Ignacio Pizarro

DOI:10.33179/BSV.99.SVI.11.CMC.24.2.5

UČENJE NA PODLAGI IZKUŠENJ: STARE LEKCIJE ZA NOVO BOJIŠČE

LEARNING FROM EXPERIENCE: OLD LESSONS FOR A NEW BATTLEFIELD

Povzetek Uvajanje kibernetske domene in zmogljivosti v večdomenske operacije so zaznamovale težave, od katerih so mnoge posledica napačnega razumevanja narave te domene kot tehničnega področja, ločeno od običajnega razumevanja bojnega delovanja. Voditelji so zato domeno previdno naslavljali, kar je povzročilo zamudo pri prilagajanju vojaškega razmišljanja novemu okolju. V prispevku poskušamo opozoriti na pomanjkljivosti in morebitne vzroke za zapozneli pristop ter izpostaviti področja, na katerih je uveljavljeno vojaško znanje, in veljavno doktrino. Za spoprijemanje z izzivom, kako kibernetske zmogljivosti kar najbolje uporabiti v vojaških operacijah, je mogoče uporabiti celo stara načela.

Ključne besede ***Kibernetski prostor, operacije, vojska, doktrina.***

Abstract The implementation of the cyberspace domain and capabilities into multi-domain operations has been plagued with difficulties, many of which come from a misperception of the nature of this domain as a technical field, detached from the usual understanding of combat operations. This has made leaders wary of addressing this domain, which has caused a delay in the adaptation of our military thinking to this new environment. In the article, we seek to point out the shortcomings and possible reasons for this delayed approach, and highlight areas in which established military knowledge, existing doctrine and even ancient principles can be used to meet the challenge of bringing cyber capabilities to their full potential in military operations.

Key words ***Cyberspace, operations, military, doctrine.***

Introduction

Military operations in cyberspace, even after more than a full decade since they first made their way into the mainstream media headlines, do not seem to have yet made their way so successfully into the mindset of military planners, decision-makers and commanders. Although cyberspace has been recognized as a separate domain of operations (NATO, 2016), it is still treated as a kind of private realm of technical experts, constrained somehow within the field of communications and information systems, and handled, and possibly understood, only by Information Technologies (IT) specialists. This creates a gap in our military understanding that needs to be addressed at all levels and during all phases of conception and planning of military operations. It is understood by many experts that military cyberspace operations, and addressing the cyber threat, still require an improvement in our conceptual and doctrinal thinking (Brantly & Smeets, 2020, p 2).

This initial understanding of cyberspace as a somehow separate and fundamentally different field, which may not even merit equal footing with all other areas of military thought, has made our response to this new environment slower than it has been in the past to other emerging threats and opportunities. Even though much has been said and written about cyberspace operations, both conceptually and practically, on their military applications, parts of this field are still considered by many to be in their infancy (Brantly & Smeets, 2020, pp 12-13).

In modern times the threat cycle for any emerging form of warfare has been consistently shown to take about a decade. This means the time between the appearance of a new kind of military threat, its understanding, its implementation into military doctrine, organization, materials and procedures and the subsequent appearance of the next emerging threat requiring a new change, has taken approximately a decade every time. For many reasons, which we will not attempt to unveil in this article, it takes military planners, organizers, and decision-makers about ten years to become aware of a new problem, understand it, devise ways to address it, and implement the solutions into military thinking, doctrine, organization, and materials. This is usually the point at which adversaries, having lost the advantage provided by the novel approach, move on to a new way of fighting to exploit different weaknesses, whether new or old.

The 1970s were the age of indirect strategy, with the main power blocks unable to confront each other directly for fear of apocalyptic consequences (Van Creveld, 1991), and resorting to battles in proxy conflicts through proxy nations to achieve their political goals. The 1980s were dominated by a revival of conventional warfare theory (Van Creveld, 2000, p 171), with the global bipolar landscape and the nuclear threat still as its backdrop, and a covert economic battle defining its final strategic outcome. The 1990s were the decade of large-scale tactical operations, of the overwhelming dominance of air power as the decisive factor of conventional battles, once the fear of nuclear escalation no longer put a stop to the deployment of a large military force. The 2000s brought the rise of Asymmetric Warfare[1] to the forefront, with armies rushing to adapt their organization, tactics and materials to this way of fighting which exploited their weaknesses and negated the strengths (Field, 2009, p 4) of the massive military forces of the previous decade. Finally, the 2010s saw the appearance of Cyber Warfare (Denning, 2012), with all its new challenges and opportunities, as well as threats of a nature and scope that we struggled to fully comprehend.

We find ourselves now in the 2020s already fully under the shadow of the Hybrid Warfare threat (Gvineria, 2017). We are addressing the new challenge of waging a war that takes place at the same time in the field of battle and in the information and cognitive landscape of the general population, and we may yet even see a return to the power dynamics and polarities reminiscent of the Cold War.

We might say we have already begun the next threat cycle, and yet we still have not fully implemented and addressed the decade-old cyber threat, which should by now be part of the last successful cycle of change in military thinking. We are late in our implementation of solutions, while our dependence on this domain has only grown.

Part of the reason for our delayed response to the cyber threat is that cyberspace seems to be a fundamentally different theatre of operations, requiring a fundamentally different way of thinking. It is not just a new way to fight, but a new space to fight in. In this sense we could equate it with the emergence of air power a century ago (Van Creveld, 2011). Military leaders of the past had as much trouble understanding air operations, and the challenges and opportunities they could bring, as modern planners have with cyberspace operations. It is a new space, with new rules, and our intuition does not always appear to give us the right answers.

However, we would be wise to notice that the same has been said before of many new weapons and methods. Many technological advances have been hailed as fundamental changes in war, and yet we find that war does not change that much in its essence. Technology brings new ways to fight the same battles, for roughly the same motives. Technology may advance but human nature remains, and the nature and purpose of armed conflict is no different now from what it has been in the past. As Carl Von Clausewitz said *»The need to fight quickly led man to invent appropriate devices to gain advantages in combat, and these brought about great changes in the forms of fighting. Still, no matter how it is constituted, the concept of fighting remains unchanged. That is what we mean by war«* (Clausewitz, 2007). Therefore, when confronted with a new problem, it would be wise to look back to the brilliant military minds who preceded us and take counsel from their experience.

[1] *Asymmetric warfare is a form of warfare between opposing forces which differ greatly in military power and that typically involves the use of unconventional weapons and tactics (such as those associated with guerrilla warfare and terrorist attacks) (Merriam-Webster Inc., n.d.).*

This is why we can look into this challenge from the perspective of many well-established and even ancient principles and lessons that may help to dispel the image of cyberspace as a mysterious domain, in which everything must be learned again. By rejecting the assumption that the problem is completely new we may find ways in which our current military knowledge applies to the threat at hand, and solutions that could have been implemented by now and would probably have been implemented if cyberspace did not have an aura of mystery. We will attempt to point out some classic approaches that may be taken to help to close those gaps in our doctrine and move on to the next threat.

1 THE SCOPE OF THE CHALLENGE

First, let us define the scope of what we will be addressing. For the purposes of this article, we will be discussing the role of cyberspace in the context of military operations. That is, we will be discussing cyberspace as a domain of operations, with military forces in cyberspace deploying and operating alongside conventional forces. We will discuss cyberspace as an integral part of military operations (CCDCOE, 2020, p 12) in a theatre that may encompass many and possibly all domains, from land, sea, and air forces to every potential instrument of military power.

The most frequently discussed form of the cyberspace threat in public forums tends to be, instead of multi-domain military operations, cyber warfare. This usually also means the hostile use of cyberspace, but it tends to refer to actions taken outside a conventional battlefield. Cyber warfare can happen, and often does, below the threshold of armed conflict. It exploits grey areas in legislation and often takes advantage of the difficulties of attribution (CCDCOE, 2020, p 21). This use of cyberspace is, of course, a constant concern, since it happens during peacetime and is not limited to an active armed conflict. Nevertheless, since the scope of this form of cyber threat is addressed by institutions far beyond the military, and it does not necessarily relate to military operations, it will not be the subject of our study this time. We, as military experts, are concerned mainly with the needs of military organizations that are still struggling with the challenge of incorporating cyberspace into their operations.

The first challenge of incorporating cyberspace into classic military thinking is that its nature, and the nature of actions within it, are fundamentally different from any other classic military action. Even the most technical disciplines employed in warfare share fewer similarities with the kind of actions carried out in this domain than one may think at first glance. Even though cyberspace operations overlap in many ways with other operational domains, the weapons and procedures used in cyberspace are unlike anything that has been used in the past. They are tailored, after all, to affect an environment that did not even exist not so long ago.

Cyberspace operations take place in a completely artificial domain (NATO, 2020, p 13), unlike any other operation in military history, and it would appear at first that this makes them different from any other kind of operation ever conceived in all aspects. As we will see, this may not be the most realistic approach. Our analysis should start, nevertheless, by addressing the fundamental differences between cyber warfare and conventional operations, and how these differences condition the way in which modern nations address the building of capabilities and the incorporation of this domain into their planning.

Cyberspace has many noticeable and frequently pointed out differences from the traditional domains of operations, although not all of them are equally relevant to the problem at hand. It would be redundant at this point to highlight the anonymity cyberspace allows its actors (NATO, 2020, p 13), the proportion of non-state actors (NATO, 2020, p 5; CCDCOE, 2020, p 22) operating in it, or the legal void that tends to accompany the reaction to the threats and the conduction of operations in this domain. All these characteristics were already present in Asymmetric Warfare, and they hardly constitute new challenges. Nations are already experienced in dealing with these aspects of the problem, and these lessons are recent enough not to have been forgotten (NATO, 2017, p 2-13).

One fundamental challenge of cyberspace which may help us understand our own slow response to the threat in this domain is the subtle nature of its effects. The threats our military forces have addressed in the past have all been highly visible, if not in practice at least potentially. Even nuclear weapons, whose use was always uncertain to the point it never materialized into a nuclear attack during the Cold War, had potential catastrophic effects that were painfully understood by all the actors involved (Van Creveld, 1991, p 16).

The cyber threat, in contrast, presents us with levels of uncertainty comparable to the Cold War, while at the same time remaining unclear and covert in its effects. The possible consequences of a cyberattack range all the way from a mere nuisance to a full collapse of command and control or critical infrastructure, and the perception of this threat suffers from this undefined magnitude of the consequences. In the last decade, military forces have known about the cyber threat at an intellectual level but have not felt vulnerable to it at the emotional level that drives truly world-changing efforts. A cyberattack may well neutralize a military operation, but it may do so in a way that is not immediately visible (CCDCOE, 2020, p 20), and that does not cause direct loss of life.

This signals the first problem of addressing cyberspace as a domain of operations. It is not a visible enough threat to be frightening, except to the experts. It places cyberspace operations, once again, only in the minds of technicians, who are rarely the ones defining policy or doctrine. The decision-makers do not feel the urgency of a threat that is not visible, and whose consequences cannot be clearly assessed, for all the efforts of the experts to warn them. It is a threat that thrives in the shadows and takes full advantage of its obscurity to remain seen as a potential threat, more than an actual one, until it is too late.

The second fundamental difference that makes cyberspace operations difficult to conceive in classic military thinking is the nature of time and space in these operations. Military commanders throughout history have understood space and time clearly. Time is a critical resource in military operations. Space is where these operations take place. All actions in a battlefield have a defined place in space as well as a known cost in time (Clausewitz, 2007, p 52). Commanders understand how long it takes for a force to move, for an attack to take place, for a weapon to reach its target depending on distance and speed. In classic warfare space and time are inextricably linked. Distance needs time to cover it. Space can even be exchanged for time when the need arises (US Army, 2012, p 13).

Cyberspace changes this known nature of space and time in the battlefield. In cyberspace, actions that used to take significant time are executed instantaneously, and distances may become meaningless (CCDCOE, 2020, pp 16-17). Distances in cyberspace are not measured in length, and are sometimes not measurable in any tangible way. Defensive lines deployed in physical space are mostly inconsequential, and enemy actions avoid classic defences and seek the least defended points from which to reach key terrain. This makes the proximity of the threat much harder to assess, and it forces commanders to think about risk in an unfamiliar way. It is easy for the threat to be perceived as closer, or far more distant, than it is. A threat whose proximity cannot be easily established is uncomfortable to any military mind. A good commander will notice this discomfort and never look away from it. Discomfort is an instinctive indicator that our position is vulnerable, and that is where a commander’s attention should focus. Unfortunately, human nature tends to do the opposite, and look away from that which causes discomfort. Looking away from a threat may provide some momentary emotional relief, but it certainly does not make it go away.

Still dealing with the subject of time, and specifically the tempo of cyberspace operations, another peculiarity arises. As quick as the execution of an action in cyberspace can be, its preparation is often the very opposite (CCDCOE, 2020, p 17). Once again, the nature of time in this domain veers away from the familiar and into uncharted territory. Preparing an action in cyberspace may require weeks, months or even years of manoeuvring. It often requires massive amounts of information that needs to be gathered, processed, and employed to drive the next steps. It requires layers in defences to be peeled away, lateral movements to be completed and assets prepositioned. The moment when, at the press of a button, a cyberattack commences, is the final step of a complex campaign that has been running in the shadows and has crossed vast distances to reach its objective, however virtual and indefinable those distances may be. In this respect, cyberspace operations resemble guerrilla warfare (US. Marine Corps, 1990), in which preparation and even most of the actions are covert if executed properly, and only the final step is detectable by the opponent. In fact, its very success depends on this.

Now that we have examined the nature of the cyberspace battlefield in some detail, and looked past the technical details that often obfuscate its understanding, we cannot possibly think these concepts of uncertainty, subterfuge, covert manoeuvring seeking the weakest defences, and long preparations before the fight breaks out are new. Once stated in these terms we cannot help noticing they take a very familiar shape. There is a long-established school of military thought in which action is swift, preparation is meticulous, covert manoeuvring is the norm, the enemy may be close or far without our knowledge, and attacks avoid the strong and well defended points to focus on the weaknesses. A school of military thought based on deception, subterfuge, calculation, and patience. This school of thought dates back 25 centuries and its most known proponent, who in fairness we must point out may or may not have been a real historical figure, was Sun Tzu[2].

This is a character, and a school of thought, that need no introduction. He is by no means the only voice of wisdom we will quote, but his work has the advantage of being particularly well suited to cyberspace operations, as well as an easy read and an accessible way of thinking despite its antiquity. His school of thought is well known, based on timeless principles, and taught even outside the military. That is why we can easily refer to his teachings, so far back in time, to explore the solutions to the problems of such a modern concept as cyberspace operations. We will look at the ways in which many of the problems we face today are no different from the challenges others faced in the past, and how we can look at the past to solve them.

2 BEFORE THE BATTLE: PLANNING FOR WAR

Sun Tzu said: *»Now the general who wins a battle makes many calculations in his temple before the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose.«* (Sun Tzu, 1910, p 5)

This old principle of meticulous planning and preparation before battle is not only still valid today, but even more prominent than ever in the battle over the cyberspace domain.

No one can deny that cyberspace operations are complex and require long preparation times, and yet current planning methods for military operations contend with time constraints that clash with this requirement, and often make it impractical for an operation to be supported in a timely manner from the cyberspace domain.

In the classic battlefields of the European theatre during the Cold War, detailed military planning was carried out meticulously during peacetime (Ambrose, et al., 2006). Scenarios were considered and forces were allocated for a confrontation in which the potential adversary was known, and the terrain in which the battle would

[2] *Sun Tzu (孫子) was a Chinese general who allegedly lived between 544 BCE and 496 BCE. He is traditionally credited for the influential work of military strategy »The Art of War«.*

be fought could be predicted. Whether these plans were realistic or not, and even if the battle would be fought, turned out to be secondary to whether the plans were in place, since none of these plans were ever carried out, to the relief of the entire planet. The calculations ensured, however, that all elements of the combat forces would be prepared, equipped, and trained for their task, and this in turn constituted a deterrent against aggression. No doubt the plans would be leaked, and enemies would know each other's script. This planning and positioning of forces were as much posturing as they were preparation, but had the battle been fought, these preparations would have allowed operations of a complexity and magnitude that a reactive approach could not have achieved in time.

This principle of meticulous preparation in a known battlefield became mostly obsolete in Western military thinking after the fall of the Soviet Union. Forces have become expeditionary, expected to respond to situations at short notice, in uncertain and distant battlefields, and against unpredictable enemies. To their credit, Western military planners have successfully adapted to this requirement and changed their methods for planning military operations (NATO, 2021) and the materials used to conduct them. In doing so they have gained new capabilities, but they also may have lost sight of some of the lessons of the past.

Dazzled by our own success in this war of projection and flexibility, we may have failed to realize that cyberspace is not necessarily an expeditionary battlefield. It is not an unknown place that requires distant deployment or long logistic tethers, even if the rest of our forces are still in that situation. Distances in cyberspace are irrelevant, and most of our deployment does not take place in a physical space, as we pointed out before. The battlefield in which this conflict is going to be fought may be dynamic and constantly changing, but its location is not undetermined. This could allow us to return to some of the quasi-deterministic military thought of the past, when generals studied a battlefield and started planning around it before war broke out. No matter where our forces may be deployed, the cyberspace domain for the battle is bound to be almost identical in many aspects. The systems deployed will be the same regardless of location, their connections will follow the same protocols, and even our enemy is unlikely to use technologies or methods that are fundamentally different from anything we have encountered, or even from the technologies we use ourselves. In the cyberspace domain our generals know where the battle will be fought, and they can plan for it long before the war begins. The calculations for battle can begin today, and they probably should have begun yesterday.

Since much of the planning can be undertaken in advance, we should ask ourselves if the same is true of the deployment. Unlike land, sea, or air forces, which cannot plan their operations, much less deploy their forces, until they know which war they will be fighting (NATO, 2021), cyber forces can and should already be deploying in peacetime. Cyber soldiers know where they will fight, and for the most part they also know what kind of enemy they will be fighting and with what weapons. They are ready to take positions for battle, but they often do not. They may fail to deploy to their full potential because they are being held back by a shackle of doctrine and procedures that ties them to conventional forces. No force can begin deployment until an operation is declared, which is valid for conventional forces, but not necessarily so for cyber forces. The sooner we realize that restriction has no reason to exist besides tradition, the sooner we can begin our deployment in a way, it must be said, that our enemies are already doing.

Let it be said this does not mean deploying cyber forces in enemy territory during peacetime. As tempting as this may be, and even convenient from an operational point of view, it is not a freedom of action any law-abiding state can enjoy (CCDCOE, 2017). We have already learned, in the decade of adaptation to asymmetric warfare, that there are methods and practices available to our adversaries that will never be available to us, and that should not be imitated without risking the compromise of the very society we intend to defend. Imitation of the adversary is a natural but dangerous consequence of any prolonged human conflict. »War is an imitative and reciprocal activity. In order to defeat an enemy in a long war one becomes more and more like him, and both sides end up feeding off the other« (Smith, 2005, p 60). Since this limitation is a legal and sociological matter, we should leave it to the legal experts to study in detail. For the moment it should suffice to say that our military deployment will probably be limited to the areas of cyberspace we already control, and any deployment within enemy territory must be planned but cannot be executed in the context of a military operation until the Rules of Engagement allow it. This will be necessarily late in crisis response planning, and not before the operational planning process has already been initiated.

This restriction places a constraint on our preparations that, once again, can make any commander feel uncomfortable. We must listen to this discomfort, as it indicates a weakness in our position that needs to be addressed, not by looking away from the discomfort and abandoning this preparation, but by realizing how much more exhaustive it must be, so that deployment, when finally authorized, can be swift.

This is no different in essence from the way a battlefield is prepared when battle lines have been drawn and positions defined, but the order to advance has not yet been given. In this respect cyberspace operations resemble the battlefield preparations common in World War II. We can, then, draw lessons from this conflict and realize that, although the battlefield is determined and the weapons are known, the actions of the enemy cannot be predicted. The only predictable action from an enemy is that they will attack – *»The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him«* (Sun Tzu, 1910, p 29) – but not where or when this attack will come. In cyberspace, just as in the physical battlefield, we do not want to establish a Maginot line only to see it outflanked by a clever enemy[3].

[3] *The Maginot Line was a series of heavy defensive fortifications established by France with the purpose of stopping a potential German offensive into French territory. It was outflanked and avoided altogether by the German Army by advancing through the Ardennes Forest on May 10th 1940.*

So, if World War II taught us that static defensive lines are unreliable, even when the battlefield is already determined, the preparation of this battlefield must follow a different pattern. This pattern can also come from past experience and established doctrine. When the battlefield is known, but a static operation is unwise or unfeasible, the response is a mobile defence and a flexible offensive force. In cyberspace this translates into the ability to react, to respond and to counter. Our battlespace must be prepared, not to be unassailable, but to allow swift defence in depth. Our friendly cyberspace battlefield must be tailored to allow our cyberspace operations full and rapid access to it, rather than on putting our trust in a single perimeter defence that any clever enemy will seek to outflank. »Military tactics are like unto water; for water in its natural course runs away from high places and hastens downwards. So in war, the way is to avoid what is strong and to strike at what is weak« (Sun Tzu, 1910, p 21).

Sun Tzu also said: *»Whether the object be to crush an army, to storm a city, or to assassinate an individual, it is always necessary to begin by finding out the names of the attendants, the aides-de-camp, and door-keepers and sentries of the general in command«* (Sun Tzu, 1910, p 55).

If preparations can be made during peacetime for defensive operations, the same can be said for Cyberspace Intelligence, Surveillance and Reconnaissance (ISR) operations. Non-intrusive collection[4] can and should be employed during peacetime to gather not only threat information, but also potential target information, vulnerabilities, user profiles and identities required to breach potential objectives, system specifications and attack surfaces. This information requires a substantial time to collect and process, which means that the deployment of this capability will follow the same principles of peacetime deployment and peacetime full activity, parallel to Cold War defensive doctrine, as Defensive Cyberspace Operations. As for Intrusive Collection[5], it will follow an approach not unlike Offensive Cyberspace Operations, which we will deal with next.

Our offensive cyber forces, as much as we wish they could follow the same principle of early deployment, will probably not be able to preposition forces inside enemy space. As we have already pointed out, these methods are at best questionable and at worst illegal for a law-abiding state. This means the slow and elaborate pattern of infiltration followed frequently by Advanced Persistent Threats (APT)[6] to

[4] *Collection methods that draw from own networks or open source intelligence on adversary and third-party networks (CCDCOE, 2020, p 33).*

[5] *Collection methods that draw from non-available, third party networks including adversary networks (CCDCOE, 2020, p 33).*

[6] *An APT, or Advanced Persistent Threat, is an adversary which possesses sophisticated levels of expertise and significant resources, allowing it to create opportunities to achieve its objectives by using multiple attack vectors (e.g. cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The Advanced Persistent Threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives (U.S. Department of Commerce, 2011).*

devastating effect may not be available to our forces, even though it is favoured by our adversaries.

Instead, our forces in cyberspace may not need to prioritize their offensive preparations to be overwhelming, but to be fast and able to occupy enemy space and make advances as the opportunity presents itself. In this, Sun Tzu's statement *»If the enemy leaves a door open, you must rush in«* (Sun Tzu, 1910, p 48) fully applies, but can only be implemented if your forces are built and capable to fulfil this very task in time. In cyberspace, as a law-abiding nation, we cannot count on an early deployment in enemy cyberspace, so we must be capable instead of a rapid one. In this operational domain, this means having the ability to compromise, carry out infiltration and perform lateral movement in enemy systems at relatively short notice. Since this will not always be feasible, a military force in cyberspace also needs to be prepared to carry out faster and less target-specific offensive actions in cyberspace, such as Denial of Service attacks. All these capabilities, even the least specific ones, will require extensive preparations long before an operation is declared. Just like in the days of the Cold War, attack plans must be drawn, and potential targets designated and reviewed periodically to keep them current, as a peacetime task.

3 PREPARING FOR BATTLE: DEPLOYING FORCES IN CYBERSPACE

Sun Tzu said: *»Whoever is first in the field and awaits the coming of the enemy, will be fresh for the fight; whoever is second in the field and has to hasten to battle will arrive exhausted«* (Sun Tzu, 1910, p 18).

Once a military operation has been declared, an arduous process begins in order to constitute a suitable force, integrate that force, deploy it, and sustain it to carry out the operation. This is a process that becomes more time-consuming and costly the longer the distance is to the area of operations. As we have pointed out before, space equals time in conventional operations. This factor behaves quite differently in cyberspace, where distance to the area of operations is a virtual metric, often independent of geography.

This drives us to an immediate conclusion, which we have already hinted at when discussing preparation of the battlefield in friendly territory. Since cyber forces are not constrained by some of the limitations of conventional forces, this alters the tempo of their deployment to the point that it will not match the tempo of the rest of the components of a Joint Force. Cyberspace offensive forces may take a long time to seize an objective and gain control of it (McGhee, 2016, p 61), but they can commence deployment immediately, without waiting for other forces to be in place. Whether this is an advantage or a challenge to be addressed depends on how we think about it.

As new as this situation may seem when we label it as »cyber«, it is most certainly not a new concept. Armies have dealt with the challenge of different deployment times and different speeds of manoeuvring since the tribes of Asia began training horses to pull war chariots – an innovation with consequences that would reach, we could even say, biblical proportions[7]. If the situation is as old as civilization, it stands to reason that the procedure to address it does not need to be new. Where should we look in time for a force that can begin deploying ahead of the main force, must do so covertly, takes time to be in position to gather information or strike a target, and keeps a low profile until a visible effect on a high-value objective is required from it? Stated in these terms, the answer is obvious. This is exactly what Special Operations elements have always done (NATO, 2013, p 1.5.1), and even if their formal existence under this name in military doctrine is recent, the concept of small agile elements deploying ahead of the main force and even behind enemy lines is ancient. Thus, we can look at our own Special Operations doctrine (NATO, 2013) to understand how the preparation of our Offensive and Intrusive Collection cyberspace operations must be carried out. Instead of looking at this capability as a purely technical element, we may want to draw parallels with the Special Operations capability it resembles. Once this is understood, the deployment requirements, already detailed in this doctrine, become much more familiar to the Commander. These commonalities also explain why offensive cyberspace operations and special operations training sometimes converge to the point of sharing exercises[8] in which no other deployed forces participate.

Defensive cyber forces deploy in a different manner, since they do not share the need to position themselves behind enemy lines, but they are not completely detached from this concept of forward deployment. As we have stated before, defensive forces and Non-Intrusive Collection capabilities must already be deployed and prepared for action in the Joint Force's own cyberspace even during peacetime. Not only deployed, but actively engaged in defensive cyberspace operations[9] and in Cyberspace ISR activities. Nevertheless, defensive and ISR cyberspace operations often need to encompass systems that are beyond the military area of responsibility. Conventional forces need to secure the critical infrastructure employed for a military operation, whether this infrastructure is military or not. Airports, port facilities, railways and water supply systems may not be military forces, but no modern military force will deploy and sustain an operation without them. If these assets can be attacked through cyberspace, cyberspace operations are needed to secure them as well. That this is

[7] *»And the Lord was with Judah; and he drave out the inhabitants of the mountain; but could not drive out the inhabitants of the valley, because they had chariots of iron« (King James Bible, 1796/2022, Judges 1:19).*

[8] *An excellent example of this is Exercise Crossed Swords, carried out every year by the NATO Cooperative Cyber Defence Centre of Excellence, in which special operations elements train together with offensive cyberspace teams.*

[9] *In this respect we are using a general concept of Defensive Cyberspace Operations (NATO, 2020, p 16), which includes all defensive actions and preventive measures even in the absence of an adversary Offensive Cyberspace Operation. We will not be referring to allied military doctrines in which a defensive operation in cyberspace is specific in time and scope and declared in response to a specific enemy offensive operation (U.S. Army War College, 2020). These can be considered a subset of the operations we refer to.*

the case is not in question. Cyberspace can indeed reach many places and be used to strike at many major assets. It is not just a space, but also a space that allows access to other key spaces. In this respect, cyberspace is what Sun Tzu called the »Ground of Intersecting Highways«[10], so once again we can look at his writings for how to occupy such ground.

Sun Tzu said: *»On ground of intersecting highways, I would consolidate my alliances«* (Sun Tzu, 1910, p 46).

Many of the critical assets an operation requires, which do not fall under the commander's authority, will belong to a host nation that may be undetermined until a crisis breaks out. This precludes the deployment of defensive forces in this vital cyberspace during peacetime, but it hopefully does not prevent the preparation and planning of this movement. Agreements and liaison with friendly nations can be established during peacetime, and a potential deployment of cyberspace defensive and ISR capabilities can be part of any defensive agreement. Building trust and mutual knowledge with potential allies is a slow process, but it will be the key to rapid deployment once operations begin. The preparation of this deployment, thus, begins in peacetime even if the deployment will not take place until the crisis begins.

There is one notable exception to this constraint when allied nations share a strong enough mutual interest to allow the deployment of friendly forces in their own cyberspace, providing mutual support and a close observation of the activities of potential adversaries. This is nowadays known as the Defence Forward concept, a conceptual descendant of the Cold War »Forward Defence« strategy (Chourchoulis, 2015), and its potential for gaining an early foothold in this domain prior to military operations cannot be stressed enough. Any deployment of defensive and intelligence assets made during peacetime, before any open opposition exists, will be far less taxing on our forces and far more efficient[11]. It is not unlike the classic concept of prepositioning forces in friendly territory, but it takes full advantage of the low profile of cyberspace activities. Positioning conventional forces in the vicinity of a potential adversary almost always risks escalation, which is why this is usually done with the greatest caution and is the subject of serious diplomacy. Cyberspace defensive forces, on the other hand, lack the visibility and threatening presence that would contribute to escalation, and can be deployed with no other requirement than the consent of the allied partner. Whenever this consent can be gained, this early deployment merits serious consideration.

If we respect these ancient principles, and translate them into our doctrine, we will find our forces at the beginning of an operation in three different stages of deployment. In the cyberspace composed of military systems under the control of the Force

[10] *»Ground which forms the key to three contiguous states, so that he who occupies it first has most of the Empire at his command, is a ground of intersecting highways« (Sun Tzu, 1910, p 41).*

[11] *»An army may march great distances without distress, if it marches through country where the enemy is not« (Sun Tzu, 1910).*

Commander, all defensive and intelligence collection cyberspace assets should have been deployed almost fully during peacetime. Any final preparations in this terrain should be mostly concerned with the coordination of efforts from different nations, their liaison, and the building of situational awareness.

Deployment of defensive and ISR forces in the areas of cyberspace which, however friendly and necessary for the conduction of Operations, are not areas under the authority of the Force Commander, should have been planned and prepared as much as possible in peacetime. This deployment may even have commenced before operations if the nation where this deployment takes place is a close ally. This deployment, unconstrained by the needs of conventional assets, can and should take place once a military intervention is authorized, and may begin before any conventional forces deploy.

Of all the cyber forces, offensive forces and intrusive ISR capabilities will probably be in the least complete state of deployment, despite a commander's wishes. Preparations will have been made, and capabilities should be ready, but deployment may not commence until the authorization is received and the Rules of Engagement are in place. As we have mentioned, this would put them on par with Special Operations elements but, unlike these elements, offensive capabilities may be less constrained by distance and support. Our cyber forces should be prepared to be the first elements of our force to enter enemy territory.

5 THE CYBERSPACE BATTLE: INTEGRATING MILITARY OPERATIONS

Sun Tzu said: *»The clever combatant looks to the effect of combined energy, and does not require too much from individuals. Hence his ability to pick out the right men and utilize combined energy«* (Sun Tzu, 1910, p 17).

With deployment underway at whatever pace the circumstances allow, and operations commencing, the commander now faces one of the most difficult challenges of cyberspace operations: integrating this space into the battlefield and translating its capabilities into an operational advantage. Let us remember we are not discussing the kind of cyber warfare that happens below the threshold of armed conflict. We are framing cyberspace in the context of the full complexity, chaos, and violence of a conventional military operation. It has been our experience that commanders lack the familiarity to integrate cyberspace capabilities once they share the battlefield with more conventional means, with which they are far better acquainted. How, then, can we find the right place for a capability that even the experts sometimes struggle to grasp?

We shall be fair and point out that defensive capabilities do not appear to be particularly challenging in this regard. They often overlap with common security and protection measures, which commanders are already accustomed to. Even when these defensive capabilities are mistaken for communications and information security measures, they are not unfamiliar.

The difficulties of integrating cyberspace operations of any kind into the flow of the battle come mainly from the obscure and often poorly understood technical nature of their actions, their effects and their requirements. To dispel this veil of mystery we will once again attempt to find similarities with established doctrine and familiar capabilities, to find the doctrinal space that fits cyberspace operations, if not perfectly, at least in ways that make the leap from the old way of thinking into the new easier.

As it turns out, this place is not so hard to find once we outline the capabilities and constraints of our force. Cyberspace operations have the capability of reaching targets covertly, striking unexpectedly, and causing minimum or no physical effects, limiting collateral damage. These capabilities also constitute their own limitations. Cyberspace effects in the physical space are often reduced, and their covert nature is as much a requirement as it is an ability. These two characteristics also make battle damage assessment challenging, both for the attacker and for the target (CCDCOE, 2020, p 20).

With regard to defensive operations, we find that the security of friendly cyberspace often depends as much on the end user and the implementation of proper procedures than on technological solutions and centralized action. Centralized monitoring of the space is key to its security, but decentralized execution of preventive measures is the norm (CCDCOE, 2020, pp 32-33).

Cyberspace ISR also works on distant targets and has access to information not available through other means. This information can be of high value and provide deep insights into the enemy's situation, plans and intentions, as long as the sources and methods of collection are kept as closely guarded as possible[12].

As we keep listing the characteristics of this capability, they begin to take another familiar shape. In our operations we already find ourselves trying to employ a capability with few or no physical destructive effects, that can act at a distance and whose effects on the target are sometimes uncertain, often hard to evaluate and may not be permanent. A capability that, when planned defensively, depends heavily on procedure and decentralized execution, and that has the potential to obtain reliable information from sources not available to other means. A capability that, interestingly, often also gets confused or mixed with Communications and Information Systems (CIS) (CCDCOE, 2020, p 19).

This capability may not be as ancient as most examples we have used so far, but it is no less familiar. All these traits, limitations and even mistakes in its implementation closely resemble the characteristics of Electronic Warfare (EW) (NATO, 2020).

[12] *»O divine art of subtlety and secrecy! Through you we learn to be invisible, through you inaudible; and hence we can hold the enemy's fate in our hands« (Sun Tzu, 1910).*

Note that we say it *resembles* Electronic Warfare, not that the capabilities are equivalent. This is a source of confusion that we should dispel before we go any further. Electronic Warfare deals with the use of electromagnetic energy (US Joint Chiefs of Staff, 2020, pp I-5), and its methods and equipment are fundamentally different from cyberspace operations, which deal with the logical layer of systems (CCDCOE, 2020, p 13), regardless of whether they employ electromagnetic energy or not. The procedures, equipment and skills used to carry out their actions are completely different from each other, even if the targets sometimes overlap.

Their similarities, nevertheless, will help us understand the role of cyberspace operations in the battlefield and how to employ them to maximum effect. Like Electronic Warfare measures, the greatest value of cyberspace operations comes from their ability to cause and prevent effects in support of the Joint Operation and the forces in it.

Like an EW action on a critical system, a cyberspace effect in isolation can be damaging, but it could amount to no more than a disruption, and possibly a nuisance. Military forces are trained, equipped and ready to handle temporary failures in their critical systems as a matter of routine business continuity. It is when these effects are combined with manoeuvre and kinetic effects that they will reach their full potential.

The main principle for employing offensive cyberspace capabilities will be, then, the combination and synchronization of efforts. Every offensive action must have a specific effect to create in the battlefield, a specific time at which to create this effect, and a specific operational purpose for it, linked to the other operational activities and coordinated. Just like Electronic Countermeasures, the use of cyberspace effects loses much of its effectiveness after the first use (McGhee, 2016, p 57), and also risks the loss of information from the target system from that point on if it was under surveillance. This means the employment of these capabilities, even in cases where it may seem safe and of low cost, must always have a clear and coordinated operational purpose. The ancient principle »Do not do anything for which there is no purpose« (Musashi, 2011) applies.

This might lead us to believe that cyberspace offensive capabilities are a tool to be held back, kept in reserve, and employed only in rare occasions. Although it is true that the culmination of an offensive action must necessarily be infrequent due to the nature of cyber weapons, we cannot forget that cyberspace offensive forces are military forces, and they must always be active. When a cyberspace offensive capability is not being employed to cause an effect, the force must be manoeuvring, prepositioning, and preparing to cause such effects when required. Inactivity cannot be the position of any military force. »When the time for action comes, the first requirement should be that all parts must act« (Clausewitz, 2007).

Conclusion

Sun Tzu said: *»The general that hearkens to my counsel and acts upon it, will conquer: let such a one be retained in command! The general that hearkens not to my counsel nor acts upon it, will suffer defeat: let such a one be dismissed!«* (Sun Tzu, 1910, p 4).

We have attempted to bring cyberspace out of the obscurity of its technical nature, and under the scope of well-established military knowledge, which is understood by all military thinkers, and which all domains in the battlefield share.

The purpose of this analysis has not been to state that all principles of ancient doctrine should be followed in cyberspace, or any other domain. Rather, we have pointed out that many such principles apply, and that the fight in the cyberspace domain is not of such a different nature that we can ignore the knowledge of war gained from centuries of human conflict. This helps us bring this new domain of operations to a level where it can be understood, framed in a familiar context, and hopefully allows it to be better addressed without having to learn from the experience of our own mistakes. It allows us to see past the differences of this new domain and focus on the similarities with other domains, which we can use to better implement the changes in our forces this new environment requires.

Cyberspace defensive forces can borrow concepts from the Cold War to plan and secure an early deployment in a battlefield that is determined, with allies that are known, and against an enemy that is familiar. They can learn from the lessons of ancient China when gathering the information to infiltrate an enemy position, whether the gates are made of wood or guarded by layers of encryption. They can learn from Von Clausewitz about the uneconomical perils of inactivity, from Miyamoto Musashi about the need for purpose in every action, and from Sun Tzu about the power of combined energy, the need for agility and the wisdom of seeking the least defended points in an enemy's defence. We can borrow procedures from Special Operations and from Electronic Warfare doctrines without mistaking our force for either one of them, and without losing sight of the unique identity of the forces that borrow these principles.

The purpose of this indirect intellectual approach to cyberspace is not to understand it in its most minute detail, but to help guide the implementation of general changes in doctrine, procedures and organization that will allow us to take full advantage of its capabilities and address the threats it contains in a timely manner. Knowledge alone will not be sufficient, if it is not translated into action. As Sun Tzu said, »One may KNOW how to conquer without being able to DO it« (Sun Tzu, 1910, p 12).

No doubt new principles and lessons are waiting to be learned in a battleground of such an unfamiliar nature: »While heeding the profit of my counsel, avail yourself also of any helpful circumstances over and beyond the ordinary rules« (Sun Tzu, 1910, p 4). However, in the same way that military experts have borrowed from the knowledge of their predecessors even when the weapons at their disposal were vastly different, we should not let our pride make us believe we have grown beyond benefiting from the inheritance of the brilliant minds of the past.

Cyberspace may be a new battlefield but war, as an act of force to compel our enemy to do our will (Clausewitz, 2007, p 13), is one of the oldest human activities. Human nature has remained constant for thousands of years, and it would be hubris to think it has suddenly changed in our generation. For as long as the nature of the commanders, the soldiers, and the purpose of warfare itself remain the same, the ancient principles will continue to apply.

Bibliography

1. *Ambrose, E. S. et al., 2006. The Cold War: A Military History. New York: Random House Trade Paperbacks.*
2. *Brantly, A., and Smeets, M., 2020. Military Operations in Cyberspace. In: Handbook of Military Sciences. s.l.: s.n.*
3. *CCDCOE, 2017. Tallinn Manual 2.0 on the international Law Applicable to Cyber Operations. 2nd Ed. Cambridge: Cambridge University Press.*
4. *CCDCOE, 2020. Cyber Commanders' Handbook. 1st Ed. Tallinn: NATO CCDCOE Publications.*
5. *Chourchoulis, D., 2015. A secondary front? NATO's forward defence strategy and its application in the southeastern region, 1966-1974. In: B. Lemke, (Ed.) Periphery or Contact Zone? The NATO Flanks 1961 to 2013. Berlin: Bundeswehr Centre of Military History and Social Sciences.*
6. *Clausewitz, C. V., 2007. On War. Oxford: Oxford University Press.*
7. *Denning, D. E., 2012. Stuxnet: What Has Changed? Future Internet, Issue 4.*
8. *Field, C., 2009. Asymmetric Warfare and Australian National Tactical Advantages: Taking the Fight to the Enemy. Sydney: Land Warfare Stdies Centre (Australia).*
9. *Gvineria, S., 2017. Information Warfare: New Security Challenge for Europe. 1st Ed. Bratislava: Centre For European and North Atlantic Affairs (CENAA).*
10. *McGhee, J., 2016. Liberating Cyber Offense. Strategic Studies Quarterly, 10(4), pp 46-63.*
11. *Merriam-Webster Inc., s.f. Merriam Webster Dictionary. https://www.merriam-webster.com/dictionary/, February 2022.*
12. *Musashi, M., 2011. The Book of Five Rings. 1 Ed. Boston: Shambhala Publications Inc..*
13. *NATO, 2013. AJP 3.5 Allied Joint Doctrine for Special Operations. A1 Ed. s.l.:NATO Standardization Office (NSO).*
14. *NATO, 2016. Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm, February 2022.*
15. *NATO, 2017. AJP-01 Allied Joint Doctrine. E Version 1 Ed. s.l.: NATO Standardization Office (NSO).*
16. *NATO, 2020. AJP 3.20 Allied Joint Doctrine for Cyberspace Operations. A Ed. s.l.: NATO Standardization Office (NSO).*
17. *NATO, 2020. AJP-3.6 Allied Joint Doctrine for Electronic Warfare. Brussels: NATO Standardization Office (NSO).*
18. *NATO, 2021. Allied Command Operations Comprehensive Operations Planning Guide COPD. 3rd Ed. Brussels: NATO Standardization Office.*
19. *Smith, R., 2005. The Utility of Force: The Art of War in the Modern World. s.l.: Allen Lane.*
20. *Sun Tzu, 1910. The Art of War. s.l.: Project Gutenberg.*

21. *U.S. Army War College, 2020. Strategic Cyberspace Operations Guide. 1st Ed. Carlisle: Center for Strategic Leadership.*
22. *U.S. Department of Commerce, 2011. Managing Information Security Risk: Organization, Mission and Information System View. Gaithersburg (Maryland): National institute of Standards and technology, U. S. Department of Commerce.*
23. *Unknown, 2022 (original work published 1769). King James Bible. https://www.kingjamesbibleonline.org/*
    [Last accessed: February 2022].
24. *US Army, 2012. ADP 3-90 Offense and Defense. 1st Ed. Washington D.C.: Department of the Army.*
25. *US Joint Chiefs of Staff, 2020. JP 3-85 Electromagnetic Spectrum Operations. 1st Ed. Washington D.C.: US Joint Chiefs of Staff.*
26. *US. Marine Corps, 1990. The Guerrilla and How to Fight Him. 1st Ed. Washington D.C.: Department of the Navy.*
27. *Van Creveld, M., 1991. The Transformation of War. New York: Simon & Schuster Inc.*
28. *Van Creveld, M., 2000. A History of Strategy: From Sun Tzu to William S. Lind. 2nd Ed. Kouvola: Castalia House.*
29. *Van Creveld, M., 2011. The Age of Air Power. Digital Ed. New York: Simon & Schuster Inc.*

e-mail: ignacio.pizarro@ccdcoe.org

e-mail: ignacio.pizarro@ccdcoe.org

Podpolkovnik Ignazio Pizarro je štabni častnik za zveze španske kopenske vojske. Šolal se je na vojaški častniški akademiji v Zaragozi v Španiji, usposabljanje s področja zvez pa je opravil v Madridu in leta 2000 pridobil čin poročnika. Končal je generalštabno šolanje na španski vojni akademiji. Opravil je različne specializirane tečaje in usposabljanja španskih oboroženih sil, ameriške vojske in Nata iz vojaških komunikacij, operativnega načrtovanja in kibernetske obrambe. Je vodja Sektorja za operacije v Natovem centru odličnosti za kibernetsko obrambo.

Lieutenant Colonel Ignazio Pizarro is a Spanish Army Signal Corps Staff Officer. He received training at the Army Officer's Academy in Zaragoza (Spain), and his Signal Corps Officer training and education in Madrid, graduating as an Army Lieutenant in 2000. He graduated as a General Staff Officer from the Spanish War College. He has received specialized courses and training by the Spanish Armed Forces, the U.S. Army and NATO in the areas of Military Communications, Operational Planning and Cyber Defence. He holds the position of head of the Operations Branch, at the NATO Cooperative Cyber Defence Center of Excellence.

*Prispevki, objavljeni v Sodobnih vojaških izzivih, niso uradno stališče Slovenske vojske niti organov, iz katerih so avtorji prispevkov.

*Articles, published in the Contemporary Military Challenges do not reflect the official viewpoint of the Slovenian Armed Forces nor the bodies in which the authors of articles are employed.