Journal of Defense Studies and Resource Management

Arbiter Framework and the Adaptive Strike Chain

Adib Einayat*

Department of Electronic and Cyber Warfare, Genesys Defense and Technologies, Columbia, USA

*Corresponding author: Adib Einayat, Department of Electronic and Cyber Warfare, Genesys Defense and Technologies, Columbia, USA; E-mail: adibenayati@genesysdefense.com

Abstract

Arbiter is a multi-domain, detail intrinsic, progressive objective-oriented framework designed to aid you in operational planning for strategic success. It introduces the adaptive strike chain and it is a part of the nightshade advanced polymorphic electronic defense and warfare doctrine.

In a brief definition, nightshade consists of a variety of frameworks with an active focus on electronic warfare and implementing it in the five domains of modern warfare, perhaps the most prominent of all is the special focus on cyber defense and security while keeping one primary objective above all which is mastering and dominating the electromagnetic spectrum for long term strategic supremacy and domination. The arbiter framework and the adaptive strike chain are just a small part of this vast doctrine, which covers both offensive and defensive strategies for covert and overt military, private and civilian operations. Nightshade argues that supremacy in modern warfare can only be achieved by mastering and dominating the EMS on current and future battlefields.

In this paper, we will discuss conventional deterrence and its possible usage scenarios as well as briefly introduce electronic deterrence and its characteristics, benefits, and possible usage scenarios, we will construct a clear definition for classical and modern electronic warfare, The role of intelligence and principles of war and ultimately, we will introduce the arbiter framework and dissect the adaptive strike chain and go over a couple of strategies that can be used within the framework for maximum effect.

Keywords: Arbiter; Electronic warfare; Adaptive strike chain; Electromagnetic spectrum; Cyber defense

Introduction

Warfare is probably the oldest science that our ancestors tried to master. Our inheritance from our forefathers, an art that every generation has tried to perfect. The rise and fall of the civilizations summarized in their advancement in the defense and warfare. Wars have been fought for different reasons, but ultimately, we must learn this is the art that plays the primary role in our very safety and survival [1].

Human civilizations have been divided for every reason that we could ever think of. Race, culture, religion. Every country wishes to advance and dominate the rest. Collaboration and cooperation as a unified race have never been an option, and it never will be. The very nature of humanity seeks conflict rather than advancing in harmony. Take a look at human history; we have never stopped crafting weapons to kill one another; we have never stopped trying to think we are one equal creation. The strong has never stopped enforcing its will on the weak. We are just a triumph equaled only by its monumental failure [2].

However, On the contrary to popular belief, warfare is not just about killing one another in the most gruesome way. The greatest general in history of humanity and the brightest mind in warfare, Sun Tzu said "the supreme art of war is to subdue your enemy, without fighting". Our world is not strategically balanced and frankly it will never achieve that balance with the current status quo, and the primary reason is our desire for conflict and exerting our will and superiority over each other.

Modern warfare has its perks; the combination of the five domains of modern warfare (air, ground, sea, cyber and space) gives us a wide range of capabilities to practice the art of war. Each domain of modern warfare is more important than the last. Domination in each domain guarantees the domination of the next; as in modern warfare they depend on each other's support. Combination of all will bring superiority to the fold [3].

Hybrid operations play an essential role in today's advanced operations. It's required to combine the domains to achieve the best outcome. Combined use of the domains will provide you with an unparalleled superior advantage on the battlefield and guarantee precision and success.

Never underestimate your enemy; a desperate adversary can surprise you; desperation brings the worst out of anyone. You cannot contain that. The other fact that you need to always remember is that never assume your defenders are perfect, there is always a way and never assume your attackers are perfect, if you are in the defensive position and you are facing an overwhelming enemy forces the moment that you assume your attackers are invincible you have already lost the war [4].

Conventional deterrence

The action of discouraging an action or event through instilling doubt or fear of the consequences is called deterrence. Nuclear weapons are considered a deterrent. Possessing the nuclear triad and a nuclear strike capability has been considered the deterrence in the modern era until this day [5]. The principal of the Mutually Assured Destruction (MAD) has been the doctrine around the use of the nuclear weapons until recently that the United States, during the trump administration decided to develop low yield tactical nuclear warheads to be able to increase the Russian nuclear threshold and to be able to use the nuclear weapons without being concerned about the massive fallout of the high yield weapons (Figure 1). The deterrence is highly dependent on the delivery mechanism, which is called the nuclear triad. The nuclear triad means the ability to deliver the weapon from sea, land, and air.
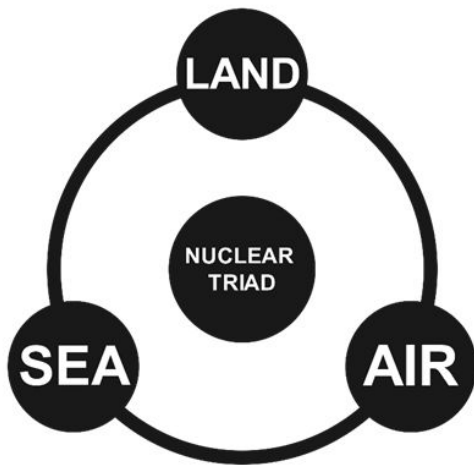
Figure 1: Nuclear triad of sea, land, and air.

According to the 1967 outer space treaty, the placement of weapons of mass destruction in outer space is prohibited. However, world powers have always considered dominating and weaponizing space simply because space is the next frontier in the development of our civilizations. The world powers do not care about the treaties they bend the rules just because they can it's an unfortunate fact. Space can very well be weaponized in the near future, consider if a nuclear weapon is placed in orbit which can drop anywhere on earth at the reentry speed (March 21) which gives the defending party and the ballistic defense shield seconds to act specially if the warhead is the glide variety, so weaponizing the space is very appealing for the world powers; considering with the advancement of the technology other things such as, total domination of the space, mining and settling are also considered and are appealing to them.

The nuclear threshold refers to the ability of the adversary to tolerate the use of a nuclear weapon on its territory without considering the use of high yield nuclear armament in response. A theory that has been widely argued, but nevertheless United States and NATO have been considering it.

Importance of the deterrence

The nuclear triad is supposed to be the strategic deference for nuclear capable countries [6]. The only factor that they have been betting on is that the nuclear weapons can be deterrence on the principles of the mutually assured destruction.

MAD is no guarantee of safety; it simply is the end of all life on earth. The military doesn't care about the long-term effects of its actions or in this case, ground zero and the entire world.

Nevertheless, we cannot deny that strategic deterrence is a necessity of modern warfare. Any country that goes to war without a strategic deterrence is ultimately the loser of the war. If you are not the winner of the conflict, you surely won't be called the loser either.

Thus far majority of the people and the military members thought that a nuclear strike was only ordered in the event that an adversary has launched the attack or when the very existence and survival of the nation is threatened.

However, that is not the case with the low yield nuclear warheads which the United States is developing under the new nuclear warhead modernization plan. Within the new strategy, a low yield tactical

nuclear strike can be ordered as a response to a mass scale conventional war on the United States and its allies.

The argument surrounding the conditions of the use of nuclear deterrence is beyond the scope of this paper and we will not discuss the moral and technical issues of the use of such weapons. However, we will discuss the possible alternatives that it can offer to the strategic use of such weapons. Remember that the military will never consider the long-term effects of such strikes. When its times for such a response only for the effects in ground zero is considered. Whether it's a counterforce or counter value or just simply a disproportionate retaliatory strike. There are four usage scenarios has been considered by the author of this paper.

Possible uses of the conventional deterrence

- High yield nuclear strike.
- Low yield tactical nuclear strike.
- Use of high yield salted weapons as a massive area denial weapon.
- High altitude air burst for HEMP effect.

Conventional nuclear strike: Anatomy of the options

High yield disproportionate/proportionate nuclear strike is essentially same as MAD. A series of preplanned target packages designated to be a response for various scenarios if the strike conditions are met. The number of warheads and targets depends on the target package and the severity of the response. The result of such a scenario, if, however, the response is on a large scale, could ultimately cause billions of deaths and be the end of all life on earth directly and indirectly. Remember, the secondary effects of the nuclear weapons are never discussed or considered in this scenario, which is why it is called Mutually Assured Destruction (MAD). Other lives do not matter, only retaliation towards the enemy to ensure that the enemy is fully destroyed and cannot recover from the attack matters.

Materials and Methods

Low yield tactical nuclear strike is essentially the use of a nuclear weapon system in a very limited way. The fallout and the destruction are proportional to the yield and the technical deployment of the weapon system ground or airburst. The use of such nuclear weapons is to ensure that a certain localized area, such as a C2ISR/C5ISR command and control bunker or a military valuable base, is destroyed or becomes combat ineffective. United States uses the w88 warheads for developing such weapon systems. Take note that the fallout of a nuclear weapon is calculated in real time and prior to an attack. The fallout depends on many factors, especially the wind direction, and weather [7]. Below you can see the crude comparison of the mushroom cloud of a tactical nuclear weapon and a strategic high yield option, which in this case is the W-78 warhead, with a minuteman III vector. (Only mushroom cloud is simulated in a ground burst attack) (Figure 2).
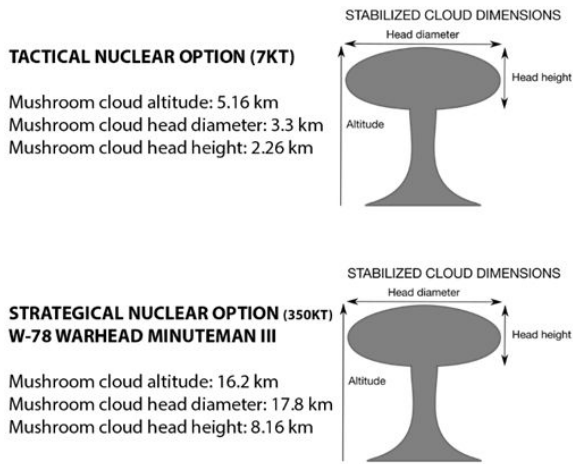
Figure 2: Crude comparison of a low yield tactical nuclear warhead with a high yield warhead (Ground burst effect).

Salted nuclear weapons are weapons that produce massive radiological fallout. It is achieved by infusing the nuclear warhead with cobalt 59 to produce cobalt 60 upon blast. The term salted refers to the fact that using such weapons will render the blast radius life-free for generations (Figure 3). It can be used as an area denial weapon system with extreme consequences for the environment and all life forms that live within the area other fallout factors aside.
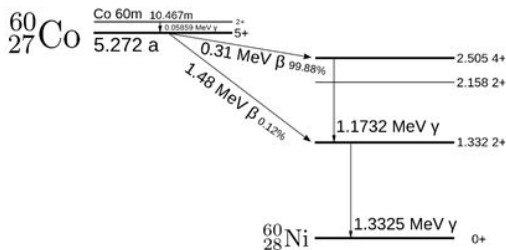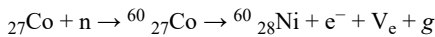
$$_{27}Co + n \rightarrow {}^{60}{}_{27}Co \rightarrow {}^{60}{}_{28}Ni + e^- + V_e + g$$

Figure 3: The decay spectrum of the cobalt-60.

A high altitude air burst can be used in two ways for a single purpose. It can be used in the beginning of a military operation or as a response to a nuclear strike. One of the awesome products of a nuclear explosion is the effect that we call a transient electromagnetic disturbance, or as the public likes to call it, the electromagnetic pulse. Thus far, there is no artificially generated EMP that can replicate the full effect of HEMP. The closest thing to it is called an "explosively pumped flux compression generator" which is the heart of the non-nuclear EMP bomb (Figure 4).
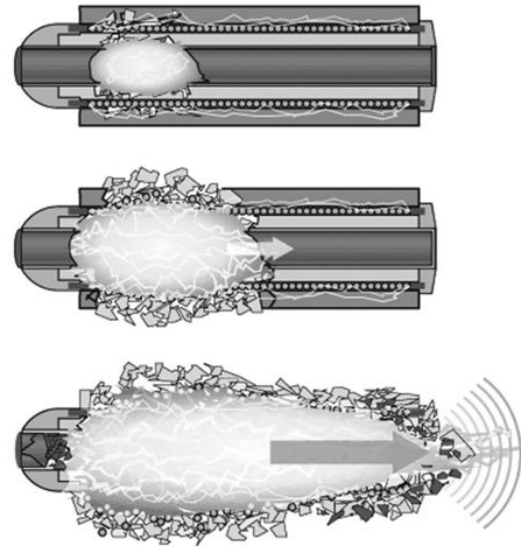

Figure 4: Explosively pumped flux compression generator simple diagram.

The use of a high-altitude nuclear blast for the purpose of using of its electromagnetic effect is a way to produce a high-powered pulse to destroy the infrastructure of a country, from the radar and radio systems to the unprotected civilian and military infrastructure. Let's put it this way, all systems will go down in a wide geographic Area based on the altitude and yield of the blast unprotected systems and infrastructure will be destroyed; bridges and pipelines will act as propagating antennas (Figure 5). Communications will not be possible due to the ionization effect of the charged particles for a considerable amount of time in military, communication is the key, even a couple of hours without communication can be considered a major disturbance When we are talking about the altitude, we are talking 200 km and above within to above the ionosphere so the risk of the nuclear fallout is minimum, remember the worst fallout belongs to the ground burst blasts as the famous mushroom cloud sucks away the dirt and mix it with the product of the nuclear fission then scattering it across a large area and when that happens it spreads with the wind and rain [8]. So, airbursts are the safest in terms of fallout.
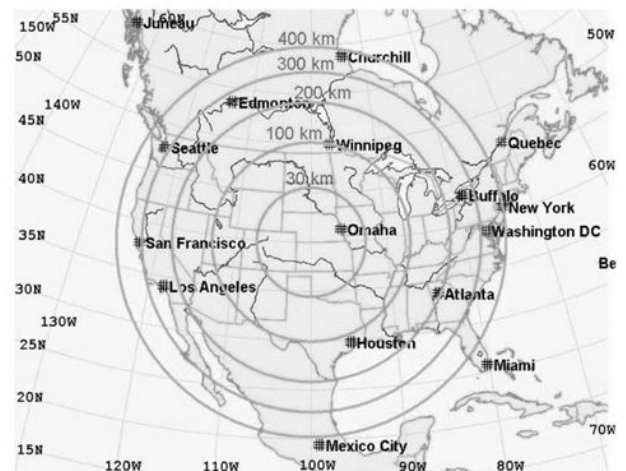

Figure 5: Effect of a high-altitude air burst blast altitude to area of effect.

Definition of the electronic warfare

The art of using the electromagnetic spectrum and using it to plan an offensive and defensive operation is called electronic warfare. Electronic warfare is split into two major categories which are active operations and passive operations. The chart below will aid you in understanding the classical components of electronic warfare (Figure 6).
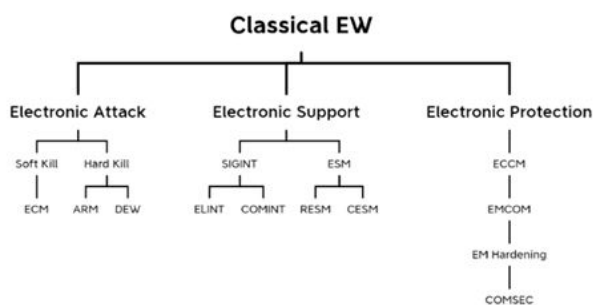

Figure 6: Classical components of electronic warfare.

The classical electronic warfare capabilities used to think of it as a force multiplier, but it all has changed. When you are fighting a symmetric war with your adversary, you cannot achieve domination and you are just in constant challenge to achieve that domination. The goal is always to have the upper hand and superiority to be able to fight in an asymmetric war in your favor. Electronic warfare and the modern operations will give you this enhanced capability (Figure 7).
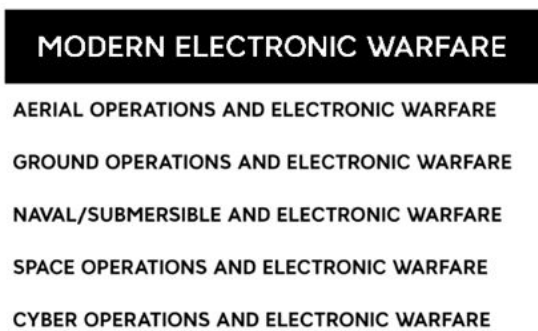

Figure 7: Electronic warfare for the five domains of the modern warfare.

Cyber operations and warfare are just a subcategory of the electronic warfare, contrary to the popular belief cyber security is very much different in the military point of view and the public point of view and as always, the militaristic point of view is the best and most complete probability and scenario planning in defense and offense.

A blast from the past: Electronic warfare in defense

You should understand that your adversary is trying to do the same thing. Superiority is an infinite goal. There is absolutely never a time that you can maintain your superiority for long.

Take Russia, for example, after the collapse of the Soviet Union, Russia had the misfortune to inherit a majority of the military hardware since Russia was also the largest country of the USSR. In case you are not aware of it, military hardware requires constant maintenance and the cost of the maintenance depends on the diversity and quality of the hardware as well as the terrain and the usage.

United States chose and adapted the "air superiority" strategy after World War II. Applying this strategy, United States had created a variety of the aircrafts. Perhaps the most notable one is the A10-Warthog or the improved version-A10 thunderbolt. A10 has been designed to be cheap and quick to produce, back then during the cold war, the idea was that if the Russians, with their vast supply of the tanks, attacked Europe, the A10s would be the response and save the day [9]. Years have passed and United States had a vast arsenal of different aircraft and therefore maintained huge air superiority over Russia.

After the collapse of the USSR, Russian military and the Russian military infrastructure could not bear the cost of the maintenance of most of the hardware, so they had to make a choice if they wanted to continue competing with the West. They decommissioned military units and hardware to cut costs and decided to invest in the opposite strategy to be able to defend them and to be able to sustain if a war ever broke out with the West, so they began to develop excellent anti-air technology and weaponry. Various weapon systems were born. These systems deterred the West from attacking Russia by air, so the Russians had a chance to fix their economy and repair their military industries.

As a result, various aircraft have been designed and produced over the years and finally they could compete with the vest to be objective. Eventually this wasn't enough, for developing state of the art fifth generation aircraft such as the T-50(SU-57) they had to establish some industries that wasn't established in Russia prior to the development of the programs (such as: Fiber optics and etc.). Some readers might not understand the importance of this. When you want to develop and build a new fighter plane as example, especially in the military industry; you must be able to reduce your reliability to the foreign supply chain. You must be able to produce quality materials and components by yourself; otherwise, there are risks such as sanctions, supply chain attacks and corruption. When you start a new line of weapon systems, you expect this equipment to last for many years, compared to the cost and the intellectual investment that you made in them [10].

If you think establishing an entire industry to support only a part of your weapon program is not practical, then you are wrong. Some technologies are dual use. Let's say fiber optics, for example, they are the backbone of the high-speed modern-day communication in the communication network along with many other uses; so, you advanced both your military and civilian infrastructure with a correct investment, not to mention creating a very secure supply chain for your military and civilian infrastructures [11].

Russia was still vulnerable. Russians invested in one thing that gave them the edge against NATO. They invested in electronic warfare and modern electronic warfare systems and countermeasures. They have developed a wide range of arsenals. It's no secret that the entire United States stealth program was based on the research of the Russian scientist "Pyotr Ufimtsev". At the time the Russians dismissed the work of this brilliant scientist but the West did understand the value of it and started their stealth program based on his research and overtime with investment, they perfected it.

Another example is that while the United States disregarded the effective use of the VHF and UHF band radars, the Russians continue to develop them, and they now use these systems in combination with other radar systems in order to detect stealth aircraft effectively.

Ultimately, Russians now have the upper hand in the modern electronic warfare systems according to the report of the Estonian defense ministry dated September 2017 and titled "Russia`s electronic warfare capabilities to 2025 challenging the NATO in the electromagnetic spectrum" with the forward of the "general retired Michael Hayden" former director of the NSA and CIA.

Alright, let's conclude that anticipating and studying your adversary and modeling their behavior using the correct frameworks and having strategic awareness and oversight will aid you in making the right decisions that will affect your safety and superiority in the long term.

Electronic warfare continues to grow and it is now more than just a force multiplier. Direct energy weapons, which are the children of electronic warfare, will be widely used in future battlefields. Quantum radars are the next generation radar systems that might make stealth technology obsolete. As I have always argued, mastering the electromagnetic spectrum is the key to all doors.

Results

Proposing electronic deterrence

The author describes the electronic deterrence as a mantra of techniques and series of pre-engaged and access maintained soft and hard strategical electronic targets with the combination of the strong intelligence and verification network as well as kinetic electromagnetic weaponry which can be used to exert pressure on the adversaries infrastructure or destroy the electronic civilian and military infrastructure as needed by preconfigured target packages verified with the enhanced damage assessment and possible response model.

The advantage of electronic deterrence is that if it executed right, you strip your adversary of the ability to respond effectively and logically or even be able to respond to anything at all.

First of all, the nightshade doctrine is designed based on the superiority of the electromagnetic spectrum. We cannot run from it. The spectrum controls our technology and our very existence in the universe [11]. Its ranges from radio waves all the way to the gamma rays. It's used in our daily lives, the very electronic devices that you use or the light that reflects back to your eyes is all part of the spectrum.

The electronic deterrence proposes the development and use of tactical electronic and electromagnetic weapons and weaponizing the electromagnetic spectrum. Imagine instead of destroying the entire city just to destroy a bunker by inducing an artificial blast or electronic weapon electronic weapon is also called cyber weapon that can destroy critical infrastructure, communication, radar and weapon systems without actually destroying them physically and cause loss of life in mass scale. Imagine, being able to destroy the ability of your enemy to fight. Destroying the economy by manipulating the banks and stock markets. Developing smart cyber weapons to be dormant within your enemy's infrastructure and be activated when you need them, just like a nuclear deterrence but the difference is that it's as fast as the speed of light. What the majority of people call cyber warfare is not as simple as simple minds think.

Cyber warfare is just the youngest child of electronic warfare. The true combination of them is pure intelligence and effective use of the spectrum. Cyber criminals introduce anarchy, but they are just simple criminals. If you wish to practice it in the art of war, then you must learn how to use it the way it's called true warfare.

"Nightshade" advanced polymorphic electronic defense and warfare doctrine is the ultimate guide for this. Bear in mind that there are military standards for the hardening of the sensitive electronic equipment in the military but not for all, and also take note that communication platforms and equipment are usually the most vulnerable and technically the right Kinetic and none-kinetic weapons with the correct amplitude/execution can achieve the desired effects. One may ask that what is so special about the electronic attacks particularly the cyber operations that makes it so unique.

Well, electronic (cyber) attacks are ambiguous and hard to attribute to one country or a person. What we mean by ambiguity is that you cannot ascertain who is behind the cyber-attack, you cannot attribute the attacks and determine the origin of attack simply because there are plenty of ways to hide your signature and footprint, manipulate traffic and even obfuscate or manipulate the code used in the exploits and malwares to pose as a different actor sponsored by another country. Attribution is important because you cannot justify a response without being able to prove that if in fact whether a state-sponsored actor or just an anarchist group is behind the attack.

Determining who's responsible for the attacks is the first phase of planning a proportional response and preparing better defenses for the future. However, in the nightshade we have a special adversary classification and identification mechanism which is vital to strategical defensive operations.

Cyber-attacks are not grounds for jus ad bellum jus ad bellum is a set of criteria that are to be consulted before engaging in war in order to determine whether entering into war is permissible however, in nightshade I have argued that there are ways to correctly attribute and investigate the attacks and plan an active military response doesn't have to be kinetic-electronic attack will suffice, but active conventional military response might be used based on the scale of the attack.

The fact that no country wishes to go to war and be the primary aggressor is why majority of the countries have a passive response to the cyber-attacks but as we know this status quo cannot last forever.

One last note on this subject, which also makes electronic deterrence more viable, is that if your country doesn't have strategic armament nuclear-based you can invest in electronic defense. The nuclear non-proliferation doesn't permit any country other than the current nuclear capable countries to have nuclear weapons. This permits these countries to maintain superiority over all others and to keep the balance of power in their own favor and dictate the terms while advancing their military industries. Conflict is inevitable especially when it comes to human nature. Your electronic deterrence doesn't necessarily need to fly over and be attached to an ICBM. Your electronic deterrence can be smart, dormant and be activated as you need at the speed of light, anywhere and anytime. With all that said, I will stop discussing this further.

Defense against the electronic deterrence

We have ballistic missile shields that can detect and take out nuclear threats in various stages; we also have counter-countermeasures to protect our own arsenal and make our own weapons systems more effective. The electronic defense in the cyber world thus far has been passive. For the first time night shade

Discussion

The role of intelligence and the principles of war

There are various conventional and modern strategies and every single one of them has its merits. The two prime categories are offensive and defensive strategies. Adaptive strike chain is an offensive strategy and falls under that category but given to its structure it can be considered both; for example, you can use the same chains to identify that you are being struck by the adaptive strike, which is actually the defensive mode of the adaptive chain.

When you are trying to choose a long-term strategy to fight an adversary, you usually choose a combination of the offensive strategies. Combining them gives you more mobility and flexibility and it very much depends on your arsenal, budget and capabilities. Modern operations rely on proper intelligence for success. Intelligence is the most important part of every operation. That means having a robust and powerful intelligence gathering and verification network is a must. Being able to verify the intelligence that you have gathered from your active and passive sources is vital to your success. Every single bit of data that you gather has value and its worth; you need to be able to categorize and prioritize them and extract the actionable intelligence before feeding them to a chain of command. Therefore, before starting any operation you are required to ensure your intelligence network is operating and it is effective.

Counterintelligence is probably at the heart of your defensive strategy and operations. Whether it is in its conventional or modern form, it should ensure that foreign operatives cannot penetrate your intelligence and military networks. You must be able to protect your own C5ISR before considering attacking others. The C5ISR is also considered your center of gravity. With the use of modern electronic equipment for communications, the role of the ELINT and COMINT is more important than ever. Critical infrastructures had to modernize to be able to compete and produce. Which again forced them to use the modern technology and as a result they are now even easier to access; just imagine manipulating and attacking the SCADA systems of a production plant or uploading a virus to disable the safety features of a nuclear plant and cause the reactor to overheat and explode. Tracking individuals based on the hardware they use with their emissions and emanations. These are just some simple scenarios that could happen with the use of modern electronic warfare.

Principles of war are the fundamental elements that are considered essential in the success of war. You are required to ensure that you follow these principles in any military operational planning. These sets of principles are:

These principles may vary in different countries but the essence is the same

- **Attack in depth:** Destruction of the enemy throughout their depth of deployment as needed.
- **Objective:** Direct every operation towards a clearly defined set of objectives.
- **Offensive:** Seize, retain and exploit the initiative.
- **Mass:** Concentrate combat power at a decisive place and time.

- **Economy of force:** Allocate the minimal essential combat power to secondary efforts.
- **Maneuver:** Place the enemy is a disadvantageous position.
- **Unity of command:** For every objective ensure unity of effort under one responsible commander.
- **Security:** Never permit your adversary to acquire an unexpected advantage.
- **Surprise:** Strike the enemy at a time and place when he least expects it and he is unprepared.
- **Simplicity:** Prepare clear plans and concise orders to ensure clear understanding.
- **Strategic deterrence option:** The author of this article defines strategic deterrence as a weapon or set of options that can change the outcome of the war to your favor or to ensure your adversary that the use of such weapon or option will inflict great damage to their ability to defend, respond or simply exist. Ultimately, strategical option must give you a unique strategical advantage to deter your enemies from attacking you or inflicting considerable damage to your abilities to defend and respond.
- **Cooperation:** Incorporation of the teamwork and the shared risks and your multidomain units.
- **Flexibility:** The ability to change when you meet new circumstances consists of agility, responsiveness, resilience, acuity and adaptability.
- **Readiness:** The ability to respond to any number of scenarios, achieved by training and practice.
- **Obedience:** Train your troops to be disciplined and subordinate.

Arbiter Framework

Progressive Comprehensive Plan of Attack (PCPA)

Arbiter framework utilizes the adaptive strike chain at its heart. Adaptive strike chains are the utility which guides you on how to plan your strikes and achieve the ultimate goal. It gives you the ultimate flexibility, adaptability and foresight in your conventional or modern offensive and defensive planning. There are some basic rules that are applied to the framework which must be precisely followed.

As we have mentioned earlier in the paper. Arbiter is a progressive framework. It means at every phase of the operations you must have defined a series of primary and secondary objectives using the intelligence gathered via your intelligence and verification networks. These objectives should help you achieve your ultimate goal or strategic objective. Your strategic objective (s) should be a finite goal. There two types of objectives;

- **Tactical:** Tactical objectives are a set of objectives that by achieving them you will be in a better tactical situation. A tactical objective can be mandatory or secondary. These types of objectives do not consider the long-term and should not be resource consuming in comparison to the strategic objective. Remember, the objectives you define should help you progress and not force you into a finite loop. Any sort of finite loops in the arbiter and adaptive strike chain is bad. Which is why defining clear objectives will prevent you from falling into a loop. There are assessment points within the chain that will aid you in considering if you need further objectives before progressing.
- **Strategic:** Strategic objectives are a set of objectives that are considered primary and vital to your success. These objectives cannot be bypassed. They should be achieved as required before progressing to the next phase and towards the final goal.

Remember, the Adaptive Strike Chain (ASC) is responsible for the identification, planning and the execution of the objectives of every phase. You are required to perform an assessment before proceeding further towards your goals. Assessment will aid you to review your progress and to reconsider further strikes, if necessary.

It also prevents you from falling into a loop. Below is a simple overview of the phases that this framework covers. These phases are a set of the rules that you should define for each phase of your operations. These are also considered the constitutional rules of the framework and cannot be bypassed. Arbiter if used properly, can bring down your adversary to heels.

Prerequisites
- Strong intelligence and verification network.
- Studying your enemy takes priority.
- Having a suitable deterrence option.
- Understand that unless all primary objectives in a phase of an operation are not completed successfully, you cannot proceed further. You cannot break the progressive framework and bypass objectives.
- Assessments should be objective and independent. Assessments are the guardian of your chain.
- Use of modern electronic operations and warfare is not only encouraged, it is recommended.
- No matter what, we are still governed by the principles of war. So, ensure you follow them in the operational planning and execution.

Guidelines
- **Define your finite goal:** Your ultimate goal should be finite. It means your goal should be achieved within a certain period of time and must be clear.
- **Study your adversary:** Perhaps I can say this is the most important part of any operation and not just this framework. Studying your adversary will give you the ability to plan your strikes effectively and to avoid chasing time-consuming and irrelevant objectives.
- **Information extraction and intelligence flow:** Intelligence is the key to all doors, never forget that.
- **Plan and execute your strikes:** Use the information you gathered and the study that you have performed on your adversary to plan and execute effective strikes and fulfill your objectives.
- **Assess your actions and objectives:** Assessment is equally important to the identification of your enemy. Not only does it help you to understand what your actions and strikes accomplished towards the finite goal. It also helps you to further analyze your adversary. As we have discussed it before, your adversary will show a certain behavior. You should understand these behaviors and re-evaluate your strategy if needed.
- **Proceed as needed:** Progress in the framework towards your finite goal depends on the outcome of the previous steps. If you have achieved your primary and secondary objectives and completed your assessment, then you are free to proceed to the next phase of your operation.

Adaptive Strike Chain (ASC)

A highly precise targeted, active and passive strike and counter-strike in order to slow down/ stop or force your adversary towards a certain outcome. These strikes are based on the conditions that you directly or indirectly are responsible for *via* the constant assessment and evaluation of the enemy's current condition in the active phase of the attack in order to plan and execute further adaptive and progressive plan of attack. There are three major possible outcomes to this.

Adaptive strike in arbiter means by crafting sophisticated and precision strikes it can be purely electronic; it can be purely conventional intelligence work, or just the mix of them in combination of the five domains. You create conditions that will the pre-requisite and precursor to your next follow-up strikes, and each strike will make your adversary weaker.

You are directing the fate of your adversary and if not all the majority of the precise incidents that will cause the adversary to weaken economically, scientifically, military, unwanted public exposures and exposes and etc. and lose control preferably without or with the limited knowledge of your responsibility. Ethically speaking without directly harming the general population, however, intelligence work is not always clean; sometimes drastic measures might be needed. In short you are the author and director of it all and in control of all that happens to your adversary in order to push your adversary towards a certain outcome that you have crafted.

If used properly, the adaptive strike chain has the ability to weaken or crush even the toughest and most sophisticated adversary.

You can achieve the goals by the effective use of the active and passive electronic operations with the combination of the five domains and effective use of the intelligence operations active, passive and decapitation by elimination. Take note that you can push your adversary in the direction that you desire. All it takes is good intelligence, strategical awareness, and proper planning.

Possible outcomes of the ASC
- **Domination:** An all-in military invasion towards the adversary. Adversary is weakened. The support is at its all-time low. Infrastructures are weakened and therefore the adversary's military capacity will be at its all-time low. Either the adversary will be unable to respond or simply the response is inadequate. But it must be considered that a desperate adversary is the most dangerous kind and sometimes their actions cannot be pragmatic, which is why studying your adversary is the most important phase in profiling and predicting the behavior and use their behavior to your advantage.
- **Golden bridge:** Your adversary has been weakened and reached to a point that cannot face you on the battlefield or oppose you. Now is the time to force a negotiation and dictate the terms.
- **Implosion of power:** This happens when the top echelons of your adversary (C5ISR) and the political leadership collide with each other and the inside battle for power begins. The higher the poverty and the corruption rate are within your adversary take note that you can cause this. Implosion of power can happen by the hand of people as well, but it's usually tougher to convince a great mass of people for such a change (Figure 8).
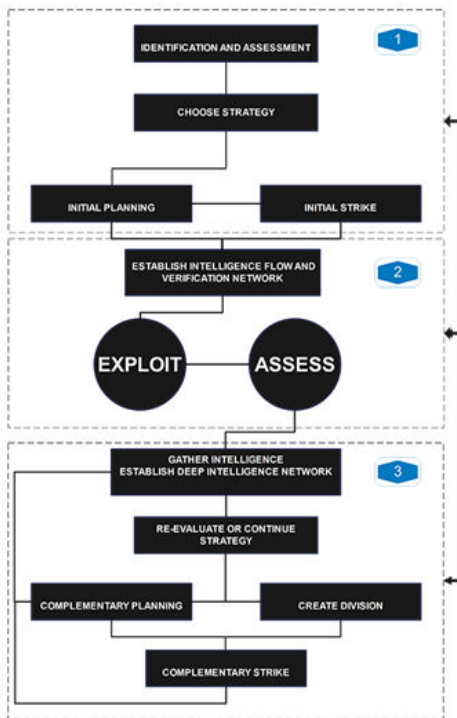
Figure 8: Overview of the adaptive strike chain redacted.

You are required to have your deterrence option ready or prepare it along the way electronic or conventional or both in order to maintain your superiority and being able to respond with the right amplitude if needed.

In each section you can return to the previous one in order to verify and create a more effective strike based on the new intelligence gathered. All of the steps are interconnected. Therefore, you can always revert and take a step back and assess, verify and gather new information that can help you make better decisions and prepare strikes and responses.

Every action and decision have a consequence; you can expect a stronger response during your early stages and when your adversary suffers and becomes desperate, which implies it's wise to have a proportional response as required. Having options doesn't mean you can use them sometimes silence is the best option.

It's a game of probability. If you strike your adversary correctly, expect less opposition and more courage to get an active response from your adversary. Your best option is to attempt and force an implosion of power. You must redesign and re-evaluate this chain according to your needs and standards. The effectiveness of this chain comes from the resiliency and importance of the intelligence flow in the decision making and operational planning nodes. One of the sections that you should pay special attention to is the damage assessment. As I have mentioned every action has its consequences. You must attempt to identify and predict your adversary's response in order to be able to defend yourself so you can proceed further. There are some ground rules to the chain which again can be adjusted according to your needs. Nothing is set in stones. One of the frameworks that you can use to evaluate your adversary is the "Anvil Evaluator" Part of the Nightshade-NOT released for public use. In short anvil is considered both a defensive and offensive framework for establishing a mathematical probabilistic state of events for the state of

power, effectivity and the ability to respond as an evaluation framework for yourself and your adversary according to the current state of affairs. Anvil is a comprehensive framework that enables you to assess the damage that has been done to you or your adversary based on hard facts and probabilistic state of events. Electronic operations permit you to have a wider range of targets and also empower your intelligence network to be more effective and secure. Intelligence is at the heart of modern operations. You must acknowledge this fact and invest in your intelligence gathering and verification network. If you don't, you will fight your enemy blindly while not being able to make the right decisions. A strong intelligence and counterintelligence network is the precursor to your success. Expect total collapse of abilities and failure if you don't have a strong intelligence and counterintelligence capability. You do not necessarily need to spend billions of dollars at once to create and maintain such a network. Creating an effective network is not always about spending and having a blank check budget.

Conclusions

- Identify your target and your objectives and define tactical and strategic goals. Gather data, create an active database of potential targets. Use the exploitation phase to enhance the database. "know your enemy as you know thyself, a thousand battles, a thousand victories-sun tzu" this is a never-ending process. Remember, your enemies evolve as you evolve. Study your target, study the history, culture, assets, infrastructure, social, and political factors. Identify vulnerabilities and critical infrastructure. Using the MASINT, ELINT, COMINT, SIGINT in order to gather intelligence and to identify the C5ISR so ultimately you can prepare precision strikes (C5ISR: Command and control, computers. Cyber intelligence and c ommunication/ISR: Intelligence, surveillance, reconnaissance).
- Plan your initial strike and choose your targets based on your objectives and maintain control.
- Exploit your targets, gain access, and maintain access to assets and infrastructure. Build a multi-layered intelligence gathering and verification network. As well as accessing and maintaining access to the critical infrastructures. Corrupt the leadership. Exploit the human elements to acquire new sensitive soft and hard targets. One of the great ways to enhance the effect and boost the effect of your strikes is to expose the mistakes of the system in a way that affects the general population and dismantles the trust mechanism that has been built over the years among them. Exposing these should be beneficial to your progress and you should gain a tactical advantage by them.
- Plan complementary strikes based on the assessment of the current developed state of the events. Update the target database based on the newly gathered data and execute.
- Create division among the political and military members and begin destabilization of the high echelons; let them take each other out; by doing so you will impose passive decapitation and you play a passive role in the scenario. Remember, you do not need to expose yourself; the less you are exposed the better. "Trusting the people is like building your castle on sand." Niccolò Machiavelli.
- Strike the critical infrastructure and tier 1 targets as needed. If you have done all the previous steps properly the system fails to respond accordingly and therefore it will lose the trust of the people and ultimately collapse either by itself or by the hands of the people it trusted.

References

1. Kim SY, Oh SY (2008) On-road vehicle detection and tracking based on road context and the ambient lighting adaptive framework. Int J Imaging Syst Technol 18:283-295.

2. Afolabi MO, Kelly LE (2022) Non-static framework for understanding adaptive designs: An ethical justification in paediatric trials. J Med Ethics 48:825-831.

3. Hu H, Wu J, Wang Z, Cheng G (2018) Mimic defense: A designed-in cybersecurity defense framework. IET Information security 12:226-237.

4. Werner M, Bair J, Fernandez VR (2014) Linking up to development? Global value chains and the making of a post-Washington consensus. Dev Change 45:1219-1247.

5. Beck S (2011) Moving beyond the linear model of expertise? IPCC and the test of adaptation. Reg Environ Change 11:297-306.

6. Williams I, Shearer H (2011) Appraising public value: Past, present and futures. Public Adm 89:1367-1384.

7. Gonzalez-Tosat C, Sadaba-Chalezquer C (2021) Digital intermediaries: More than new actors on a crowded media stage. J Media 2:77-99.

8. Orlitzky M (2017) How cognitive neuroscience informs a subjectivist-evolutionary explanation of business ethics. J Bus Ethics 144:717-732.

9. Peteraf MA, Bergen ME (2003) Scanning dynamic competitive landscapes: A market-based and resource based framework. Strateg Manag J 24:1027-1041.

10. McBride JR, Ivan JC, Rhode DS, Rupp JD, Rupp MY, et al. (2008) A perspective on emerging automotive safety applications, derived from lessons learned through participation in the DARPA grand challenges. J Field Robot 25:808-840.

11. Gupta M, Kumar R, Shekhar S, Sharma B, Patel RB, et al. (2022) Game theory-based authentication framework to secure internet of vehicles with block chain. Sensors 22:5119.