrations tests, and threat hunting exercises in an undetectable pattern. In doing so, the adversary must address the risk of detection and alter the strategy to remain undetected.

In applying both stealth and ambiguity, Surprise is achieved and the will of the adversary is weakened if not broken.

[xiv] Tao is the Chinese word for "the Way" – It is the first of the five working fundamentals of strategy and is what inspires people to share ideals and expectations
[xv] Sun Tzu, The Art of War
[xvi] Warfighting, p 42

Deception involves misleading the enemy regarding your plan of action. At a fundamental level, all war is deception and it is through maneuver that deception is created. In a proactive cyber defense plan, the ability to maneuver and create confusion for the adversary is essential in today's evolving threat environment. The strategy is to move when it is advantageous and create changes in the situation by dispersal and concentration of forces. It must be understood that nothing is more difficult than the art of maneuver. The difficulty rests in the ability to make the devious route of response the most direct and turn misfortune to advantage.

This is probably the most difficult approach to achieving Surprise in cybersecurity warfare. It might be most applicable when responding to a successful breach that has compromised critical data.

Through the futures scenario analyses conducted according to the Boldness principle, planned actions of maneuver could be rehearsed for the purpose of deceiving the adversary and stopping the exfiltration of data.

4. Focus

Focus is the center of interest or activity. In conventional warfare, focus is the generation of superior combat power at a particular time and place. In information security, the generation of superior combat power must be achieved through a multi-disciplinary risk mitigation focus involving data scientists, human factor risk experts, risk researchers, computer scientists, and network architecture engineers who create new mental models to add to the existing latticework of mental models that form the mindset and perspective of how to mitigate the continuously evolving threat risk.

The change in mindset and perspective that results will improve the organization's ability to observe activities in their industry and make better decisions regarding orienting people, processes and technology to achieve the goal of acceptable risk tolerance.

Focus must include planning, preparation, and training in all three components of cybersecurity, people, processes, and technology, in an enterprise program to mitigate risk. Each component must receive equal priority if the enterprise risk mitigation program is to achieve maximum success. Such a Focus will better enable the organization to shift resources and manage the business risk with the implementation of measures that target the sophisticated adversaries of today and, be better prepared to counter unexpected risks (i.e., inherent risks – a vulnerability that exists within an organization before security measures are implemented). This latter ability is particularly relevant to the response aspect of a cybersecurity action plan.

The security vision of an organization is what creates unity and aligns every member of the organization. The Focus of the effort is critical to success; it requires considerable

balance and creativity if it is to be maintained. It also requires the willingness to assume certain risks presented by a situation.

Designate a primary initiative as this will ensure that Focus is a formalized process which will help reduce conflicts associated with the assignment of resources. Commit your most skilled security personnel to frontline leadership roles to directly supervise the application of resources in order to provide the best opportunity to achieve that Focus. This often requires placing people in positions outside their Comfort Zones but, will lead to more well-rounded security specialists able to adjust to the continuously changing threat environment.

As the situation changes, the security leader may shift the primary initiative in the direction that offers the greatest success but introduces new risks. This entails training the team to become comfortable with shifting quickly to meet a new situation. This training is an element of "Continuous Oversight" and must be reinforced with regular communication to the team that includes advanced (i.e., as early as possible) notice of a pending change.

In all situations, threat intelligence can provide insight to weaknesses associated with a specific attack vector. Knowledge of an opponent's weaknesses can provide the opportunity to bring strength, in the form of controls, against the attack. Integrating all available information will help to both guide the application of resources and enable a smoother change of Focus dictated by a change in the threat environment.

"Knowledge of an opponent's weakness can provide the opportunity to bring strength, in the form of controls, against the attack."

Proactive management of the risk associated with a particular Focus will improve flexibility when change is required. Communication with your team as well as the business units affected by the change in Focus will help ease the transition. Before making a change, consider the downside when weighing the risk and the level of effort needed to shift the resources back after the threat has been mitigated.

Developing a high degree of proficiency in Focus can help overcome the deficiency in technology, people, and funding that so many security teams experience.

An incident response plan will help you in dealing with cyberattacks. It is the most important component of cyber risk mitigation strategy. Threats can come in any shape and size. Thus, you can't protect your business from every cyber threat. An IRP will help you in minimizing the damage of a cyberattack. You should ensure that your employees are ready for a data breach. They should follow your incident response plan for minimizing the effect of a data breach.

The purpose of an IRP is to better observe the existing cybersecurity mindset by expanding the Focus beyond prevention to include detection of, response to, and prediction of future attacks. In general, the focus of cybersecurity is the reduction of risk associated with the loss or compromise of critical digital assets.

5. Decentralized Decision Making

"Never tell people how to do things. Tell them what to do, and they will surprise you with their ingenuity."[xvii]

A good security posture is both centralized and decentralized. Centralized with respect to intent and decentralized with respect to decision making that leads to speed and tempo while done in compliance with strategic intent.

Every individual has the need to feel competent in what they do. There is no better way to satisfy that need than to demonstrate confidence in their decision-making capability by giving them the authority to make decisions in critical situations.

In any dynamic and rapidly changing environment such as a cyber event, success is often the result of an immediate action. Decentralized Decision Making relies heavily on an understanding of the security leader's intent and enables those closest to the action to take advantage of on-the-spot information, not immediately available to their superiors, and allows them to exercise initiative. The individual who can make and implement decisions consistently faster gains a tremendous, and often decisive, advantage.

Anyone who operates in a complex and potentially hostile environment must make tough decisions under severe duress, usually with little time and information (the classical definition of a cyberattack). Few people are ever taught how to make a decision. Decision making is either something you are assumed to have learned throughout life or are taught as a lengthy deliberate process. Teaching decision making, at all levels of the organization, regarding the proper behavior, is key to having a mature and high performing cyber hygiene model. Neil Patel, marketing expert and entrepreneur, is quoted in Forbes Magazine as saying, "Emotion influences the entire cognitive milieu of the decision-making process."

In the case of cybersecurity action plans, the confidence necessary to reinforce this principle is built during the regular Table Top exercises, testing the Incident Response Plan and the "Continuous Oversight" of the daily execution of the plan. By delegating the authority to make these decisions and tailoring communications with the aim of arming the frontline personnel with the "bigger picture" into which their actions fit, they will vigilantly supervise the directives of the Action Plan.

Distributed authority is, by nature, chaotic and has the potential to add increased chaos to the dynamic and uncertain situation that surrounds a cybersecurity attack. This chaos can result in a higher prevalence of mistakes, especially when an overzealous subordinate fails to act in concert with the security leader's intent. When executing on this principle, the risk/reward trade-off must be accounted for in the Action Plan. The situations in which such a decision, by an individual, disproportionately determines the outcome of a large-scale competitive encounter also carries considerable risks.

There are three variables that require attention to detail if this principle is to be used successfully.

[xvii] General George S Patton

1. "Confidence probability"[xviii] and open communications must include a clear understanding of the security leader's intent. Confidence in decision making ability is earned through the daily supervision and presence of the leader. As a result, communication channels and processes are developed that enable the free flow of communication during the period of stress. The leader is then able to ensure his intent is being achieved without suppressing the individual's initiative.
2. The degree to which the subordinate has authority to make decisions will vary by individual. In best case scenarios, the subordinate has been delegated the full authority to respond in a manner that results in sufficient speed to allow the organization to avoid missing opportunities. By not having to request permission and wait for orders from higher authority, opportunities will be seized and the level of potential compromise minimized.
3. The security leader's intent, while originating from the top, is actually a mutual agreement. The agreement includes the leader's vision integrated with the actions of the subordinates. Both pieces must be honored by each party and the subordinate must not fear the leader's wrath if he must seek help to avoid a potential disaster.

By addressing these variables, "Decision making thus becomes a time-competitive process, and timeliness of decisions becomes essential to generating tempo."[xix] These frontline decisions can mean the difference between experiencing a breach requiring the organization to make public notification of the compromise of critical assets or stopping the infiltration before such action is required.

[xvii] The standard use of the term "confidence" refers to a probability in a particular situation. In this situation confidence should be defined as the probability that a decision or a proposition, overt or covert, is correct given the evidence and complies with the security leader's intent in the situation; a critical quantity in complex sequential decisions

[xix] Warfighting, p 89

6. Tempo

Tempo is relative speed in time. Always maintaining the offense requires precision. Strategic advantage must be channeled and the timing of execution must be precise. War is a series of battles, moves and countermoves, such that the supreme consideration is speed in which the Tempo of execution is important. The competitor who is able to respond faster than the opponent can identify opportunities and make decisions that force the opponent into a constant state of reaction. The constant state of reaction results in breaking the opponent's will to continue the attack and causes a move to another target.

Currently, the threat actor's Tempo continues to increase at a pace that exceeds that of the typical organization. The rapid increase in malware variants designed to exploit vulnerabilities of existing infrastructure, new technology and persistent human error or negligence are outpacing the industry's ability to respond. In addition, the typical organization has other priorities that interrupt or delay Tempo, including prioritization of compliance over security. Consequently, the typical organization is not matching the Tempo of the threat actor, much less operating at one that exceeds the adversary and causes them to respond to the security team's techniques, tactics, and processes.

The rapid increase in malware variants designed to exploit vulnerabilities of existing infrstructure, new technology, and persistent human error or negligence are outpacing the industry's ability to respond.

Air force Colonel John Boyd first introduced the mental process of Tempo in his lecture, "The Patterns of Conflict." He identified the four-step mental process of: observation, orientation, decision, and action.
He theorized that each party to a conflict first observes the situation.

- On the basis of the observation, he/she orients, that is, makes an estimate of the situation.
- On the basis of the orientation, he/she assesses possible actions to better position the organization, i.e., makes a decision, and implements the decision – takes action accordingly.
- Because the action created a new situation, the process begins anew.

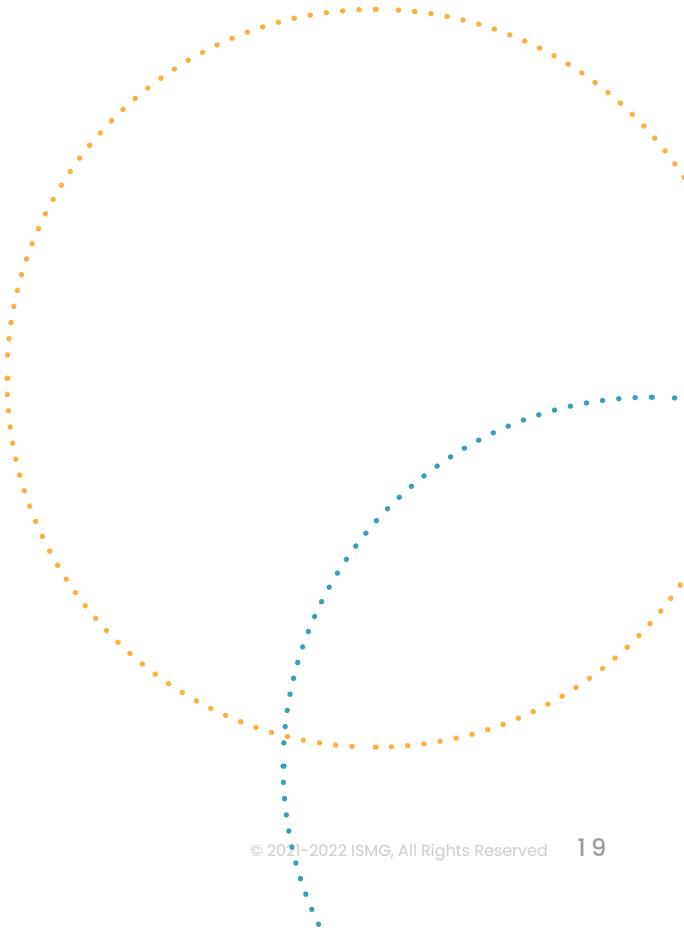
Boyd argued that the party that consistently completes the cycle faster gains an advantage that increases with each cycle. The enemy's reactions become increasingly slower by comparison and therefore less effective until the will to continue is broken.

In cybersecurity warfare, this process has great merit and is the basis for improving performance of the skill of maneuver in the Incident Response Plan. If the orientation and decision steps are integrated with threat intelligence, the subsequent action should provide an advantage to the defender relative to the risk/reward trade-off resulting from a bold decision.

"Continuous Oversight" plays an important role in Tempo. The principle of Tempo is only effective if leadership is regularly visible and stressing the importance of enterprise security as envisioned by the Focus. By leading from the front and pushing decision-making to lower levels, the Tempo of a response will increase. Decentralized decision-making eliminates excessive debate, and the maneuver warfare practitioner is able to seize the initiative.

In seizing the initiative, a superior state of preparedness for the countermove and a position of relative advantage are assured, resulting in an enhanced ability to predict and prepare for the adversary's next move.

Your adversary is not pausing their evolution of threats in order to allow you to be prepared. As with traditional warfare, the ability to rapidly and successfully maneuver to change your situation, relative to threat conditions beyond your control, is dependent on the principle of Tempo.



6. Combined Arms

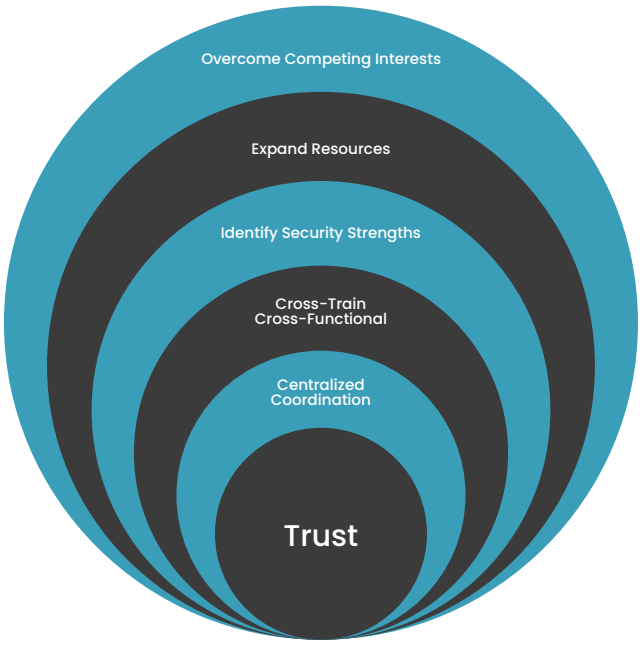
"The challenge for every organization is to build a feeling of oneness, of dependence on one another because the question is usually not how well each person works, but how well they work together."[xx]

Combined Arms can be incredibly effective but it is an inherently complex and difficult endeavor that demands the utmost cooperation, practice, communication, and implicit understanding throughout the organization's Mature Cyber Model.

Its effectiveness is dependent on extensive cross training of the security team members' specialties to instill a better understanding between functional areas regarding their role in the combined effort.

A key determinant of success in the use of this principle is overcoming competing interests that might exist within the IT department, the information security team and the business departments dependent on both to operate in a manner that enables achievement of their business objectives. In information security, the operational environment is most often seen as a source of multiple attack vectors and therefore is at a disadvantage when developing a defense. Digital transformation, the continued expansion of IoT and IIoT technology, insufficient situational awareness training that results in human error and work from home have placed security teams at an ever-increasing disadvantage.

The Elements of Combined Arms



"Combined Arms is the integration of complementary weapons in a manner that creates a synergistic effect and places an opponent in an inescapable, hopeless situation, otherwise known as the horns of a dilemma."[xxi] In information security, this is the integrated deployment of technology, people, and processes in a manner that increases the collective effectiveness."

If the organization takes the strategic approach of identifying third-party Combined Arms team members with a high confidence probability, such as strategic supply chain partners, third-party technology providers and security advisors, the operational environment can be strengthened. By deploying these expanded resources in a manner that enables the maneuver warfare practitioner to have a response no matter where the adversary attempts an infiltration, a higher likelihood of success can be expected.

[xx] Vince Lombardi, Head Coach, Green Bay Packers
[xxi] The Marine Corps Way, p123

This approach requires confidence and efficiency of performance in coordination throughout the organization and all parties of the Combined Arms team. The team must have one leader to effect centralized coordination, execution and cross-train all team members on standard operating procedures. The efficient and effective execution of such coordination will result in a multi-faceted, custom-tailored team that improves the understanding of the security vision being implemented.

Because success requires a high confidence probability between functional leaders and their subordinates, cross functional cooperation must be rewarded with recognition, compensation, or promotion, and there must be a constant reinforcement of the Combined Arms mindset.

An example of the strategic use of this principle, from an adversarial perspective, might be the circa 2009 cyberattack on Estonian systems (i.e., banking government websites, state sponsored media outlets, and electrical systems to any other connected system) that were of military or strategic importance to the Russian military forces moving into position at the border. This combined effort provided the ability to force their will on the Estonian government without having to engage in a traditional war.

MANEUVER WARFARE IN SUMMARY

The principles for maneuvering in the continuously changing threat environment are applicable to any situation that requires flexibility and rapid response to that change. Each of these principles can be applied individually but, Maneuver Warfare is about applying these principles simultaneously – in subsets, or as an integrated whole – to affect the most decisive and positive outcome at the least cost.

Maneuver Warfare is difficult and requires a high degree of self-confidence, a healthy appetite for calculated risk and the unwavering commitment of the leader and executive team. In any industry, it will require a radical change in culture relative to security as a business priority not an IT issue.

Applied in an integrated manner, the principles complement and reinforce one another. It does not require the leader to become a master tactician but it does require an increase in bidirectional trust if it is to be executed efficiently.

In this world of digital transformation, a high confidence probability in the identity of a user, device, or service is essential to the protection of critical assets.

The efforts to achieve such a high confidence probability, through the design principles of the Zero Trust model and strategy, can be further supported with the incorporation of the principles of DoMW with the design principles of the Zero Trust model and strategy.

ZERO TRUST AND THE PRINCIPLES OF THE DOCTRINE OF MANEUVER WARFARE

"We have to change the way we think about cyber – broaden the mindset and change the perspective regarding cybersecurity defense."[xxii]

It is universally accepted that as the implementation of technology to meet digital transformation objectives expands, so too will the attack surface available to the cybercriminal. If this continuously expanding attack surface is to be defended, the perspective on how we achieve that defense must change.

The perspective of any mindset can only change if the person or organization continuously strives to increase knowledge, apply that new knowledge in addressing situations and use that experience to adjust their perspective regarding how to approach a similar situation in the future.

Zero Trust is a reference framework and a strategy to plan and execute the journey to broaden the mindset and establish the proper perspective for setting a flexible and adaptive cyber defense in an organization's operational environment. The strategy of Zero Trust is to shrink the attack surface, reduce the excessive trust landscape of the organization, and, through rigorous always-on monitoring and continuous insistence that users prove who they are and why they need access, improve identity management. Such a strategy elevates the confidence level in the claimed identity

[xxii] General Keith Alexander (retired). Former Director of the National Security Agency, Chief of the Central Security Service, and Commander of the United States Cyber Command.

and contributes to achieving the goal of risk mitigation.

Implementing the DoMW principles as a tactical component of Zero Trust can, and will strengthen the will of an organization to develop and maintain the security behavior necessary to meet the security leader's intent in all situations. The principles can change the rules of engagement to the defender's advantage and assist in creating an offensive/proactive defense posture for risk management.

In each of the five design step principles of the Zero Trust architecture, one or more of the DoMW principles are potential tactics to be implemented in support of the architecture design.

ZERO TRUST DESIGN PRINCIPLES

The execution of the Zero Trust strategy using these design principles will be consistent for all protect surfaces. The implementation of tactics in support of the design of a specific protect surface can and will vary. The Principles of the Doctrine of Maneuver Warfare both support the Zero Trust strategy and improve the organization's ability to adapt to and overcome obstacles encountered on the journey to a mature Zero Trust operating environment.

STEP 1: IDENTIFY CRITICAL ASSETS AND DESIGN THE PROTECT SURFACE

A protect surface is orders of magnitude smaller than the attack surface of the organization. Because it is a single area of focus, the principle of Focus can have significant value in this first step.

The center of interest is answering the question, "What do you need to protect?" Every protect surface has a DAAS element – Data, Assets, Applications, & Services – that is the answer to the question.

A central tenet of Zero Trust is collecting as much information as possible regarding the current state of the DAAS element, the network infrastructure, and communication. Each of these components will have existing vulnerabilities that must be identified and addressed. The principle of Target Critical Vulnerabilities is a tactic in support of this tenet for each component of the DAAS element. It will provide valuable insight regarding both the controls and their placement within the protect surface.

The principles of Bold and Surprise are tactics to consider in preparing the defense of this protect surface. Being Bold in any competitive situation is critical in controlling the move/countermove process. In the case of Surprise, employing deception can be invaluable.

STEP 2: MAP TRANSACTION FLOW

It is critical to understand how systems should work and flow, and how various DAAS components interact with other resources on the network if the protect surface is to be properly designed. The way traffic moves across the network, specific to data in the protect surface, determines how it should be protected. The intelligence gained through Target Critical Vulnerabilities and used in conjunction with the principle of Combined Arms would enable a more informed design of the protect-surface architecture.

STEP 3: ARCHITECTURE

The architecture is constructed around the protect surface and will vary depending on the differing needs of the organization's business and use cases chosen to extend Zero Trust.

A multi-disciplinary focus involving data scientists, human factor risk experts, risk researchers, computer scientists, and network engineers is an example of the principle of Combined Arms in this step. The benefit of this principle in this step is the change in mindset, so critically needed, and subsequent perspective as a result of the new mental models, generated by the multiple disciplines of the members, that will be created and added to the existing mindset. These new mental models will better enable leveraging network segmentation, prevent lateral movement, provide Layer 7 threat prevention and simplify granular user access control.

The principle of Focus, as it pertains to planning, preparation and training, and providing equal priority to people, process, and technology, has relevance in completing this step in the design process.

STEP 4: ENFORCE POLICY

Enforce policy by answering the questions:

1. Who should have access?
2. What application to what resource?
3. When should they have access, if they don't need it – turn it off, from where do they have access?
4. Why are we doing this? – Data classification, sensitivity level.
5. How should we protect it?

The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture. The principle of Target Critical Vulnerabilities may be a source for some of this information.

As the organization continues on the Zero Trust journey, significant changes to the system – such as new devices, major updates to software (especially Zero Trust logical components) and shifts in organizational structure – may result in changes to the workflow or policies. If a change occurs to the workflow, the operating Zero Trust architecture needs to be reevaluated. In such a situation, the Target Critical Vulnerabilities principle would serve the reevaluation effort.

With such change, the Combined Arms principle may add to the understanding of how existing technologies and controls will integrate with the changes being made.

STEP 5: CONTINUOUS MONITORING AND MAINTENANCE

Zero Trust is an iterative process and intelligence gathered in the Continuous Monitoring and Maintenance step can be used to support the seven principles of DoMW.

This may be where the DoMW has the greatest value in support of Zero Trust. The intelligence gathered through this step can be applied to all of the principles and improve the organization's ability to maneuver as the situation demands.

Increased intelligence gathering from continuous monitoring provides greater insight related to the vulnerabilities identified using the principle of Target Critical Vulnerabilities.

The principle of Focus, as the organization works to improve the security of the protect surface, will benefit from the intelligence accumulated from this continuous gathering of information. The focus on risk mitigation, using this data, will provide the ability to create scenarios for testing the defense against targeted vulnerabilities.

Confidence gained in decision making, as a result of the scenarios, will enhance the execution of the principle of delegated decision-making for the protect surface. The security leader will have greater assurance that decisions made at this level will improve the Tempo of response and be made in a manner that supports security intent.

CONCLUSION

As Sun Tzu says, "Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat." There are numerous tactics available to the cybersecurity strategist and the Principles of the Doctrine of Maneuver Warfare are a set that compliments and supports the Zero Trust strategy.

Cyberspace is, in all truth, the battlefield on which the war of the future is currently being fought. It is the only domain on the planet where a nation state such as North Korea or Iran can have the same devastating effect as the most powerful nations.

The current mindset must change if corporate America is to develop the warrior perspective required to compete on this battlefield. The Zero Trust model and strategy is the path to achieving that perspective.

Supported by the tactics of DoMW, the ability to maneuver, adapt to the changing threat environment, and rapidly respond and seize the Tempo necessary to control the battlefield!

Time is of the essence. The impact of a data breach on an organization and compromise of critical data can be devastating.

The organization that is willing to make the initial investment and maintain the necessary commitment to take this war seriously will succeed in reducing the likelihood and impact of a breach at a significantly higher rate than those who do not.

THE CYBER THEORY INSTITUTE - ZERO TRUST

Invented by our co-founder, John Kindervag, Zero Trust is becoming both the security model of choice for enterprises looking to up their game and change the relationship dynamic between the attackers and defenders, and a pure marketing movement at the same time.

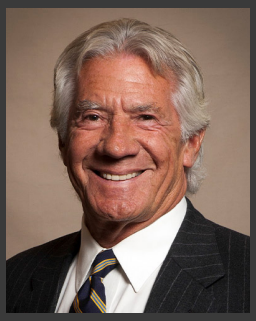
Far too valuable and necessary a concept and operational model to be abused by hype, we have organized founding members of the Zero Trust community into a fellowship designed to promote and advance the Zero Trust agenda throughout the world by demonstrating all of the ways in which Zero Trust can and should be implemented and for all of the right reasons.

Our goal is to change the shape of cybersecurity's defense agenda so that it fits around the Zero Trust strategy and forever rearranges the attacker/defender dynamic.

AUTHOR BIOS

CLIFF KITTLE

A graduate of the U.S. Naval Academy, and following his service as a Captain in the Marine Corps, Cliff spent 20+ years in the cybersecurity market with companies like Secureworks, Booz Allen Hamilton and SafeLink. Cliff is a highly regarded thought leader, author, and lecturer in cybersecurity issues and matters.



STEVE KING

The managing director of the CyberTheory Institute, a think tank with a mission to drive change through dialogue, leadership, and action to help solve the greatest cybersecurity challenges of our time. Steve has been in the cybersecurity space for 25+ years, started and exited three start-ups, and currently is responsible for multiple initiatives for ISMG.

JOHN KINDERVAG

The 'Father of Zero Trust,' who as an analyst at Forrester invented the term and defined the reference architecture for a network whose five basic principles defined the notion of zero trust. John is also the co-founder of the CyberTheory Institute and an Executive Fellow. John went on to become the CTO of Palo Alto networks, influencing the design of their network product suite whose policies now determine who can transit the microperimeters at any point in time, preventing access to what John has coined the "protect surface" by unauthorized users and preventing the exfiltration of sensitive data.

Editorial credit to Kiren Chaudry