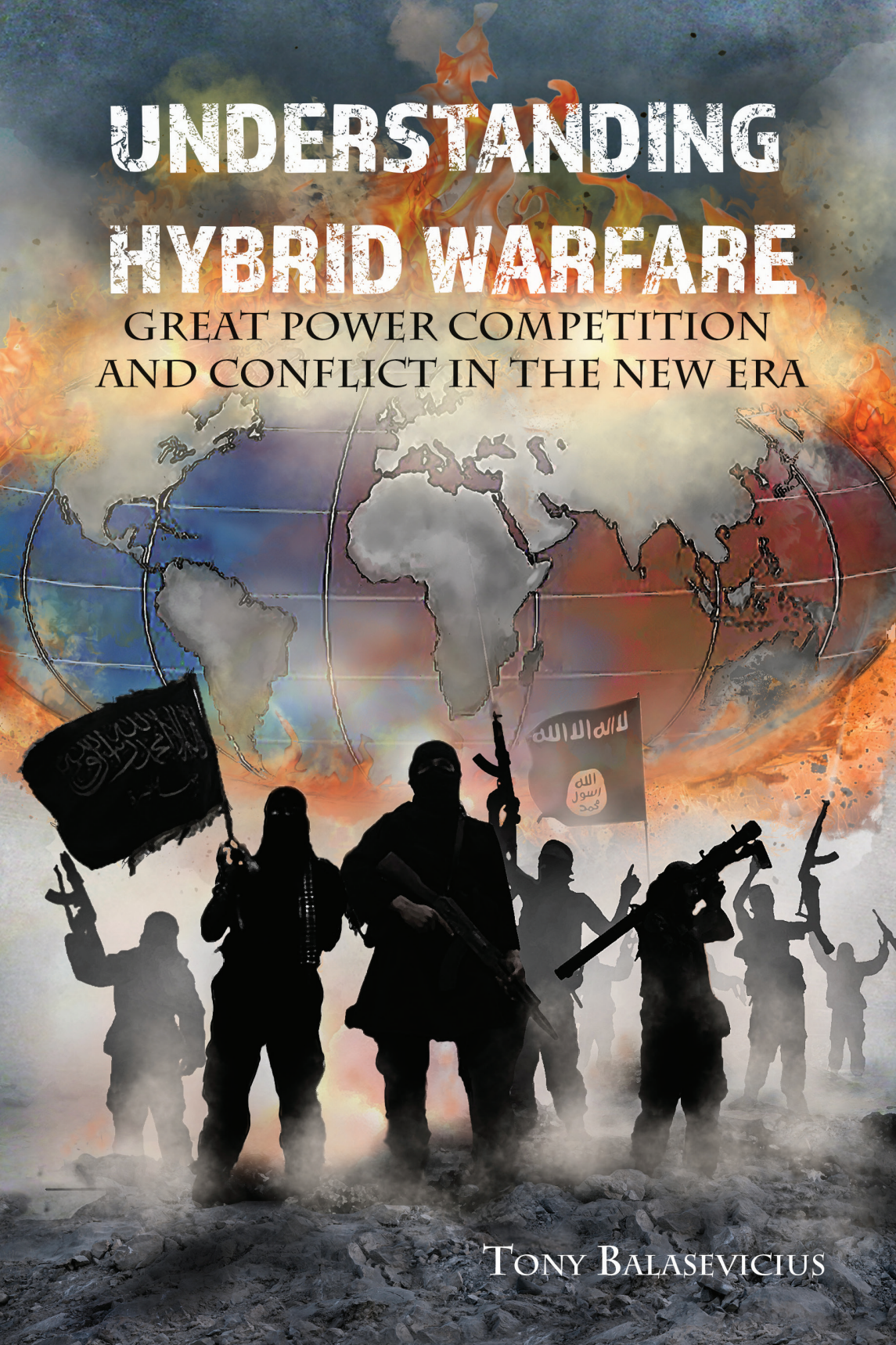
UNDERSTANDING HYBRID WARFARE

GREAT POWER COMPETITION AND CONFLICT IN THE NEW ERA



TONY BALASEVICIUS

UNDERSTANDING HYBRID WARFARE

UNDERSTANDING HYBRID WARFARE:

GREAT POWER COMPETITION AND CONFLICT IN THE NEW ERA

TONY BALASEVICIUS

Canadian Special Operations Forces Command
101 Colonel By Drive
Ottawa, Ontario K7K 7B4

Produced for CANSOFCOM Education & Research Centre
by 17 Wing Winnipeg Publishing Office.
WPO32517

COVER GRAPHIC: Artwork by Silvia Pecota

ISBN 978-0-660-75693-6 (Print)
ISBN 978-0-660-75692-9 (PDF)

Government of Canada Catalogue Number D2-693/2025E (Print)
Government of Canada Catalogue Number D2-693/2025E-PDF (PDF)

Printed in Canada.

1 3 5 7 9 10 8 6 4 2

DISCLAIMER

The views expressed in this publication are entirely those of the author and do not necessarily reflect the views, policy, or positions of the Government of Canada, the Department of National Defence, the Canadian Armed Forces or any of its subordinate units or organizations.

TABLE OF CONTENTS

PART I

TOWARDS A DOCTRINE OF HYBRID WARFARE

PART II

CASE STUDIES IN THE EMPLOYMENT OF HYBRID WARFARE

PART I

TOWARDS A DOCTRINE OF HYBRID WARFARE

INTRODUCTION TO PART 1

Continuing events and increasing instability in the world seem to indicate that the established international order is in transition, if not under attack. Russian military operations in Ukraine, as well as its gray zone operations in Europe and Scandinavia; Chinese operations in the South China Sea, Taiwan and around the globe; Iran and its proxy forces' actions in the Middle East; North Korean troops fighting on behalf of the Russians are all examples of a disintegrating global order of things. Quite simply, the strategic environment is shifting from the unipolar system based on American dominance, to a multi-polar world where peer and near-peer adversaries are asserting their influence and attempting to challenge the existing rules-based international order in the pursuit of their own national interest.

Not only are these nations becoming increasingly assertive on the world stage, they are beginning to display capabilities and performance levels that have the potential to undermine Western military and technological superiority. Moreover, they have shown abilities to limit or prevent short term access to important emerging capabilities such as space, cyberspace, and the electromagnetic spectrum.[1]

Of greater concern for Western powers is the fact that the warfighting doctrines of these actors are moving away from direct military confrontation. In fact, they have begun integrating strategic, operational and tactical operations into a holistic construct. This approach, combined with their employment of various instruments normally associated with national power, is allowing them to carry out sustained attacks on all aspects of their opponents' existence. Their assaults impact adversaries' economies, culture, foreign relations, environment, natural resources, legal frameworks, as well as their cyber and information domains to name but a few. The purpose of such attacks is to destroy a nation's collective will through the application of what is now being termed Hybrid Warfare.

These actions are being done by understanding a target country's weakness and using a series of selective, but coordinated and comprehensive

attacks, against those weaknesses to erode public confidence in the established authority. Such methods, properly employed and sequenced, have the capacity to throw a stable and thriving state into disorder and chaos, by creating social unrest, humanitarian upheaval, and in some cases civil war. Once established, such conditions make the target country susceptible to intervention and defeat. Within the design of a Hybrid Warfare attack, a new phenomenon is emerging in the form of the "battlefield of battlefields" concept.

The creation of a "battlefield of battlefields" is forcing nations to simultaneously fight for a host of strategic capabilities, outside of the protections traditionally provided by military forces. As a result, we are beginning to see changes in how nations start, conduct, and manage competition, conflict and war. Success in future war will increasingly depend on a nation's ability to manage, control and integrate the various aspects of total conflict, in all its forms. As a result, Western nations will need to take a longer-term view and more holistic approach to the concept of planning and conduct of competition and conflict and how it relates to the traditional idea of conventional warfare.

Recent Western experience with the application of Hybrid Warfare suggests that peer and near peer adversaries will wish to avoid direct engagement with Western powers for as long as possible. This reality will require a national-level focus on how to coordinate operations short of war in order to deal with such issues as economic, cyber and information conflict, proxy, and insurgent wars. More importantly, the outcome of these activities must be positioned to support the eventual transition into conventional warfare should that become necessary.

With direct military confrontation being delayed for as long as possible, non-state actors will play an increasingly important role for both Western states as well as peer and near peer adversaries as time goes on. They can become a serious threat to states, as well as important allies to others. Recent events in Syria and Iraq, have demonstrated that advanced armed non-state actors such as Hezbollah have the ability to take on regional powers. They have also shown a capacity to fuse their operations with regular armies to produce various forms of compound warfare.

This means that complexity at the strategic level will now force defence planners to overcome the problems of dealing with a broader concept of conflict. However, complexity at the tactical and operational level will force military planners to deal with the conventional military force and armed non-state actor mix as a routine part of military operations.

As strategic, operational and tactical operations become more interrelated on the field of battle, the ability of governments and their military forces to transcend this complexity with adaptive command and control capabilities, flexible doctrine and resilient force structures will become increasingly important.

Over time, as these activities become more coherent and drift further away from the constructs of purely conventional or irregular war a clearly established Western doctrine for Hybrid Warfare will need to emerge. In fact, this requirement is already apparent. Western analysts and their leaders used the phrase "Hybrid Warfare" to describe all non-conventional aspects of warfare. For example, Hybrid Warfare has been used to described everything from Russian and Chinese operations in Estonia, Crimea and the South China Sea to Hezbollah's tactical fighting style in its 2006 war with Israel.

To provide readers with a better understanding of what this type of warfare entails, this volume seeks to identify and explain the important trends that have emerged since the Russian cyber attacks on Estonia in 2007. It will highlight the various levels of Hybrid Warfare in an effort to establish the links towards a holistic warfighting concept while examining how such operations are likely to impact Western militaries and their governments in a future conflict. Finally, it will analyze what Western nations must do to prepare for, and counter, this type of warfare.

To accomplish this task, the book is divided into three sections. Part I: *Towards A Doctrine of Hybrid Warfare,* looks at the modern theoretical development around this type of warfare. Part II: *Case Studies in The Employment of Hybrid Warfare,* reviews key events that highlight specific aspects of Hybrid Warfare and provides readers with a better understanding of the practical application of this type of warfare and how it could play out. Part III: *Countering The Hybrid Warfare Threat*, offers

recommendations on what Western governments could do to prepare for, and mitigate, the effects of this type of conflict.

In order to comprehend this type of war and the changes that are occurring, it is important to start with a baseline understanding of the construct of war.

CHAPTER 1

UNDERSTANDING THE CONFLICT CONSTRUCT

In their book *Making Strategy: An Introduction to National Security Processes and Problems*, Dennis Drew and Donald M. Snow assert that there are three types of war that modern armed forces might be required to fight. They state that these wars include conventional, counterinsurgency, and strategic nuclear warfare.[1] These specific conflicts have been broken down into what the North Atlantic Treaty Organization (NATO) referred to as View 1, 2 and 3 environments.[2]

The View 1 environment is defined as conventional battle between national entities and suggests that such conflicts will see "established military forces engage in high-tempo operations that involve the application of complex technologies."[3] In this respect, conventional warfare can be defined as:

> a form of warfare conducted by using conventional military weapons and battlefield tactics between two or more states in open confrontation. The forces on each side are well-defined and fight using weapons that primarily target the opposing army. It is normally fought using conventional weapons and not with chemical, biological or nuclear weapons. The general purpose of conventional warfare is to weaken or destroy the opponent's military force thereby negating its ability to engage in conventional warfare.[4]

An example of this form of war in recent times is the 1991 and 2003 Gulf Wars between the American-led Coalition and Iraq. Since 1945, there has been an average of two View 1 conflicts per decade.[5]

The next type of conflict within the construct is the idea of View 2. View 2 clashes are referred to as asymmetric in nature. Asymmetric warfare is war between belligerents whose relative military power or whose

strategy or tactics differ significantly. In this regard, asymmetric warfare can describe a conflict in which the resources of two belligerents differ significantly in essence. As such, they attempt to exploit each other's characteristic weaknesses. Such struggles often involve strategies and tactics of unconventional warfare: the weaker combatants attempting to use strategy to offset deficiencies in quantity or quality. Also, it is important to note that such strategies may not necessarily be militarized.[6] The assumption is that this type of conflict "envisions the nation state opposed by armed bodies that are not necessarily armed forces, directed by social entities that are not necessarily states, and fought by people who are not necessarily soldiers."[7] In fact, many security analysts still believe that the international community will be facing this type of conflict, primarily in the form of insurgencies, for the foreseeable future.[8]

The third element within this construct is View 3, strategic nuclear warfare, or war involving the extensive use of nuclear weapons. Although, nuclear warfare is beyond the scope of this study, it is important to have a general frame of reference about this aspect of conflict. Nuclear warfare is described as a military conflict in which nuclear weapons are used to inflict damage on an enemy. In contrast to conventional warfare, nuclear war can produce far greater destruction in a much shorter timeframe and can have a far longer impact on the enemy it is used against. This impact includes the long-term effects from the radioactive fallout that is released. Nuclear warfare can be divided into two sub-groups including a limited or a full-scale nuclear war.

A "limited nuclear war" refers to the small-scale use of nuclear weapons by two (or more) belligerents. A limited nuclear war could include targeting military facilities – either as an attempt to pre-emptively cripple the enemy's ability to attack as a defensive measure, or as a prelude to an invasion by conventional forces as an offensive measure. The second type of nuclear war, a full-scale nuclear war, would consist of large numbers of nuclear weapons used in an attack aimed at a county's entire military, political, social and economic infrastructure.[9]

Of course, few conflicts fall neatly into one or the other of these Views. In fact, many, if not most, conflicts have been mixtures of at least two Views. As a result, there is recognition that transitions may and will occur

from one form of conflict to another very quickly, as happened during the French Indo-China conflict from 1948-1954. Conversely, these different Views may occur simultaneously, as happened in South Vietnam during the period 1963-1968.[10] Warfare between the realms of View 1, 2, and 3 has been referred to by some analysts as hybrid conflicts.

According to Frank Hoffman of the Centre for Emerging Threats and Opportunities, hybrid conflicts "entail a convergence and fusion of regular and irregular warfare techniques that can be employed both by states and non-state actors."[11] Within this construct, no one type of warfare would necessarily predominate. In fact, the employment of a wide range of fighting methods, "involving conventional capabilities, irregular tactics and formations, terrorist acts, coercion, and criminal disorder are all used singularly or in combination to achieve synergistic effects."[12] When looking at these different views and their manifestations on a graph they would appear somewhere within the range of Figure 1 below.

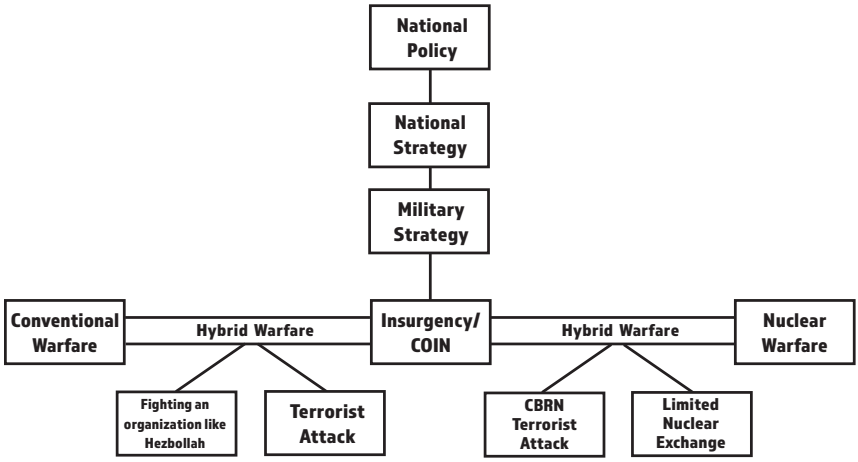


FIGURE 1: The Conflict Construct[13]

Asymmetric warfare occurs because many nations lack the resources necessary to address all conceivable tasks across the entire spectrum of the conflict construct so they must determine where to focus their energies and resources, balancing the most likely anticipated operational requirements they may face against the one with the greatest threat. To achieve this outcome, force planners attempt to determine what View of

conflict their military must be prepared to deal with in the future and what additional capabilities, if any, it will be required to have sufficient flexibility to adapt its force structure to deal with other unexpected threats should they arise. For example, if a military force focuses its development of joint forces to be optimized for View 2 type operations, then it must also decide what additional capabilities it will need in order to transition into a more conventional View 1 conflict, at least for a limited period of time. Moreover, planners must determine what trade-offs should be made to its optimized force structure for such an eventuality. In dealing with these trade-offs, nations will usually look for asymmetric solutions to compensate for their lack of capabilities in specific areas.

Traditionally, states have fought conventional wars while non-state actors have focused on more asymmetric forms of warfare. However, it is now clear that this trend is changing as near-peer nations begin to use state-level hybrid or asymmetric warfare. In fact, this type of warfare was successfully employed by the Russians in their occupation of Crimea in 2014.

In this example, the Russians were able to achieve an asymmetric result by fusing their actions at the strategic, operational and tactical levels of war and integrating a broader selection of national tools into a more comprehensive concept of conflict. This specific concept seeks to create a political or diplomatic *fait accompli* before an opponent's military force can be applied.[14] In such cases. national tools often include the coordinated use of political, economic, informational, cultural and diplomatic means, as well as the environmental, and natural resources, among others, all focused on a specific strategic outcome.

Although, there has been debate in the West on whether this is actually something new or just repackaged traditional methodology, there is general agreement that the coordinated use of these techniques have had extremely effective results while creating additional complexity and confusion within the traditional military operating environment.[15] Undeniably, Western nations have had difficulty in finding effective counters to this threat.

This failure is due in some part to the fact that many believe that such operations are little more than well-executed military campaigns backed-up by an extensive use of deception and information warfare. Unfortunately, although these factors are present, they constitute only a small part their success. In order to better understand the specific changes that are occurring within the context of this type of conflict, it is important to undertake a deeper look into the genesis and components of this type of conflict/warfare. In order to do that, it is first imperative to understand the changing character of war.

CHAPTER 2

THE CHANGING CHARACTER OF FUTURE CONFLICT

As the international security environment continues to move towards a multi-polar world, there has been a visible change in the focus of Western nations on the world stage. Specifically, there has been a shift from dealing with non-state actors in failed or failing states to viewing emerging powers as the greatest threat to the existing world order. With this rebalance in threat perception comes a distinct change in awareness of how future wars should be fought.

A paper published by the American Army's Training and Doctrine Command (TRADOC) in January 2017, suggested that in the future, Western forces will need to contend with potential opponents that are far more modern and versatile than has been the case for a number of decades.[1] This rise in peer competitors is also forcing a change in the character of future warfare. Realizing that it would be some time before they can match Western military strength and performance on the modern battlefield, emerging powers started adopting asymmetric strategies in an attempt to even the playing field. These strategies are specifically designed to avoid joint level operational art (i.e. military campaigns) by moving the focus of the fight to the strategic and tactical levels of warfare by, as Lieutenant General Ben Hodges points out, "embracing the simultaneous employment of multiple instruments of war."[2]

Taken together, these trends are moving conflict into a more holistic state-controlled, or "whole of government" approach than has previously been the case. This move is due in part to the fact that authoritative governments understand democracy's strength lies in the institutional checks and balances which prevent long-term cooperation between the different governmental institutions. In this respect, peer and near-peer adversaries, are attempting to use democracy's strength against itself. By forcing democracies into a fight where long-term interagency cooperation

is critical to success, authoritative governments can gain the upper hand by rewriting the rules for conflict and forcing a fight into an area where they are stronger.

Within this context, a country's citizens become the primary target in winning the war and the strategic outcome of future conflict shifts from defeating an enemy's army on the battlefield to creating unrest and revolt within the social fabric of an opponent's society. The net result of such actions is to formulate a political crisis where military forces simply become one of many tools needed to produce a victory.

In order to address this shift of methodology for waging conflict, one that could threaten Western dominance, a new way of thinking about how wars are fought needs to be developed. Historically, Western political and military thinking has been confined to the results that can be achieved by conventional military forces on the battlefield where victory or defeat was clearly established. In this scenario, military victory sets the conditions for a political solution. In future war this type of thinking will no longer be valid.

As demonstrated, in Figure 1 [page 7], historically the idea of war has been confined to conventional warfare, insurgency and nuclear conflict. More recently, however, the expansion of insurgency doctrine, and the idea of moving away from the operational level of warfighting to fighting at the strategic and tactical levels has become increasingly prevalent. In order to better understand this concept, it is important to examine the basic foundation that is underlying this new approach.

THE CONCEPT OF UNRESTRICTED WARFARE AND ITS IMPACT ON THE CHANGING CHARACTER OF WAR

Traditionally the Chinese People's Liberation Army (PLA) relied on a "Peoples War" doctrine as well as an emphasis on numerical conventional force advantage to offset the technical superiority of its perceived opponents. However, as it started looking at power projection capabilities in the 1980s, the Chinese realized they needed to modernize both their force structure and doctrine.[3] The stunning victory of the American-led coalition in the first Gulf War against Iraq gave the

Chinese an opportunity to study best practices in modern military operations. From the PLA perspective, the conflict demonstrated that the balance in warfare had shifted heavily in favour of smaller, high technological forces.[4]

The Chinese were particularly impressed with the American use of new technologies such as networked computers, precision-guided munitions, Global Positioning System (GPS), global telecommunications, and unmanned aerial vehicles.[5] They realized that these capabilities gave the Americans an unprecedented degree of information about the opposing forces, and they believed this played a vital role in their subsequent destruction. As a result, PLA analysts started seeking ways to overcome this informational advantage.[6]

The result was a two-step process. First the PLA embarked on a program to become more technologically enabled by acquiring advanced equipment and weapon systems. However, they also looked at options to mitigate the advantages given to a high technological enemy.[7] Part of this latter effort bore fruit in February of 1999, when two PLA Air Force colonels, Qiao Liang and Wang Xiangsui, published a book entitled *Unrestricted Warfare*.

The thesis of their work was based on the idea that there was little value in directly confronting American operational excellence on the battlefield. As a result, the focus of conflict needed to move away from conventional warfare as the only method for winning a war. They argued this could be done by broadening the idea of conflict to include the various elements of national power. The authors reasoned that current advances in technology and weapons, globalization, and the diffusion of state power had combined to create the needed conditions for this new form of warfare.[8] Moreover, they suggested that those involved in the planning and conduct of warfare had generally viewed the non-military domains as little more than accessories that serve military requirements. As a result, the development of the modern battlefield, as well as possible changes in strategy and tactics, had been limited to that one domain.[9]

The authors understood that developing a strategy involving a number of different domains would require integrating a complex mix of

information and resources. This process would start with producing a detailed knowledge of the strengths and limitations of one's own national security capabilities. Armed with this information, a country would be able to superimpose "political and military factors on the economy, culture, foreign relations, technology, environment, natural resources, nationalities, and other parameters to draw out an 'extended domain.'"[10] Once the strategic requirements (resources) were in place for this "extended domain" a nation would be able to create what they referred to as the "battlefield of battlefields."

In theory, the creation of the "battlefield of battlefields" would allow a nation to reduce the impact of superiority in one (military) battlefield by forcing an opponent to deal with many battlefields simultaneously.[11] They termed the synthesis of these ideas "modified combined war that goes beyond limits."[12] A key pillar of this concept is to exploit the benefits of "combinations" in types of organizations and among the various domains of national power.[13]

In this respect, the authors reasoned that the key to victory on the "battlefield of battlefields" was understanding and coordinating the effective use of four specific types of combinations: Supra-National Combinations (combining national, international, and non-state organizations to a country's benefit), Supra-Domain Combinations (combining battlefields and choosing the main domain), Supra-Means Combinations (combining all available means, military and non-military, to carry out operations), and Supra-Tier Combinations (combining all levels of conflict into each campaign).[14]

Integrated within the idea of combinations was the use of eight principles that they outlined as follows:

1. Omnidirectionality;
2. Synchrony;
3. Limited Objectives;
4. Unlimited Measures;
5. Asymmetry;
6. Minimal Consumption;

7. Multidimensional Coordination; and

8. Adjustment and Control of the Entire Process.

Three of these principles are of special interest to the West in attempting to understand state level Hybrid Warfare. These include Omnidirectionality, Synchrony, and Asymmetry:[15]

> **Omnidirectionality** – is the starting point of "unrestricted war" ideology and is a cover for this ideology..., there is no longer any distinction between what is or is not the battlefield. Spaces in nature including the ground, the seas, the air, and outer space are battlefields, but social spaces such as the military, politics, economics, culture, and the psyche are also battlefields. And the technological space linking these two great spaces is even more so the battlefield over which all antagonists spare no effort in contending. Warfare can be military, or it can be quasi-military, or it can be non-military. It can use violence, or it can be nonviolent.[16]

> **Synchrony** – [is about] Conducting actions in different spaces within the same period of time... So many objectives which in the past had to be accomplished in stages through an accumulation of battles and campaigns may now be accomplished quickly under conditions of simultaneous occurrence, simultaneous action, and simultaneous completion. Thus, stress on "synchrony" in combat operations now exceeds the stress on phasing.[17]

> **Asymmetry** – No matter whether it serves as a line of thought or as a principle guiding combat operations, asymmetry manifests itself to some extent in every aspect of warfare. Understanding and employing the principle of asymmetry correctly allows us always to find and exploit an enemy's soft spots. The main fighting elements of some poor countries, weak countries, and non-state entities have all used "mouse toying with the cat"-type asymmetrical combat methods against much more powerful adversaries... Instead, the weaker side has contended with its adversary by using guerrilla war (mainly urban guerrilla war), terrorist war, holy war, protracted war, network war, and other) forms of combat.[18]

The fundamental precept derived from the idea of combinations used within the context of these principles is that there is no longer a distinction between what is or is not a battlefield. Along with the traditional battlefields normally associated with military operations (Air, Land, Sea, Cyber, and Space) everything from politics, economics, culture, to the national psyche may now become a possible battlefield. The key feature of this type of warfare is the ability to conduct, coordinate and synchronize actions within these different battlespaces, which potentially can, and in many instances should, occur at the same time.[19]

The authors theorized that throughout history military victories "display a common phenomenon: the winner was the one who could combine well."[20] To highlight the idea of combining activities within multiple battlefields they introduced the concept of "simultaneously" and emphasized that it would play an increasingly important role in future operations.[21] They reasoned that if a state could achieve a single full-depth, synchronized action across all battlefields the paralysis caused to the enemy could be sufficient to decide the outcome of an entire war.[22] The authors provide an example of how such an operation might unfold as it links into the concept of combinations:

> ...by using the combination method, a completely different scenario and game can occur: if the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in an attacking nation advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty.[23]

In their analysis, Liang and Xiangsui suggested that preparation for, and specific activities related to, this form of conflict would have to occur well before the start of a formal declaration of war. Moreover, they saw the centre of gravity focused on creating social panic leading to a political crisis. Once the crisis had developed sufficiently, conventional military force could be applied but only to the extent necessary to achieve victory.

In developing this asymmetric approach, the authors concluded that asymmetry, which is at the heart of this type of warfare, should be used to find and exploit an enemy's soft spots. They asserted that poor countries, weak countries, and non-state entities have all used some type of asymmetrical combat methods against much more powerful adversaries as a means to even the playing field. This means that when a country faces a technologically superior enemy, the key to success lies in moving the fight from purely military operations to a much broader interpretation of warfare. Namely, one that includes Financial Warfare, Cultural Warfare, Media Warfare, Technological Warfare, Psychological Warfare, and Network Warfare, to name a few.[24]

By using such methods, a nation or armed non-state entity could minimize the impact of technological superiority and the associated increase in combat power that such advantages currently provide a conventional military force. In so doing, a nation would make the enemy fight one's own type of war, which if done correctly, would occur on a number of different and more complex battlefields than has previously been the case. Interestingly enough, this is exactly what the Russians were attempting to achieve with their involvement in Eastern Europe and Syria.

How much the Russians have been influenced by Chinese thinking on the subject of state-level asymmetric warfare is difficult to ascertain. However, it is clear that many of the key concepts underlining *Unrestricted Warfare*'s philosophy, particularly the ideas of coordination, synchrony, the "battlefield of battlefields," creating social panic leading to political crisis, and the judicious application of military force, have all been displayed in recent operations undertaken by the Russians. Also, much of this philosophy has been articulated in public statements by senior officials on how the Russians view the future of conflict within the context of what some analyst referred to as "New Generation Warfare."

CHAPTER 3

INSURGENCY AND THE RISE OF HYBRID WAR AT THE TACTICAL LEVEL

A key component of the modern approach to state level Hybrid Warfare is the use of non-state actors, particularly armed ones. Armed non-state actors have been an important part of Russian actions in Crimea, Eastern Ukraine, and Syria, while forming the foundation of Iran's hybrid strategy and the manifestation of the Axis of Resistance. In fact, the influence and capabilities of armed non-state actors has steadily increased since the end of the Cold War, to the point where they now pose a major security challenge to international stability in their own right.

Of particular interest to nations are the unique challenges conventional military forces face when dealing with sophisticated groups such as Hezbollah, and Daesh, also known as the Islamic State in Syria and Iraq (ISIL). In addition to being dominant regional players in their own right, their growing capabilities, particularly at the tactical level, are now being fused with peer and near-peer adversaries' capabilities and doctrines to give these groups global influence.

The development of these armed non-state actors as a major threat to regional and international stability has been influenced by many of the same factors that have given state military institutions their advantages. These factors include advances in technology, the rise of globalization, and the increased capabilities of modern weapons, all of which have combined to create a new context for conflict. In many cases, armed non-state actors have been at the forefront of these changes while states often seem slower to react.

As Richard H. Shultz, Douglas Farah, and Itamara V. Lochard, point out in their monograph, *Armed Groups: A Tier-One Security Priority,* armed groups can now acquire the capacity to execute violent strikes that can have a strategic impact on even the most powerful nation-states. They explain, "This is analogous to a revolution in military affairs (RMA),

in which the conduct of war dramatically changes as the result of major alterations by a nation-state in military organization, technology, doctrine, and/or leadership."[1] From the perspective of the non-state actor, these changes have created a new conceptual approach to military operations, one that allows them to quickly transition from View 2 (insurgency) to View 1 (conventional) operations and back again with little or no effort.

This flexibility is due to the fact that advances in information technology have started to blur the lines between different types of warfare, the organizations that fight them, and the technologies that are used.[2] In essence, non-state actors now have the ability to use multiple types of warfare simultaneously as they, out of necessity, continue to bring together various types of fighting methods into a single operational methodology.[3] This flexibility is allowing such forces to emerge as an operationally decisive force on the military battlefield.[4]

Traditionally such forces have required a great deal of time to break down their enemy and achieve victory. This requisite was largely due to the fact they did not have the means to decisively defeat their opponent quickly. However, the ability to switch from one method of fighting to another, or to combine different methods simultaneously, has provided irregular forces with the means of fighting the decisive battle and in the process, fundamentally changed that dynamic on the modern battlefield. Moreover, it has created a complex security challenge for any conventional military fighting these types of forces.

The second development that has given armed non-state actors an advantage in fighting conventional military forces has been access to key advanced technology weapon systems. An example of this trend can be seen as far back as the Soviet-Afghanistan conflict of the 1980s. By 1986, the Soviets were gaining the upper hand over the Mujahideen through the use of high mobility operations based on helicopters. However, this advantage was quickly neutralized when the Americans started providing the Mujahideen with stinger missile systems in the fall of 1986. Almost overnight the conflict shifted back in favour of the Afghan fighters. A similar situation can be seen with Hezbollah, during the 2006 war with Israel when Hezbollah fighters employed different missile systems to strike Israeli cities, take out tanks and damage a naval vessel.

In seeking to defeat such forces, the first question that needs to be addressed is from where does that force derive its core strength? The answer to this question lays in understanding the character of an armed non-state actor's irregular warfare capability and what they are trying to achieve. In this regard, most successful armed non-state actors have based their organization and fighting capabilities on creating an insurgent organization based on the doctrine of Mao's *People's War* that has been adapted to meet the requirements of the local situation.[5]

In its broadest terms, the insurgency model is designed to mobilize supporters and establish a viable alternative authority to an existing government, while employing military means to attack and weaken the state through a relentless process of escalating violence.[6] This construct was designed, and has evolved, to defeat a stronger and more technologically superior enemy. This has been achieved by avoiding the enemy's strengths and constantly hitting his weaknesses over an extended period of time. This is the same concept used by peer nations that employ state level Hybrid Warfare. So, it is important to understand insurgency doctrine in order to comprehend the larger picture of what is trying to be achieved.

THE INSURGENCY IS THE TACTICAL HEART OF HYBRID WARFARE FOR THE ARMED NON-STATE ACTOR

Shultz, Farah, and Lochard define an insurgency as:

> protracted political and military set of activities directed toward partially or completely gaining control over the territory of a country through the use of irregular military forces and illegal political organizations. The insurgents engage in actions ranging from guerrilla operations, terrorism, and sabotage to political mobilization, political action, intelligence/counterintelligence activities, and propaganda/psychological warfare. All of these instruments are designed to weaken and/or destroy the power and legitimacy of a ruling government, while at the same time increasing the power and legitimacy of the armed insurgent group.[7]

Historically, insurgencies have been successful because they have evolved to meet the specific conditions of their environment and circumstances.[8] The idea is to integrate political, social and economic elements into what has been essentially a military activity.[9] This integration is at the heart of the insurgent's potential on the future battlefield and is the foundation of state-level Hybrid Warfare. As such, it allows those using this method the flexibility to strike at the strategic, operational and tactical level targets of their opponents. It is this ability to select the level of war on which to fight at that allows the user to circumvent their opponents' strengths. This will likely become a defining feature of future conflict.

MOBILIZATION

Within this new construct, the key to success is to develop the human potential. This is done through a process of political or religious mobilization. As Mao explained, "To wish for victory and yet neglect political mobilization is like wishing to 'go south by driving the chariot north,' and the result would inevitably be to forfeit victory."[10] In order to mobilize the masses the insurgents need to first gain the people's support. To this end, they promise the people a number of reforms such as land redistribution, a fair justice or taxation and various services such as health care and garbage pickup. These things allow the insurgents to gain the support of the people which in turn allows mass organizations to be built, recruits to be found, and leadership talent to be reared up through the organizations.[11] In essence, political or religious mobilization within the context of an insurgency model becomes a process devoted to winning over and then preparing the people for conflict.

Western literature has often referred to this idea as winning the "hearts and minds." However, this phrase is extremely misleading. Within the context of an insurgency the idea is really about control and using that control to achieve specific goals. As author Edward Rice explains, the concept of Chinese Communist land reform was little more than a simple but extremely innovative motivator for controlling the people, "They [the Communist] would mobilize the peasants of the countryside against the status quo authority with such things as the seizure and redistribution of the land. They would arm the peasants, who would [then] have to fight if they were to protect their gains."[12] In order to efficiently mobilize the

people, insurgents need some way of harnessing the process. The only organization big enough for such a task is their military capability.

As such, the military usually has two roles, fighting and executing the organization's work.[13] As a result, this dual function can only be achieved by close co-operation between the organization's leaders, their fighters, and the people. To attain this unity, the insurgent leadership will usually reduce the basic fighting formations within their force to company or battalion size units for better control. They will also establish a cadre of spies in each formation starting at platoon level. This cadre is usually controlled by a political or religious officer, who is responsible for looking after the organization's interest, while providing political or religious instruction. Many insurgents believed that the political or religious cell within the fighting element is the "lifeline of all work as it would control the political indoctrination process of both the soldiers and the people."[14]

In the Chinese Communist insurgency, control over the army was further strengthened when a designated political officer and military leader became co-commanders.[15] The actual exercise of control was done through what appeared to be a very democratic organization called the people's councils.

These councils were initially established as a forum for administration and a method of understanding and dealing with local disputes and issues. More importantly, the system also created an opportunity for the party to educate the people in such things as reading and writing, understanding the Revolution, and the evils of foreign aggression.[16] However, over time the councils evolved and developed a much darker side to them.

In the example of China, Mao found that they were an ideal method of monitoring the "proper development" of the people. They could also be used by the party to manipulate public opinion. As Han Suyin, an authority on Mao writes, "the most powerful educational method consisted of the conference - debate." Where, "All rank disappeared, soldiers had full rights to free speech." During the conference "Not only were battles and campaigns discussed, but the individual conduct of any commander or fighter could also be criticized."[17] This public criticism also allowed CCP officials to manipulate the downfall or rise of specific individuals.[18]

THE STRATEGIC FRAMEWORK OF AN INSURGENCY

In order to provide a strategic framework for their fight against the established authority insurgents will usually lay out the steps that are necessary to eventually achieve victory, these could include:

a. Arousing and organizing the people;

b. Achieving internal unification politically;

c. Establishing bases;

d. Equipping forces;

e. Recovering national strength;

f. Destroying enemy's national strength; and

g. Regaining lost territories.[19]

Resource limitations within an insurgency will not allow these objectives to be accomplished simultaneously; therefore, insurgency leadership will divide them into phases or stages.

The first stage is often referred to as the strategic defensive, in which the insurgents are clearly on the defensive. During this phase the insurgency will not become involved in direct military action with the enemy, but rather it will harass the enemy by engaging in such activities as espionage, terrorist attacks, and civil unrest.[20] As such, Stage I, according to Mao is "devoted to the organization of an underground resistance movement for the purpose of spreading propaganda and eliciting support for the movement." Mao insisted, "The main purpose of this stage is to lay the ground work to overthrow the existing authority."[21] Whatever that authority may be, is irrelevant.

The second stage is commonly referred to as the strategic stalemate stage. At this point the enemy still retains the upper hand but both sides have reached some state of equilibrium. This period is characterized by small-scale combat operations. Activities during this phase will often include such things as widespread terrorism and guerrilla warfare.[22] Once the insurgent forces obtain local superiority, the insurgency can proceed

to stage three and what is referred to as the strategic counteroffensive. This last stage is characterized by the extensive use of large-scale mobile operations that are used to carry out the final destruction of the enemy.[23] It is during this stage, as insurgents make the transition from guerrilla warfare to mobile operations, that the hybrid nature of insurgent operations comes to the forefront.

MILITARY OBJECTIVES OF AN INSURGENCY

The strategic objective of an insurgency is to reverse the power relationship within a country. This is achieved at the operational level by wearing down the establishment's strength, while the insurgents attempt to build up their own through sustained efforts at mobilizing support.[24] In order to achieve these operational objectives, an insurgency needs to establish and then maintain certain tactical conditions throughout a campaign. As a minimum they had to have, "a cause to fight for, support from the local populace, bases, mobility, supplies and information."[25]

These conditions allow the insurgency to meet the operational objective of building strength through mobilizing support. This in turn, provides the foundation for achieving the other operational task. However, before an insurgency can move forward, it needs a place where it can establish the necessary tactical conditions to achieve the operational objectives. For Daesh/ISIL this was in Raqqa, and for Hezbollah it is in Southern Lebanon.[26]

THE INSURGENCY BASE

During the active life of the insurgency the base becomes the political, economic and military hub of its existence. It is used to provide protection for its forces, a house for its supplies, and it becomes a platform from which to expand power. To be effective the placement of the base has to consider a number of factors such as the geographical conditions in the area, the enemy's situation, the population, the ability to develop political power and mass, and the ease of putting a party type organization in the area. Most importantly, each base area has to be strong enough to withstand large-scale attacks without having to draw on the resources of other bases.[27] Once the base has been

established, the insurgents seek to use it as a springboard for expansion into the surrounding regions.

This method of expansion is often referred to, by Western analysts, as the "Oil Spot Strategy." This is a tactic used by both the insurgents and counterinsurgency forces as it recognizes that neither side has sufficient resources to secure the entire country at least during the initial stages of an insurgency. As a result, each side attempts to consolidate the areas that will protect their core support as they attempt to increase their authority outward from their bases.[28] In the insurgent's case, once the base was firmly established this growth could begin with the infusion of military operations that were focused on the expansion.

With regard to military operations, insurgents believed that the "object of war is simply to preserve oneself and to annihilate the enemy. To annihilate the enemy means to disarm them or to deprive them of the power of resistance, and not to annihilate them completely in a physical sense…"[29] In general, the insurgent's military operations are based on Ten Principles of War, these included:

1. Attack isolated enemy forces first, attack strong enemy forces later;
2. Take towns and rural areas first, take big cities later;
3. Wiping out the enemy's strength is the main objective, not seizing territory;
4. Only attack enemy forces that can be completely overcome;
5. Fight no battle you are not sure of winning;
6. Have courage in battle and no fear of sacrifice or fatigue;
7. Attack the enemy when he is on the move;
8. In cities, seize all weakly defended battlements; wait before attacking strong enemy lines;
9. Use captured arms and personnel to reinforce; and

10. Rest, train and consolidate in short intervals. The enemy should be permitted scant breathing space.[30]

Over time these principles have been distilled into a slogan, which became known as the famous four: "When the enemy advances, we retreat, When the enemy halts and encamps, we trouble them, When the enemy seeks to avoid battle, we attack and When the enemy retreats, we pursue."[31]

FIGHTING DOCTRINE OF THE INSURGENT

During the initial phases of an insurgency, non-state actors do not have the numerical or material resources to take on the military forces of an established authority directly. To overcome this problem, they have created a flexible, multi-tiered force structure that is based on regulars (the Army) and irregulars (guerrillas). These forces are trained and organized to eventually carry out three types of warfare. This includes guerrilla, mobile, and positional warfare. How they employ their forces and the specific type of warfare they use is based on the quality of the soldiers and equipment that is available.[32]

GUERRILLA WARFARE

Guerrilla warfare is a form of combat where small groups of irregulars used mobile tactics that are primarily based on ambushes and raids to attack larger and less mobile forces. Guerrillas often attempted to draw larger enemy units into unsuitable terrain in order to minimize their superior firepower and then used the ground, and the elements of surprise and mobility to attack their vulnerable points. Most non-state actors view guerrilla warfare as the war of the local population.[33]

Insurgents believe in the guerrilla's ability to wear down the enemy and accept the value of guerrilla units in providing local security, acting as scouts or watchers, and for gathering intelligence. However, within the construct of Hybrid War, the main operational roles of guerrilla units are confined to deterrent and harassment missions. This is due to the realization that despite their many benefits, guerrillas cannot achieve decisive results on the battlefield.[34] That being said, insurgents will integrate guerrilla warfare into their overall concept of operations. This is due to

the fact that the main advantage of guerrilla warfare is that it can be carried out by the people with very little training or equipment. However, in order to compensate for this weakness guerrillas are expected to use 'cunning' in their operations. In this regard, the essential requirements for successful guerrilla operations included the "retention of the initiative, alertness; and carefully planned tactical attacks."[35]

Insurgents recognize that they must form guerrilla units as early as possible. Ideally, this process will start during the initial stages of the "mobilization" process.[36] To this end, such units can be developed in the following ways:

1. From the general population;
2. From regular army units temporarily detailed for the purpose;
3. From regular army units permanently detailed;
4. From the combination of a regular army unit and a unit recruited from the local population;
5. From local militias;
6. From deserters from the ranks of the enemy; and
7. From former criminals and criminal groups.[37]

In the present hostilities, no doubt, all of these sources have been, and will be, employed.

Insurgents understand that creating guerrilla units is one thing but having them carry out effective operations is something quite different. They realize that success with poorly trained and equipped personnel is based on the quality of leadership that can be developed at the grassroots level.

In this respect, insurgents believe they need brave and positive men whose loyalty is dedicated to the cause."[38] For example, "An officer should have the following qualities: great powers of endurance so that in spite of any hardship he sets an example to his men and be a model for them; he must

be able to mix easily with the people; his spirit and that of the men must be one in strengthening the policy of resistance…" More importantly, "If he wishes to gain victories, he must study tactics." Mao believed, "A guerrilla group with officers of this caliber would be unbeatable."[39]

Despite the emphasis on leadership, cunning and detailed planning, the fact remains that successful guerrilla operations depend on two critical factors, first, they need the full support of the population they are securing and secondly, they need to have intimate knowledge of the terrain they are fighting on. When insurgents begin to expand their base, these advantages are no longer available to the guerrilla fighter.[40] As a result, guerrilla units tend to remain a local resource, but they do have strategic potential.

Although dated, Mao's concepts are timeless. In modern conflict, the strategic role of guerrilla warfare has two purposes. First, to support regular military operations. Second, to transform itself into a regular force. This is done by using the regular forces at the disposal of the non-state actor, and although this regular force could be used to carry out guerrilla warfare when necessary, its primary military focus needs to be on mobile and positional warfare or conventional military operations.[41]

MOBILE WARFARE

Insurgents view mobile warfare as the conduct of operations by large forces operating as self-contained organizations. Interestingly, the key characteristic of these operations is usually the absence of fixed battle lines or any type of established front line. As a result, "lines of operation" are usually determined by the direction in which the force is moving.[42]

Mobile warfare for non-state actors is often broken down into a series of distinct operations; these include active and passive defence, preparations for combating "encirclement and suppression" campaigns, strategic retreat, and strategic counter-offensive.[43] It is generally acknowledged that, while such operations can create the conditions for victory, they cannot in and of themselves achieve a real victory. This is because "to bring about victory or defeat a decisive battle between the two armies is necessary."[44] Thus, the end result of all mobile operations is the

complete destruction of large enemy forces through a "war of annihilation," or what is commonly viewed within Western literature as the decisive battle.

In order to achieve decisive battle, mobile warfare must be based on quick-decisions using offensives that operate on exterior lines within the framework of a strategy along interior lines.[45] To be successful such operations must employ forces that can operate over an extended and fluid front where the force has the ability to make swift advances and withdrawals, swift concentrations and dispersals.[46] Although these concepts may appear familiar to Western soldiers it is important to note that these ideas regarding mobile warfare diverge from the "Western way of war" in many respects.

This difference is especially relevant in the emphasis of time and space. In Western military thinking, the purpose of manoeuvre is to capture and hold ground; however, the non-state actor has no interest in holding territory outside their base area. In fact, time and space become important weapons rather than goals.[47] The idea is to use space to manoeuvre the enemy into a favourable position and then attack. In this respect, the principles of mobile warfare were similar to those of guerrilla operations. From a practical perspective, operational manoeuvre is not always possible, especially for a force that has spent much of its time on the strategic defensive. This means that the forces of non-state actors will have to transition into what is termed 'positional warfare.'

POSITIONAL WARFARE

Insurgents view positional warfare as a war of fixed lines similar in concept to the European "Way of War" during the First World War. In general, they are not particularly fond of this type of fighting. They believe that if one concentrates forces on a narrow front for a war of attrition, they would be throwing away the advantages of geography and economy of organization.[48] However, their view of staying away from positional warfare does not mean they abandon the idea completely.[49]

Insurgents recognize that these operations are important to defending key points or positions. Moreover, they are likely to become very prevalent

during the end of the third stage, where forces would have to attack the cities and other strong points of the established authority. Mao referred to this inevitability when he stated, "In this third stage positional warfare will undoubtedly play a greater role, for then the enemy will be holding fast to his positions, and we shall not be able to recover our lost territory unless we launch powerful positional attacks in support of mobile warfare."[50] It was for this reason that the concept has remained an important part of all contemporary non-state actor war. Daesh operations in Iraq and Syria provide a graphic example.

Although the theory of Hybrid War sounds straight forward, like all doctrines, its execution is less so. In reality, the progress of non-state actors will be extremely uneven. This is especially so during the strategic counter-offensive (the third stage) when the unevenness will often result in the third stage occurring in some areas while the second or first stage is happening concurrently in other regions. To overcome this problem, non-state actors will use the flexibility that is inherent in their eclectic force structure and their operational methods to optimize capabilities for each circumstance.[51]

COMPOUND WARFARE

This operational flexibility and how it was used by non-state actors is particularly important to understanding the underlying military success of contemporary Hybrid War. This is due to the fact that they believe that regular and irregular units are very complementary. In fact, Mao stressed, "Considering the revolutionary war as a whole, the operations of the people's guerrillas and those of the main forces of the Red Army complement each other like a man's right arm and left arm, and if we had only the main forces of the Red Army without the people's guerrillas, we would be like a warrior with only one arm."[52] Mao often grouped his guerrilla units with his mobile forces creating a synergistic effect. This phenomenon of using conventional and irregular forces against an enemy has been defined within the Western military context as compound warfare.[53]

Within the construct of Hybrid War, guerrilla forces provided important advantages over mobile forces. These included developing intelligence

information while suppressing the enemy's intelligence. Guerrillas can also provide supplies and quick passage through their territory, while denying this ability to their enemy.[54] Conversely, mobile regular forces also provide certain advantages to the guerrillas. For example, they often pressure the enemy to withdraw or force them into, or out of, areas where the guerrillas are operating, creating conditions for greater freedom of action.[55]

From an historical perspective, the synergy derived by combining regular and irregular operations makes compound warfare effective for smaller forces especially when they are operating over large areas or in difficult terrain. In this respect, many of today's armed non-state actors have both of these advantages and have used compound warfare as a combat multiplier to significantly enhance the overall flexibility and the effectiveness of their forces.[56]

THE ROLE OF ARMED NON-STATE ACTORS IN FUTURE WARFARE

The flexibility of the insurgents' fighting doctrine makes it a critical part of the armed non-state actor's doctrinal model for both proxy and conventional (compound) warfare. The current trend is for major powers to maximize the use of such forces in order to do as much of the heavy lifting as possible. This is done by supplementing these groups with special operations forces (SOF) and other specialists, who have access to Intelligence, Surveillance, Reconnaissance (ISR)/strike capabilities along with other types of selected conventional military support usually in the form of training, logistics, information/intelligence, and advance equipment. Examples of this pairing have been seen with the Russian use of these forces in the Crimea, Ukraine and Syria, as well as with the American use of similar forces in both Iraq and Syria. Given the increasing capabilities of such forces, it is likely their importance and influence will continue growing on both the irregular and conventional battlefields of the future.

More importantly, as the emphasis of conflict continues shifting towards a focus on social stability this type of conflict is likely to continue evolving with states employing various types of non-state actors to create civil unrest in an effort to undermine the position of the national

authority. In this regard, armed non-state actors will likely serve as part of the building blocks of a more modular and flexible state military doctrine that can allow such forces to be quickly integrated into SOF and conventional units.

In order to counter armed non-state actors that are using the insurgency model, it is important to understand that they are as much a political force as they are a military threat. As such, like any state use of hybrid or asymmetric warfare, they will focus their efforts at the strategic and tactical levels to circumvent the established authority's strength in military capability at the operational level. This will initially manifest itself with terror tactics aimed at undermining or destroying public confidence in the governing authority's control of the situation and direct attacks on its security forces. When armed non-state actors reach the point where they are openly displaying capabilities that directly challenge the operational level capabilities of a military force it is a sign that they are in a position of strength in relation to the established authority.

Defeating such forces militarily does little except to force them back into a guerrilla warfare posture so they must also be defeated politically. To defeat these forces as a political entity, they must be isolated from their base of support and from any external help they may be getting. If this cannot be done, victory cannot be achieved. However, if the armed non-state actors can be isolated politically, they can be defeated.

Fighting an insurgency against a sophisticated armed non-state actor is difficult in and of itself. Doing so while simultaneously dealing with coordinated cyber attacks, criminal activities, social conflict, and economic warfare, creates a situation that becomes increasingly layered with complexities. If one does not understand the different types and layout of the various battlefields they are fighting on, how does one hope to win?

In seeking to understand the concept of Hybrid Warfare's battlefields and what they might look like, one must comprehend the fact that although each battlefield is unique in terms of what it is trying to accomplish and where it is actually operating, they are all connected in terms of their strategic outcomes.

CHAPTER 4

UNDERSTANDING THE EXPANDING NATURE OF FUTURE BATTLEFIELDS

Major conflict in the future will witness potential adversaries attempting to counter Western military strengths by degrading or sidestepping key capabilities to gain advantages through the use of asymmetric strategies. Such actions will likely be integrated into political outcomes with the hope that they can be achieved before conventional Western military forces can react. If this cannot be done, adversaries will attempt to operate under the threshold that triggers a decisive counteraction, specifically a military response, for as long as possible. In order to counter such a strategy, the West will need to broaden its understanding and philosophy of war to include the utilization of other instruments of national power.[1]

The first step in this process is to conceptualize the idea of the future "battlefield of battlefields" and then to reconsider the expectations of military forces to accomplish specific national objectives.

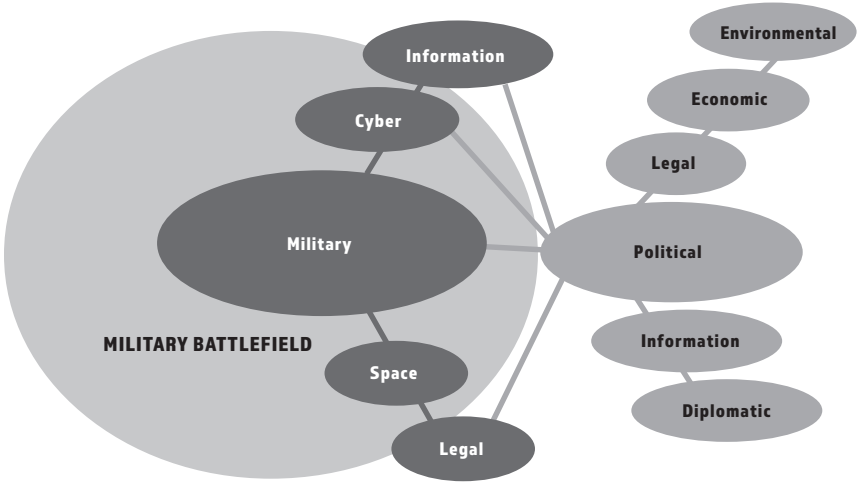
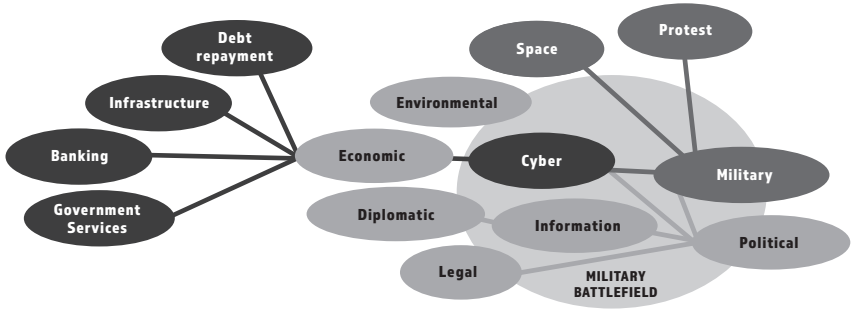


FIGURE 2: The Traditional Battlefield

Within the traditional Western view of war (Figure 2), the military is the preeminent instrument of national security. As such, political leaders pass various state capabilities over to the military in order to support or fight the battle(s). These capabilities are then employed within the context of the "military problem set" as viewed by commanders in order to achieve victory.

In this situation, the government is responsible for making sure that the military victory will produce, or advance, the strategic end-state it is seeking (i.e., its political objective(s)). Unfortunately, Western governments have not been particularly good at turning military victories into strategic success. This failure is due to a number of factors, not the least of which is the fact that the military may not be the best instrument of national power to use for a particular objective or problem, although, for many Western governments, it has certainly become the most convenient. Within the context of future war, potential enemies are attempting to de-emphasize the military option by placing it into a supporting role within a much larger political/national conflict. So, the question becomes, how must the West deal with the various battlefields that are now becoming available to a potential adversary?



In theory, the creation of the "battlefield of battlefields" would "reduce the impact of an overwhelming advantage in a specific (military) battlefield".

FIGURE 3: The "Battlefield of Battlefields"

In order to support a much larger political/national effort, the military battlefield of the past will become the "battlefield of battlefields" of the future, where national capabilities are employed by political leaders to achieve very specific strategic end-states/political objectives. In

fact, trends indicate that every effort will be made by peer and near-peer adversaries to reduce the military option as much as possible. In this respect, military force is only introduced when it is necessary to do so and in a measured amount for as little time as possible. In this sense, as displayed with Russian success in Crimea, victory is measured by how little military effort is actually needed to achieve the political result.

The key difference between the conventional battlefield (battlespace) of today and the future "battlefield of battlefields" is the integration of various state-controlled domains onto what has traditionally been the military playing field. This integration of national and military domains will serve to extend the modern battlespace in order to increase and better coordinate the effect and impacts. In addition to the traditional understanding of the military battlefield, national planners will also need to deal with the idea of the Strategic Effects Zones on both the friendly and opposition side. A linear visual representation of this concept is outlined in Figure 4 below.

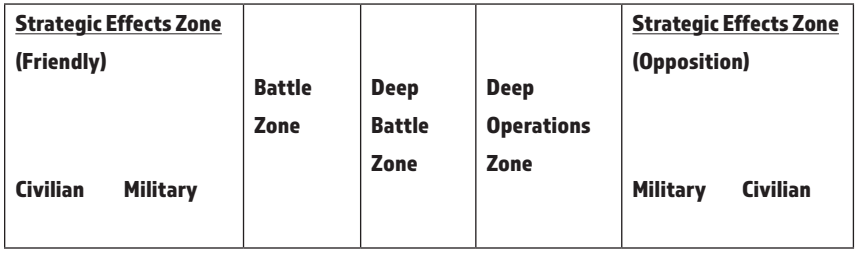


FIGURE 4: The Future Battlefield

At the tactical level, the Battle Zone and Deep Battle Zone will remain the military's primary domains as will, for the most part, the Deep Operations Zone. These are areas where direct military engagements will occur along with the shaping and exploitation battles to defeat the enemy's military forces should conventional operations become necessary. The Deep Operations Zone is the area designated for successive follow-on battles to occur if these are needed. It, along with the Strategic Effects Zone, will become the zones where proxy wars, diplomatic, economic, legal and environmental warfare, among other activities will be planned, monitored and played out.

Once a state of war has commenced, success in future conflict will depend on a nation's ability to coordinate the effects desired in the Strategic Effects Zone with ongoing military operations in the battle and operational zones. Prior to examining the specific zones in detail, it is necessary to examine some of the major developments that have influenced force structures, tactics and the design of the battlefields for tactical and operational success in the future.

CHAPTER 5

THE CHARACTER OF FUTURE WAR AND ITS BATTLEFIELDS

THE REVOLUTION IN MILITARY AFFAIRS

Despite the move towards fighting strategic campaigns and the use of the fuller range of national tools, Western nations will still need to rely on military forces to back up and support many of their initial efforts. However, once a certain level of support is reached, nations will likely transition from the competition phase to actual military operations. Once this has occurred the character of future military operations, between peer and near-peer adversaries, will be heavily influenced by the maturing technologies and doctrine changes that resulted from what some term the Revolution in Military Affairs (RMA), which occurred during the mid- to late-1990s.

Andrew Marshall, director of the Office of Net Assessments in the Office of the Secretary of Defense, defines a revolution in military affairs as "a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organisational concepts, fundamentally alters the character and conduct of military operations."[1] Within this construct of technological, doctrinal and organizational change, key technologies were beginning to mature to form the core of this process. In fact, some of these advancements initially started to make their appearance during the 1991 Gulf War.[2]

These technologies include precision-guided munitions (PGMs); intelligence, surveillance and reconnaissance (ISR); and advances in command, control, communications, computing and intelligence processing (C4I) power.[3] In order to take full advantage of these new developments, the Americans looked at a number of different concepts to exploit these advances during this period. According to Elinor Stone, a Canadian Defence Analyst, the overarching theme for many of these changes "was

a need to make the shift from the massive, heavy, armies of the Cold War, to lighter, and more deployable 'expeditionary' armies that would go to operational theatres around the world.''[4] Rapid deployability, she stated, ''would be facilitated in part through the application of new technologies to make military platforms lighter.''[5] She added:

> Mobility on the battlefield was another key doctrinal tenet of the RMA. Military operations, it was argued, would be characterized by highly dispersed forces facing no front line of ''enemy'' combatants. Soldiers would have to be able to move quickly to respond to rapidly changing situations. Battlefield mobility would be facilitated by the use of medium- or heavy-lift helicopters and, in some cases, combat helicopters, as well as the lighter ground force platforms.[6]

The concept that attempted to initially bring these ideas together was the American *Force XXI Operations*, a TRADOC pamphlet that came out on 1 August 1994.[7] This document describes the conceptual foundations for the conduct of future operations both in war and in operations other than war (OOTW). To achieve this goal, TRADOC envisioned a future force defined by five characteristics. These included:

1. Doctrinal flexibility;
2. Strategic mobility;
3. Tailorability and modularity;
4. Joint and multinational connectivity; and
5. Versatility to function in war and OOTW.

Doctrinal flexibility was designed to meet changes and challenges, as well as the diversity of tasks expected in the future. Strategic mobility focused on anticipation, pre-positioning, early entry, lightness, lethality, survivability, and investment in strategic lift. Tailorability and modularity were critical to the idea that Western armies would be required to be expeditionary forces. Moreover, in tight fiscal/deficit fighting environments there would be pressures to reduce funding, and as such, force deployments would need to be tailored according to the particular requirements of each respective contingency. This meant that joint, multinational, interagency connectivity; and, finally, versatility – resting on

a qualitative edge, would become the decisive determinants in both war and in operations other than war.[8]

Furthermore, an important feature of future joint and multinational operations was information flow. Doctrine writers envisioned including a "push-down" hierarchical command process combined with "pull-down" logistics and intelligence models. The new doctrine also envisioned integrated information systems that facilitated shared situational awareness, creating a "flatter" and more versatile organization.[9]

Another key concept that evolved from TRADOC's work was the idea of a "picture" (common operating picture) of the battlespace that stretched beyond the commander's traditional area of operations (AO). This conceptual battlespace represented the ability of the commander and his/her staff to visualize the AO and the way that forces would interact within this domain.

The common operating picture was important as it would greatly improve force-level dominance by enhancing situational awareness and ensuring rapid, clear communication of orders and intent, potentially reducing the confusion, fog, and friction of battle.[10] The idea of the battlespace as an operating picture would grow with the capabilities of future weaponry, which would facilitate "greater lethal reach and dominance. Deep reconnaissance and attack, force dispersion, power overmatch, precision fires, digitized sensor-to-shooter linkages, and force protection were keynotes."[11]

DEPTH AND SIMULTANEOUS ATTACK

Critical to maximizing these new capabilities and organizations was the idea of depth and simultaneous attack. In fact, the TRADOC document suggested a possible reassessment of the traditional fire and manoeuvre relationship in the "seamless" and simultaneous application of lethal power throughout the extended battlefield. This would be done with the aid of a new battle command system, employing digitized joint communications.[12] The document expounded on simultaneity by stating:

> RMA may transform the familiar form and structure of military campaigns as a chain of sequentially phased operations. Advanced

> forces will possess the capability to achieve multiple operational objectives nearly simultaneously throughout a theater of operations. This simultaneity, coupled with the pervasive influence of near-real-time military and public communications, will blur and compress the traditional divisions between strategic, operational, and tactical levels of war. We have seen simultaneity first attempted in Grenada, followed by use in Just Cause in Panama and Desert Storm against Iraq. During Desert Storm, no enemy force in the Kuwait theatre was safe from simultaneous attack. No enemy force began to move, however, until coalition ground forces attacked. Yet the coalition massed those land forces for only a short period to gain the strategic staying-power effect.[13]

TRADOC strategists believed that in order to dominate the extended battlespace an army required agile and robust deep and simultaneous attack capabilities. By combining the concepts of deep operations and simultaneous attack using both lethal and non-lethal means, one could create a dynamic capability to extend the battlespace in space, time, and purpose and thus reduce, or eliminate, the time and need to shape the battlefield. This would allow commanders to directly influence the enemy wherever they might be. The document states, "By massing the effects of long- and short-range area and precision fires, integrating information operations designed to blind, demoralize, and deafen the enemy, concurrent with rapid combined arms maneuver, ground and from the air, a larger and less agile enemy force can be quickly and decisively defeated."[14]

The ultimate goal of depth and simultaneous attack was to overload the enemy's ability to cope with the situation by presenting it with an overwhelming number of actions throughout the entire depth of its battlefield. The measure of success in executing depth and simultaneous attack was based on efforts to leverage emerging technologies in four general categories:

1. Battlespace preparation;
2. Synchronization;
3. Simultaneous attack execution; and
4. Force protection.

The TRADOC planners believed that for operations to be successful, force protection was critical against tactical and theatre missiles, as well as against enemy long-, medium-, and short-range rockets and ballistic missiles. They also insisted that effective air defence against such things as cruise missiles, unmanned aerospace vehicles (UAVs), and remotely piloted vehicles (RPVs) must be actively pursued.[15]

THE CHARACTER OF FUTURE COMBAT IN THE BATTLE AND DEEP BATTLE ZONES

The fighting forces for this concept would be modular and thus more mobile and agile. This would facilitate mission tailoring to meet each contingency.[16] To deal with the complexity of high technology and simultaneous attack, soldiers would need to be highly qualified, trained, and educated.[17] Moreover, they would need a new understanding of the tactical battlefield since they were no longer expected to just fight a contiguous linear style of operations typical of the Second World War, or those expected during the Cold War. Specifically, these tactical battlefields or AOs were identified as follows:

> **Contiguous Linear.** Linear operations in a contiguous AO typify sustained offensive and defensive operations against powerful, echeloned, and symmetrically organized forces. The contiguous areas and continuous forward line of own troops (FLOT) focus combat power and protect sustaining operations. Commanders normally shape the deep area, conduct decisive operation in the close area, and sustain in the rear area.[18]

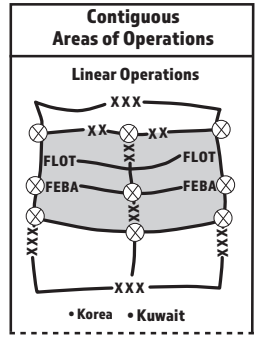


FIGURE 5: Contiguous Linear

Non-Contiguous Linear. In a non-contiguous linear (NCL) AO, the higher headquarters retains responsibility for the portion of its AO outside the subordinate unit AOs. The higher headquarters operational design uses non-linear operations while the subordinate units are conducting linear operations. The subordinate units' battlefield organizations have close, deep, and rear areas; the higher headquarters battlefield organization does not. This configuration might be appropriate when the higher headquarters is conducting widely separated simultaneous operations.[19]

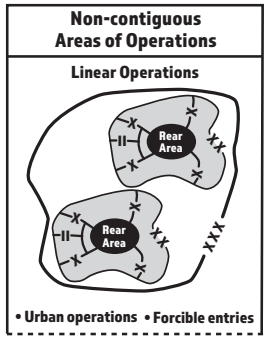


FIGURE 6: Non-Contiguous Linear

Non-Contiguous Non-Linear. In a non-contiguous, non-linear (NCNL) AO the operations of both higher and subordinate units are non-linear. The size of the land AO, composition and distribution of enemy forces and capabilities of friendly forces are important considerations in deciding whether to use this battlefield organization and operational design. In Somalia in 1992, for example, [the American] Army conducted non-linear stability operations and support operations in widely separated AOs around Kismayu and Mogadishu.[20]

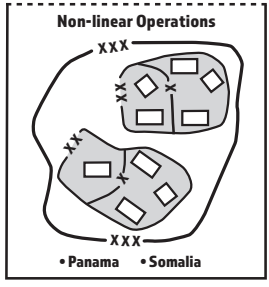


FIGURE 7: Non-Contiguous Non-Linear

Contiguous Non-Linear. Figure 8 illustrates non-linear operations being conducted in contiguous AOs. This combination typifies stability operations, such as those in Haiti, Bosnia, and Kosovo. Hurricane Andrew support operations also followed this design. The higher headquarters assigns the responsibility for its entire AO to subordinate units. Within the subordinate AOs, operations are non-linear, with the subordinate headquarters receiving support and resources from the higher headquarters. On a tactical scale, search and attack operations are often non-linear operations conducted in contiguous AOs.[21]

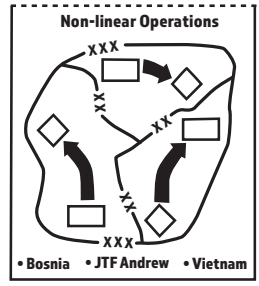


FIGURE 8: Contiguous Non-Linear

With the modular force structure and a refocus on more fluid operations within and through the different types of battlefields, a change in war-fighting techniques was needed. This change occurred in the form of distributed operations.[22]

DISTRIBUTED OPERATIONS WAR-FIGHTING CONCEPT

The distributed operations war-fighting concept was released by the United States Marine Corps (USMC) in April 2005. It was subsequently adopted in various forms by the American Army and other Western nations. The concept was designed to deal with adaptive enemies operating in a more complex environment by providing conventional forces the ability to decentralize both decision-making and force distribution as necessary. More importantly, distributed operations would provide commanders with the ability to employ tactical units across the entire depth and breadth of the non-linear battlespace, which was a key requirement of Force XXI operations. As the Marine concept paper explained:

> Distributed Operations describes an operating approach that will create an advantage over an adversary through the deliberate use of separation and coordinated, interdependent, tactical actions enabled by increased access to functional support, as well as by enhanced combat capabilities at the small-unit level. The essence of this concept lies in the capacity for coordinated action by dispersed units, throughout the breadth and depth of the battlespace, ordered and connected within an operational design focused on a common aim.[23]

At the tactical level, distributed operations envisioned manoeuvre units operating within a disaggregated fashion. Companies, platoons, and sections could disperse beyond the range of mutually supporting organic direct fires, but be linked through a common command and control network. To do this, units needed to be organized, trained, and equipped to facilitate such operations, which meant, particularly at the lower levels of command, they would need a host of new equipment and training. The trade-off would be to reduce their vulnerability to enemy observation and fire. However, with all these changes they still needed to possess significant combat power to close with and destroy the enemy.[24]

To maintain the ability to destroy the enemy or support other missions, distributed units also required the capability to rapidly re-aggregate.[25] This ability to distribute and aggregate would provide commanders with the capacity to operate using the fuller range of tactical employment methods that were complementary in character. For example, the concept envisioned sea-based forces projecting power using ship-to-objective manoeuvre in an aggregated fashion while being complemented by additional units using distributed operations.[26]

It was recognized that distributed operations were most effective if units were networked, which provided commanders with a means of dealing with ambiguity in the battlespace environment. Employed properly, they would present the enemy with a complex puzzle. Their relative mobility, situational awareness, and modular structure would enable rapid adaptation and self-reorganization, presenting the opponent with a greater degree of uncertainty regarding locations, intentions, and objectives. This complexity was designed to induce confusion and ambiguity.[27] The

key to rapid adaptation and self-reorganization was the ability to transition as quickly as possible within a modular force structure.[28]

With the emergence of peer and near-peer adversaries, many of these concepts will remain valid for high-intensity combat operations into the foreseeable future. In fact, the increased sophistication in ISR/strike capabilities, proliferation of UAVs, and RPVs in the Russian/Ukraine war and the addition of significantly more firepower from modern systems will likely force greater dispersion on the battlefield than originally envisioned. However, the modular force structure of today will require an extensive overhaul if it is to remain relevant on the future battlefield.

MULTI-DOMAIN BATTLE

In addition to reviewing its force structure the American Army was also constantly reviewing its war-fighting doctrine and equipment needs. In February 2017, TRADOC published a White Paper entitled, *Multi-Domain Battle: Combined Arms for the 21st Century*.[29] The document started the process of debate regarding the future direction of this new war-fighting concept. It acknowledged that recent operations undertaken by both Russia and China have displayed capabilities that now threaten Western Joint Force interdependence by turning long-assumed Western strengths into weaknesses. It observed that "over the last 25 years, assumptions of air, land, maritime, space, and cyberspace domain superiority drove the doctrine, equipment, and posture of U.S. and Western forces."[30] The document also conceded that these assumptions are now proving to be invalid in light of recent changes to potential adversary capabilities, capacities, and approaches.[31] As a result, the White Paper contends that Western forces can no longer assume continuous superiority in any domain.[32] To this end, it asserts that a new approach to war-fighting is needed.

Based on recent experience, particularly from Russian operations, the White Paper postulates that Western forces will likely "confront sensor-rich militaries of peer states and proxies who will employ precision-guided munitions that will make modern battlefields highly lethal and restrict Joint Force freedom of manoeuvre and action. To do this, potential adversaries are in the process of countering Western strengths such as air and maritime superiority, while degrading key capabilities by limiting access to space, cyberspace, and the electromagnetic spectrum."[33]

As a result, the American Army and its Western partners now face the possibility of the loss of Western superiority in both methods and material. The White Paper reveals:

> Potential Adversaries have combined new operational methods with modernized capabilities. For example, ground formations of top tier competitors now have parity or overmatch with Western forces in many weapons systems' range, lethality, protection, and mobility. The latest generation of Russian and Chinese combat vehicles and artillery offer equivalent and, in some cases, superior protection, range, and lethality to U.S. … fighting vehicles, and indirect fires systems. These developments in ground systems match similar qualitative improvements in enemy air, maritime, space, and cyberspace capabilities.[34]

This revelation has forced the Americans to reduce expatiations on the future battlefield. To this end, the document suggests, "Implementing Multi-Domain Battle entails three components: creating and exploiting temporary windows of advantage; restoring capability balance by building flexible, resilient formations in the Joint Force; and altering force posture to enhance deterrence."[35] Another key component of Multi-Domain Battle is the fact that the Americans are attempting to integrate all military domains (Air, Land, Sea, Space, Cyber, Information, and SOF) into a cohesive fighting doctrine/domain based on a known threat.

Although, *Multi-Domain Battle* appears to be headed in the right direction, historically a key weakness of Western doctrine has been a focus on the tactical battle and a corresponding lack of integration between tactical, operational and strategic outcomes. With *Multi-Domain Battle*, such integration will be critical to success as key capabilities within many potential domains (e.g., informational cyber, economic, and space) are also controlled by state organizations and agencies outside of the military's control.

As major competitors have already started a move towards a strategic doctrine of conflict, any lack of integration by Western governments between their military forces and other state tools will be a critical and possibly even fatal weakness in future conflicts. With this in mind,

it is now important to look at the foundation battlefields of the Deep Operations Zone, and the Strategic Effects Zone in more detail.

THE DEEP OPERATIONS ZONE

For the purpose of Hybrid Warfare, the Deep Operations Zone is the area between the Battle Zone/Deep Battle Zone and the Strategic Effects Area. It is based on the idea that defeating peer and near-peer adversaries will likely require a succession of battles that move beyond the tactical focus of the immediate battle and Deep Battle zones. This is done by allowing military forces to carry out exploitation operations after the initial defeat of an enemy force has occurred. More importantly it serves as an intellectual link between tactical operations and the operational objectives that produce strategic outcomes. For example, the Russian view of this concept evolved from a two-phased approach that included the tactical deep battle, followed by deep battle operations.[36]

Deep Battle was designed to break the enemy's forward defenses, or tactical zones, through a massive initial combined-arms assault. Any breakthrough or penetration would be exploited by Russian follow-on mobile reserves that would drive towards the strategic depth of an enemy. Operations were supported by air forces, airborne forces and ground forces in order to create a "simultaneous blow throughout the entire depth of the enemy's operational defense."[37]

The purpose of such operations was to inflict a decisive defeat on the enemy's logistic capabilities, its command-and-control nodes, as well as to delay, disrupt, and defeat any reserves positioned in the specific area of operations being attacked. In order to move into the rear areas as quickly as possible, Russian offensive forces were required to surround enemy units holding their front-line positions to allow the exploitation forces to surge into the defender's operational and strategic depth.[38] Ideally, this would be in the form of a pursuit. However, it could also be completed in the form of a series of successive battles.

In future conflict, Western militaries will need to adopt similar tactics and engage their enemy in the Deep Operations Zone to achieve the same intended results. However, the major difference will come from how the

exploitation and deep penetration tasks are accomplished. This requirement is due to the fact that dispersed enemy peer forces are unlikely to be decisively defeated in a single major engagement confined to the local battle and Deep Battle zones. As such, future Joint Forces must plan for the possibility of having to engage, push back or bypass enemy forces within the depth of the enemy's Deep Operations and possibility into its Strategic Effects Zone.

Although, military operations in the Deep Operations Zone will be critical for eventual military success on the main battlefield, the difficulty with entering this zone of peer and near-peer adversaries' defence is that successive advances or battlefield victories increase the likelihood of triggering a limited or full nuclear attack and/or exchange. This result is likely to occur when one side or the other feels it is losing the initiative or is threatened with total defeat.

Within the holistic view of the future battlefield, it is important to note that the Deep Operations Zone also provides an intellectual focal point of transition between the tactical and operational battle, which is critical to reaching a strategic military end-state. More importantly, it provides a link from the military battlefield to the national Strategic Effects Zone where such things as diplomatic, economic legal and environmental warfare, among others will also be played out.

STRATEGIC EFFECTS ZONE

In future conflict, the Strategic Effects Zone will become the main focus of national operations against peer and near-peer adversaries. As the aim of future conflict is to induce social chaos leading to a political crisis and defeat, the military will only be used when and if necessary to support the other national efforts. As a result, the Strategic Effects Zone becomes the main battlefield within the conflict where operations directly or indirectly target the critical instruments of the enemy's national power.

Historically, Western nations have attempted to achieve these strategic results, primarily by military means, through the use of such things as naval blockades to restrict vital resources entering the country or airpower that directly attacks the enemy's infrastructure in its rear area/

homeland. For air campaigns, emphasis was usually placed on the specific destruction of infrastructure directly supporting the war effort or of high political significance.

However, despite massive efforts and great destruction, it was often difficult to determine how much a strategic bombing campaign can or will actually contribute to eventual victory.[39] In an effort to bring more precision to this form of attack, Colonel John Warden, an American Air Power theorist during the 1991 Gulf War, advanced the idea of the enemy as a system that has an organization.

Warden postulated that, like all organizations, an enemy's is based on certain principles that can be clearly identified and attacked. He asserts, "Whether we are talking about an industrialized state, a drug cartel, or an electric company, every organization follows the same organizational scheme." The idea was to identify and target centers of gravity within the organizational scheme until the enemy submitted to your will. He explained, "As we understand how our enemies are organized, we can easily move on to the concept of centers of gravity. Understanding centers of gravity then allows us to make reasonable guesses as to how to create costs which may lead the enemy to accept our demands."[40]

In order to better articulate his idea, Warden represented the enemy system organization in a concentric rings format, with each ring representing a layer of the enemy's center of gravity. The priority of effort he emphasized was in descending order of importance starting with the inner most rings and working out. This included leadership, system essentials, infrastructure, population, and the military. He viewed the leadership ring as the most important and focused on the state's leaders as they control the systems of the state. System essentials represent key production critical to the state's survival, such as oil, food and money. Infrastructure, transportation, and electricity keep the system together. The population is the state's civilian population, and a fielded military is the security mechanism that defends the state from attack.[41]

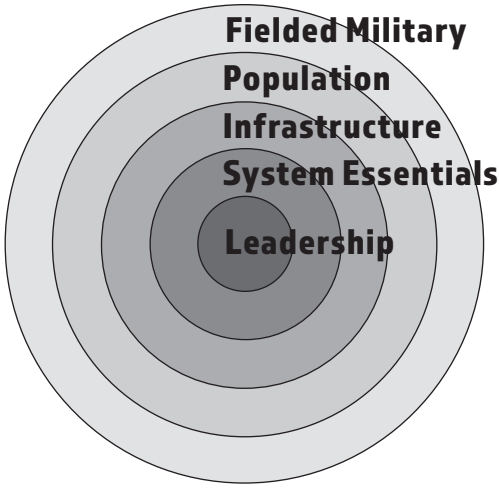


FIGURE 9: Warden's Concentric Ring Format

As the object of war is to force your will onto the enemy, Warden felt that the most effective and quickest way to achieve this was through a simultaneous attack on all of the components of the enemy's inner ring or its leadership. Only if one was unable to attack an enemy's leadership does Warden recommend attacking, in ascending order of importance, the latter or outer rings.[42] Although there has been a great deal of debate regarding the validity of the model and the actual effects it achieved in defeating the enemy during the Gulf War, it did attempt to identify and prioritize strategic targets in a systemic way. This is important, particularly when one examines what constitutes a strategic attack.[43]

The difference between Warden's model and the concept behind "Unlimited Warfare" or "New Generation Warfare" is that with this form of warfare, the idea is to target the population in such a way that it forces its leadership to seek a solution to the problem, preferably by stopping the conflict altogether. In this respect, under Warden's construct, all the rings must play their role. However, the population and its leadership, not the destruction of infrastructure, becomes the primary focus of attack.

The remaining rings are used to assist in the process based on the perceived weaknesses of the target country. This means that once identified, there should be a simultaneous attack on all rings including the center of

gravity, but in a way that will influence the population and its leadership. Moreover, this needs to be done within the context of the "battlefield of battlefields" or multi-domain approach.

The problem with this approach is that this is not always as simple as it sounds. This is due to the fact that the population and its leadership must be viewed within the context of the other elements of national power. According to David Jablonsky, a professor of National Security Affairs, Department of National Security and Strategy at the U.S. Army War College, "Most scholars focus on power as a means, the strength or capacity that provides the ability to influence the behavior of other actors in accordance with one's own objectives."[44] He adds, "National power is historically linked with military capacity, a natural relationship since war in the international arena is the ultima ratio of power."[45] However, he cautions, that one element of power on its own cannot in itself determine national power. He states, "In this context, the elements of national power, no matter how defined, can be separated only artificially. Together, they constitute the resources for the attainment of national objectives and goals."[46]

THE ELEMENTS OF NATIONAL POWER

Jablonsky breaks down the elements of national power between natural and social determinants of power. "The natural determinants (i.e., geography, resources, and population) are concerned with the number of people in a nation and with their physical environment. Social determinants (economic, political, military, psychological, and, more recently, informational) concern the ways in which the people of a nation organize themselves and the manner in which they alter their environment."[47] The problem when isolating and attacking an enemy's different elements of national power, as in Warden's theory, is that one element like leadership is difficult to separate from the others, as all are intertwined and it is this interconnectedness that creates national resiliency. As Jablonsky points out, in practice, it is impossible to make a clear distinction between the natural and social elements of power.[48] For example, "resources are a natural factor, but the degree to which they are used is socially determined. Population factors, in particular, cut across the dividing line between both categories. The number of people of working age in the

population affects the degree of industrialization of a nation, but the process of industrialization, in turn, can greatly alter the composition of the population."[49]

BREAKING THE NATIONAL WILL

Historically, strategic military attacks by Western countries on their enemies have focused primarily on the physical destruction of critical infrastructure, resources, the population, as well as political, and military capabilities. Information and economic warfare have been centered on the population, including military personal and politicians through the use of psychological operations. The problem with such attacks has been that despite great physical destruction, the resiliency of the society has continued to survive within the national structure. For example, allied strategic bombing of Germany during the Second World War was based on a policy of "area attack" which meant that the primary objective was to attack "the morale of the enemy's civil population and in particular, the industrial workers."[50] The idea was that bombing raids would destroy Germany's factories and surrounding residential areas. It was believed that such attacks would "force Germany to reallocate resources, overwhelm the civilian sector, and eventually destroy the German war machine while breaking the morale of the German people."[51] Unfortunately, for the Allies, despite great physical damage, the morale of the German people remained intact. According to Ryan Patrick Hopkins of East Tennessee State University, "In fact, it angered the populace, possibly explaining why the Germans continued to fight on for months, even as it became increasingly obvious that the Germans were going to lose the war."[52]

In order for such attacks to work one must not only attack each of the natural and social determinants but do so in a coordinated way that will break down the resiliency of the society through its population. However, this can often take a great deal of time and effort. The key is to find the right set of conditions to start and then accelerate the process when and if it is needed.

That is why some countries in Europe are seeing ongoing information and disinformation campaigns being pushed by the Russians. The Russians are trying to prioritize their national set of "tools" for strategic attack

by focusing assaults on the population, specifically towards the psychological and political components of national power. The other elements of national power are attacked usually when there is a clear weakness and it is opportunistic to do so. Starting such strikes before an apparent increase in inter-state tensions allows a possible opponent more time to wear down that social resilience. Using non-state actors to conduct confrontations against minorities within the target country is another.

By attacking the strategic zone of a democratic country, an opponent attempts to exploit the very fabric of democracy by using its own strengths (e.g., freedom of expression/speech, protest) against itself. This is possible because democratic countries need strong and independent government institutions to provide the necessary checks and balances in order to prevent the concentration of power. However, it is this independence of different levels of government and governmental departments that hinders intergovernmental cooperation for any extended period of time. Real cooperation, when it does happen, usually only occurs during a national emergency.

Once the emergency is over, organizations within the government structure see little value in continuing cooperation as they compete for resources, relevance and influence. It is this inability to work together during non-crisis periods that doctrines such as "New Generational Warfare" or "Unlimited War" attempt to exploit. They do this by driving wedges between the governmental institutions and into the checks and balances within a democracy. In the process, they strip away the layers of national resiliency by creating or expanding on discontent, thereby preventing effective government response to crises as they arise. Ultimately, the aim of such actions is to separate the people from their government.

In this respect, the specific "battlefield of battlefields" that is used is target country-dependent and will need to adjust with the changing situations of that targeted country. It is this specific-to-situation analysis and coordination at the strategic level that has made Russian & Chinese successes so quick and efficient thus far. For their part, the Russians are moving quickly towards achieving a single full-depth, synchronized action across the entire "battlefield of battlefields" that

could cause paralysis to Western countries and their militaries. It is important to remember that the preparations for and specific activities related to this form of conflict are likely occurring right now. For example, interfering in American and other Western nations' elections are only the beginning of what is yet to come.

CHAPTER 6

TOWARDS A TEMPLATE FOR HYBRID WAR

If specific activities relating to Hybrid Warfare are currently being carried out by peer and near-peer adversaries, what should authorities be looking for that could indicate a possible attack? The main problem with detecting these attacks is that once they initially begin it can be difficult to attribute them as a systematic attack, as they could simply be a series of isolated incidents.[1] Fortunately, we do have a template that can put these activities into context.

The Russian version of Hybrid Warfare was first introduced to the public in a paper published by General Valery Gerasimov, the Chief of the Russian General Staff, in February 2013.[2] In it, Gerasimov lays out the key principles behind Russia's thinking on the possibilities of this type of warfare. The first is the idea that the world is now in a continual state of conflict. He states that "in the 21st century we have seen a tendency toward blurring the lines between the states of war and peace." He adds, "the conduct of wars has changed as they are no longer declared and, having begun, they move in different and unfamiliar directions."[3] Gerasimov asserts, "This unfamiliar template refers to asymmetrical operations using a host of [strategic] capabilities" to "nullif[y]… an enemy's advantages in armed conflict."[4]

Gerasimov believed that the specific capabilities needed to effect change on the ground would include the extensive use of Special Forces linking up with internal opposition groups within the target country to create an operating front that would eventually extend throughout the entire depth of the enemy's territory. These actions would be combined with information operations, cyber warfare, legal warfare, economic war and other state-level activities that were linked to a strategic outcome. Specific activities would be constantly modified to meet the needs of a particular operation.[5]

The Russians deem that such methods, employed and sequenced properly, could, in a very short period of time, throw a stable and thriving state into a web of chaos, humanitarian upheaval, and outright civil war, making it susceptible to foreign intervention.[6] Although Gerasimov acknowledged that such events were not traditionally part of what would be considered wartime activities, he believed that they will now become typical of conflict in the 21st century.

The idea of collapsing a state onto itself through social upheaval, before a declaration of war was declared, was an important part of Hybrid Warfare's underlying methodology. Gerasimov stated, "The very "rules of war" have changed…[as] the focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other non-military measures — applied in coordination with the protest potential of the population."[7] The example he used to illustrate his point was NATO's role in Libya, where a no-fly zone and naval blockade were combined with the use of private military contractors working closely with the armed formations of the opposition.[8]

Gerasimov understood that new information technologies have allowed much of this change to occur. As a result, the information space has opened the door to the widespread use of asymmetrical possibilities for reducing the fighting potential of the enemy, particularly through the use of influence operations.[9]

Jānis Bērzinš, Managing Director for the Center for Security and Strategic Research at the National Defense Academy of Latvia, emphasized this specific point. He affirms, "The Russians have placed the idea of influence operations at the very center of their operational planning and use all possible levers of national power to achieve this."[10] He adds that the Russians, "have demonstrated an innate understanding of the key target audiences and their probable behavior… Armed with this information they knew what to do, when and what the outcomes are likely to be."[11]

The Russians felt these changes reduced the importance of frontal engagements by large conventional military formations, which they believed were gradually becoming a thing of the past. This transition is due to the fact that even if conventional operations are required to finish off the

enemy this will be done primarily by using standoff operations throughout the depth of an enemy's territory.[12] The Russians believed this shift towards irregular war and standoff operations was blurring the lines between the strategic, operational, and tactical levels, as well as between offensive and defensive operations.[13]

According to Gerasimov, this new doctrine manifests itself in the use of asymmetric and indirect methods along with the management of troops in a more unified informational sphere.[14] Should the conflict need to escalate, these activities would be followed by the massive use of high-precision weapons, special operations and robotics. This assault would be followed by simultaneous strikes on the enemy's units and facilities with battle on land, air, sea, and in the informational space.[15]

In writing about the Russian approach to modern warfare, Bērziņš articulated these ideas, into what has become known as the eight phases of Hybrid Warfare. As such, they provide a good template for understanding how peer nations, using such a doctrine, might conduct state-level operations in the future. They are as follows:

- **First Phase**: deals with non-military asymmetric warfare (encompassing information, moral, psychological, ideological, diplomatic, and economic measures as part of a plan to establish a favourable political, economic, and military setup);

- **Second Phase**: [specific] operations are used to mislead political and military leaders by coordinated measures carried out by diplomatic channels, media, and top government and military agencies. This is done by leaking false data, orders, directives, and instructions;

- **Third Phase**: is focused on intimidation, deceiving, and bribing government and military officers, with the objective of making them abandon their service duties;

- **Fourth Phase**: destabilizing propaganda to increase discontent among the population, this is boosted by the arrival of Russian bands of militants, escalating subversion;

- **Fifth Phase**: establishment of no-fly zones over the country to be attacked, imposition of blockades, and extensive use of private military companies in close cooperation with armed opposition units;

- **Sixth Phase**: This phase deals with the commencement of military action, which is immediately preceded by large-scale reconnaissance and subversive missions. This includes all types, forms, methods, and forces, such as special operations forces, space, radio, radio engineering, electronic, diplomatic, secret service intelligence, and industrial espionage;

- **Seventh Phase**: combination of targeted information operations, electronic warfare operations, aerospace operations, continuous airforce harassment, combined with the use of high precision weapons launched from various platforms including (long-range artillery, and weapons that are based on new physical principles, such as microwaves, radiation, non-lethal biological weapons); and

- **Eighth Phase**: roll over the remaining points of resistance and destroy surviving enemy units by special operations conducted by reconnaissance units to spot which enemy units have survived and transmit their coordinates to the attacker's missile and artillery units; fire barrages are used to annihilate the defender's resisting army units by effective advanced weapons; airdrop operations to surround points of resistance; and territory mopping-up operations by ground troops.[16]

Each of these phases can occur in sequence or simultaneously depending on the specific situation. Regardless of the actual tools being employed, this template manifests itself by using asymmetric or indirect methods within a unified informational sphere.[17]

As a result, peer and near-peer adversaries would likely employ private military and security companies, criminal organizations or Special Forces to further develop their operations. This could include creating or enhancing discontent among the population, conducting sabotage

operations and preparing a framework for the start of conventional military operations to occur. Moreover, these organizations would likely link up with internal opposition groups within the target country. Regardless, based on the specific phase being employed, activities would focus on achieving the following outcomes:

- gain physical or cyber control over critical infrastructure, including government and military systems;
- employ Information Operations (Information War) against target nations and target groups;
- use criminal organizations or private security companies to carry out intelligence, the movement of weapons, and strategic level espionage or sabotage if this were to become necessary;
- conduct cyber-warfare including espionage, denial-of-service (DoS) attacks, data modification and infrastructure manipulation;
- employ Airborne or Special Forces to carry out attacks on infrastructure or to create discontent among indigenous peoples and other minority groups; and
- employ conventional military forces to provide support for ongoing operations by Airborne or Special Forces, criminal organizations, private military and security companies and for intimidation.[18]

From a threat perspective, it is important to understand that peer and near-peer adversaries now have the ability to circumvent vast distances and strike directly at the heart of a target nation's critical infrastructure and public confidence while provoking internal tensions. Moreover, they can do this, in most cases, without their military forces entering a country or resorting to a formal declaration of war.

If Western nations are to effectively deal with this threat, they will need to address the security issues specific to the application of this new type of warfare. This includes preventing peer and near-peer adversaries from acquiring the target nation's companies and infrastructure, monitoring

operations by possible surrogate organizations, and countering a likely information or cyber warfare attack. Let us look at each of these in a little more detail.

Cyber Warfare – A central component of a Hybrid War is cyber warfare. Long before any increase in tensions occurs, peer nations will attempt to infiltrate Western government organizations, research institutes, armed forces, energy distribution facilities, telecoms companies, financial services, and logistics management capabilities within the cyber domain.[19] In addition to carrying out espionage, specific cyber activities could include such things as propaganda, and sabotage in the form of denial-of-service attacks, data modification and infrastructure manipulation.[20]

Should peer nations decide to launch an all-out cyber attack against a Western nation, they will likely hit banking, government, media outlets and other targets that rely heavily on the digital medium to function. The primary method of assault will be a series of denial-of-service attacks that could result in shutdowns to many of these essential services.[21] Also at risk is the internet infrastructure, along with government ISP addresses, which will be hit in an attempt to disrupt communications between government agencies and the various levels of government.[22]

Information War – Another key component of this strategy is the employment of "information war." Peer and near-peer adversaries view these operations in a holistic manner and as such they encompass a wide range of activities including cyber operations, electronic warfare, psychological operations, and influence operations.[23] As a result, information war not only deals in disinformation campaigns that could contain such things as half-truths and leaks, it actively attempts to reinvent reality in an effort to shape the global narrative.[24]

To reach global opinion, the peer nations are very active on social media. For example, the BuzzFeed website recently reported that the Russian government is recruiting large numbers of online trolls in an effort to change global sentiment regarding the invasion of Ukraine.[25] These trolls are currently driving discussions on many of the principal Western online media outlets, including "Fox News, Huffington Post, The Blaze, Politico, and WorldNet Daily."[26] Such activities are intended

to get Russia's message out while creating confusion and uncertainty within the targeted community.

Should peer and near-peer adversaries decide to unleash an information campaign against a country, it will be a coordinated effort using psychological and influence operations. They will attempt to capitalize on internal tensions between regions, provinces, states, religions, and ethnic groups. The main focus of any campaign will be to isolate different groups within a country from its government while attempting to disrupt the public's confidence in the ability of its elected officials to deal with the situation effectively or to protect them should a confrontation escalate.[27]

The Acquisition of Private or Public Companies – Peer and near-peer adversaries will also attempt to penetrate established companies within a target nation, likely through full or partial commercial acquisition. According to Andrew Davenport, Deputy Executive Director of PSSI in Washington, "Russia makes significant use of its State-Owned Enterprises for strategic purposes, pursuing key roles in the energy sectors and power production industries of target countries…"[28] Such control will allow them to use these assets to pressure decision-making, engage in economic warfare, or simply give them a bargaining tool against a government should an appropriate situation arise. This use of acquisition for economic and political influence means that a government must be cautious about what it allows any foreign power to acquire, particularly regarding resources and critical infrastructure within the country.

Surrogate Organizations – Another aspect of Hybrid Warfare's operational approach is the use of surrogate organizations to do much of the peer and near-peer adversaries' dirty work. In this regard, there are two specific threats to the West that must be monitored, Private Military and Security Companies (PMSCs) and criminal organizations.

There has been speculation that the Russians have used criminal organizations to perform various tasks in Eastern Ukraine. For example, Tom Porter, writing for the *International Business Times,* stated, "It is alleged that Russian organized crime figures have served as agents for Russia in east Ukraine, where they have been used to foment pro-Russian unrest, and transport arms and supplies to rebel groups."[29] José Grinda González,

a Spanish prosecutor who has spent a great deal of time looking into the activities of Russian organized crime in Spain reinforces this claim. He believes Russian spies often use senior mafia bosses to carry out criminal operations such as arms trafficking. He states that "Law enforcement agencies such as the police, spy agencies and the prosecutor's office operate a de facto protection racket for criminal networks."[30]

The close relationship between peer and near-peer adversaries' government and crime organizations means that as these countries expand their commercial interest and presence around the world, so to will their organized crime networks. More importantly, as organized crime becomes more established in a target country, their Security Services will have a direct link to a possible pool of contractors already operating within the country. As a result, these gangs have moved from a purely criminal justice problem to a national security threat and both government and law enforcement must be extremely vigilant regarding these organizations and their activities within the West.

An emerging international security threat will have to be dealt with is the deployment of peer nation PMSCs. For example, the Russians have been monitoring the employment of Western PMSCs in Iraq and Afghanistan for some time and are keen to start providing similar services.[31] Once in operation, this capability will likely become an increasingly important part of "New Generation Warfare" doctrine. As Dr. Mark Galeotti of *In Moscow's Shadows* points out, "The Kremlin regards all Russian companies and institutions–and especially those owned, backed or facilitated by the state–as potential tools at its disposal."[32] He states, "Gazprom turns off the taps when there is a need to squeeze a neighbor; arms companies flock to do deals with despots the government would support…" He goes on to say, "Russia's PMSCs would no doubt be expected to act at the Kremlin's behest when need be."[33] Galeotti concludes his assessment of PMSCs by stating, "The employment of these companies is 'neither the soft power of influence and authority, nor the traditional forms of hard power,' this would be a kind of 'elastic power'–flexible much of the time, but surprisingly tough and painful when wielded with intent."[34]

Employing PMSCs to protect the interest of national owned companies would be viewed by many as nothing out of the ordinary. However,

these companies usually employ members with specialized military backgrounds and they could be used by the governments of peer and near-peer adversaries to carry out missions ranging from reconnaissance and sabotage on critical infrastructure, to providing assistance to resistance groups or criminal organizations. Because the PMSC personnel are actually working for commercial enterprises, peer nation governments have a built-in plausible deniability should they be apprehended.

PART I SUMMARY

In summary, peer and near-peer adversaries are seeking to move the center of gravity for conflict from the operational level where conventional military forces played a predominant role, into the strategic realm where the integration of strategic planning and the coordination of state tools becomes the critical denominator. This coordinated action is achieved by converging different methods, battlefields, and force structures so that they are blurred into a single entity operating within the same battlespace and where the irregular component (e.g., insurgents, agitators, protesters) within this combined action may prove to be operationally decisive.

This idea of conflict originates from the Chinese idea of creating the "extended domain." This is done by integrating information from an opponent, such as their national interests and national security requirements, and mapping any vulnerabilities onto a larger "strategic situation map" that allows for the creation of a holistic strategy to attack the opponent. Once the strategy is mapped out, the product allows for engagement across the entire "battlefield of battlefields." If the strategy is coordinated correctly, the methodology allows for a reduction in the impact of the West's overwhelming advantage in conventional military operations.

This is no longer simply conjecture. The Russian have already shown that they are well on their way to developing this concept in the form of "New Generation Warfare." Based in part on the theory of "Unlimited Warfare," they will become increasingly effective over time, as experience creates sophistication of both process and capabilities.

PART II

CASE STUDIES IN THE EMPLOYMENT OF HYBRID WARFARE

INTRODUCTION TO PART II

Hybrid Warfare, carried out by peer and near-peer adversaries, is nothing new. In fact, it has been around in various forms for some time. However, what makes this current iteration different and far more effective than has previously been the case, is that fact that many more tools are being employed simultaneously, within the context of a unified informational sphere. Common practice for this type of warfare is to start the process with an assortment of non-military weapons. This includes things such as information, moral, psychological, ideological, diplomatic, and economic measures as part of a larger plan to establish favourable political, economic, and military conditions or to create the specific conditions for future activities.

In fact, Norway is currently experiencing the beginning of this process. According to Ben Taub, a journalist for *The New Yorker*, "For the past few years, civilian life in northern Norway has been under constant, low-grade attack. Russian hackers have targeted small municipalities and ports with phishing scams, ransomware, and other forms of cyber warfare. Individuals travelling as tourists have been caught photographing sensitive defense and communications infrastructure."[1] He states, "Norway's domestic-intelligence service, the P.S.T., has warned of the threat of sabotage to Norwegian train lines, and to gas facilities that supply energy to much of Europe. A few months ago, someone cut a vital communications cable running to a Norwegian Air Force base."[2]

The Norwegians believe the Russians are in the process of mapping their critical infrastructure, and that most attacks being carried out are deliberately murky, so it makes it difficult to attribute. They also believe these are acts of Hybrid Warfare, designed to subdue the enemy without fighting. According to Norwegian officials, the strategy appears to "subvert, to sabotage, to hack, to destabilize, to instill fear—and to paralyze Western governments by hinting at even more aggressive tactics."[3] Taub reported that since Russia annexed Crimea in 2014, Russia's "military and intelligence services have been experimenting with hybrid warfare and influence operations in Kirkenes, treating the

area as a "laboratory." Taub went on to state, that the regional police chief put it to him that "Some attacks were almost imperceptible at first; others disrupted everyday life and caused division among locals. To understand what was happening in her district, she started reading Sun Tzu."[4]

Unfortunately, the activities being experienced by Norway are only the start of a process that will increase significantly in scope and duration as time goes on or the need arises. To better appreciate the scope of the problem a Western nation could face, this section will examine a number of case studies that had national or regional impact. The case studies will cover a variety of incidents including the development and employment of armed non-state actors. It will also cover the use of SOF to achieve specific objectives without resorting to the use of conventional military forces.

The analysis will begin with the 2007 cyber attacks on Estonia where Russia attempted to infiltrate and sabotage Estonian government departments, research institutes, armed forces, energy distribution facilities, telecoms companies, financial services, and logistics management capabilities within the cyber domain while trying to aggravate social unrest. This was done in the form of various denial-of-service attacks, data modification and infrastructure manipulation and also included a sophisticated level of influence operations. In this respect, the case study provides a holistic view of what future cyber attacks might look like and what can be done about them.

The subsequent chapters will provide an overview of selected armed non-state actors. Specifically, they will examine Hezbollah, and Islamic State in Syria and Iraq (ISIL) and focus on the development of their fighting methods. In the process, the case studies will highlight the conditions that allowed these armed non-state actors to become regional players, as well as the evolution of their doctrine in that success.[5]

CHAPTER 7

THE 2007 CYBER ATTACKS ON ESTONIA

Sabotage is a deliberate action focused on destructive, disruptive or obstructive military, paramilitary, economic, or political actions. It is carried out by a nation's agent or proxy to hinder an opponent's political objective(s) or to further one's own. In order to achieve the maximum impact with the least amount of risk, saboteurs typically try to hit the weakest link in the security chain while still being able to achieve their goals.[1] Moreover, saboteurs will often attempt to conceal their identities in order to avoid the consequences of their actions. By doing so, they hope to delay or prevent invoking effective counter measures to address their actions.[2]

Because sabotage can hit many different parts of an organizational construct, it can take many different forms and vary in its complexity. For example, it can be highly technical in nature such as a government supported *coup de main* where a great detail of planning, logistics, and coordination are needed for success. Or, it can comprise simple acts that can be undertaken by individuals requiring little or no training. In such cases, actions can be as simple as delaying important government decisions, or they can be so bold as destruction of crucial equipment and infrastructure.[3]

In fact, the scope and amount of activity carried out by saboteurs is only limited by the resources, skills, and opportunities available to them. This flexibility allows sabotage to be used as an isolated act or as a weapon in combination with other actions.[4]

Limited resources combined with risk has resulted in sabotage operations remaining local affairs often focused on the highest priority or profile targets. However, this situation is changing. With the widespread adoption of modern communications, particularly the internet, both states and non-state actors become increasingly reliant on worldwide interconnectivity. Although this new connectivity brings with it a number of

advances, it also creates structural weaknesses. These structural weaknesses are now providing saboteurs, in the form of hackers, with unique opportunities and expanded reach to carry out their operations.

Although the basic principles and outcomes for sabotage have remained unchanged in the digital/information age, the tools used to achieve those outcomes have evolved. Malicious software, viruses, and hackers have now become the weapons of choice for individuals and groups wanting to disrupt government activities, target specific industrial systems, paralyze commercial activity or change policy direction within a targeted country through sabotage.

An early example of digital/information age sabotage was an action executed by the United States Central Intelligence Agency (CIA). During the early 1980s, the CIA were alleged to have tried to sabotage the Soviet economy through the covert transfer of technologies that contained hidden malfunctions. This included software. It is believed that it was corrupt software provided by this operation that eventually triggered a large explosion in a Siberian natural gas pipeline in 1982.[5]

A more recent example of cyber sabotage is the Stuxnet computer worm. This virus was reportedly designed to destroy numerous centrifuges in Iran's Natanz uranium enrichment facility by causing the centrifuges to burn themselves out.[6] It generated significant media attention at the time of its discovery in 2010, because it was the first known virus specifically designed to cripple or destroy hardware. Of greater interest is the fact that it appeared to have been created by a joint effort between by the U.S. National Security Agency, the CIA, and Israeli intelligence for government sabotage operations.[7]

In April of 2007, another instance of digital sabotage occurred in the form of an all-out cyber assault on a country. In this instance, a number of coordinated attacks were launched on Estonia by so-called "digital activists" from within the Russian diaspora. As Estonia was considered one of the most "connected" countries in Europe at the time of the incident, it is generally believed that this attack was specifically targeted to obstruct government operations, and significantly disrupt the country's economy in order to effect change in its policy direction.[8]

The events that unfolded in Estonia in the spring of 2007 serve to illustrate the increasing ability of saboteurs to use digital tools to inflict damage, disrupt society and challenge the policies of nation-states.[9] This chapter will examine the cyber attack on Estonia and provide an overview of the country's response. It will review possible reasons behind the attack and outline some of the steps that have been taken in its aftermath to better prepare states for such a situation in the future. Finally, it will look at what this attack means to the future of cyber sabotage. For context, in order to better understand the attacks, it is important to first review the political situation between Estonia and Russia at the time of the incident.

BACKGROUND ON THE ATTACKS

Historically, there has always been an underlying degree of tension between Estonia and Russia. Prior to the start of the Second World War much of this tension was based on continuous Russian encroachment and settlement into eastern Estonia. Many of the current issues dividing the two countries have their genesis with the Soviet annexation of the Baltic States in 1940 and subsequent occupation of the country during the Cold War (1947–1991).[10]

In an attempt to increase cohesion within the Eastern Bloc but ultimately to completely "Russify" Estonian culture, the Kremlin pursued an aggressive policy of resettlement. In the process, it relocated hundreds of thousands of ethnic Russians into Estonia throughout much of the Cold War period. With the dissolution of the Union of Soviet Socialist Republics (USSR) in 1989, ethnic Russians accounted for an incredible 26 per cent of the county's total population.[11]

When Estonia finally regained its independence in 1991, the Government moved quickly to implement a number of policies specifically designed to reduce Russia's overall influence on both its political infrastructure and its culture. Over the years, these policies have served to frustrate Moscow as it seeks to maintain influence in what it believes is its sphere of influence in the Baltic States.[12]

In January 2007, the Estonian government decided to relocate a Soviet era gravesite and monument honouring the sacrifice of Russian troops

during the Second World War.[13] The monument, located in the center of Tallinn, had become extremely controversial. For ethic Estonians it was a constant reminder of the Soviet occupation and oppression. However, for the Russian minority in the country, it represented Russia as the liberator. As a result, it had become a lighting rod of tension between pro-Kremlin and Estonian nationalist movements.

In an attempt to defuse the situation, the Estonian government tried to come up with what it believed was a compromise solution.[14] It would move the monument, along with the accompanying remains, to a nearby military cemetery just on the outskirts of the city. There, it could still be a focal point of remembrance but in a more appropriate and far less visible setting. The planned move infuriated Moscow. Concerned that its former Soviet republic was cutting ties to its post-war history, the Russian Upper House took immediate action. It adopted a resolution demanding the Estonian government stop legislation to relocate the monument. Russian First Vice Prime Minister, Sergei Ivanov, went so far as to suggest a boycott of Estonian goods and services.[15]

In the end, these threats were not sufficient to deter the Estonians, and work on the monument's relocation began on the morning of 26 April 2007. Unfortunately, these actions were not without incident. As work began, pro-monument protesters gathered in a peaceful demonstration at the site in an effort to stop the move. When it became clear that the effort was not going to succeed, the situation turned violent. According to the British Broadcasting Corporation, "On 26 April 2007, Tallinn erupted into two nights of riots and looting. 156 people were injured, one person died and 1,000 people were detained."[16]

Police were eventually able to regain control of the situation but not before the rioters looted and caused significant damage to buildings in the surrounding area. What few understood at the time was that this incident proved to be only the beginning of what would become a far more coordinated and prolonged action.[17]

THE ATTACKS

On 27 April 2007, the following day, the country was hit with a series of cyber-attacks on its networks and information systems. The attacks, which lasted for 22 days, were carried out in two phases. The first phase comprised of a series of un-coordinated attacks that targeted high-profile websites including the President's office, Parliament, police, political parties, and a number of major media outlets. The majority of the hacks involved different forms of denial of service and distributed denial of service (DDoS) attacks.[18]

A denial-of-Service (DoS) attack is designed to shut down a specific machine, website or network by making it inaccessible to its intended users. This type of an attack is normally carried out by flooding the target with traffic, or sending it information that triggers a crash.[19] A distributed DDoS attack occurs when multiple systems target a single system for a DoS attack. In this way the targeted network is bombarded with packets from multiple locations that are rerouted through different countries.[20]

Heavily involved in this first phase were low-level hackers, commonly referred to as "script-kiddies." Script-kiddies are usually younger web page defacers. At times they unwittingly aid and abet criminals or professional hackers through their constant probing and compromising of systems. In this case, they were able to hack their targets using copied scripts or rented botnets created and distributed by professional hackers.[21] In the attack on Estonia, evidence shows that the hackers planning the assault encouraged script-kiddies in Russian chat rooms and other online forums to go after the Estonian sites. Once the script-kiddies started the process the sophisticated hackers moved in to do their work under the noise being created while remaining anonymous.[22]

Unfortunately, these initial attacks were just the opening round as things got much worse before getting better. In the second and main attack phase, which occurred between 30 April and 18 May, the attacks became automated as much of the attack coordination was delegated to the command-and-control servers of real botnets.[23] These botnets are a collection of internet-connected devices infected with malware that hackers can control remotely.[24]

This phase ran in four waves of different intensities, focusing on different targets in each wave while using different attack techniques.[25] According to Andreas Schmidt of the Delft University of Technology:

> The first wave of this phase occurred on 4 May and focused on websites and DNS systems. The second wave ran between 9 and 11 May and hit primarily government websites and financial services. The third wave on 15 May included botnet-based DDoS attacks against government websites and financial industry. The fourth wave again consisted of attacks against governmental websites and banks.[26]

Once these attacks started, Estonian online services went down in quick succession, as banks, media outlets and various government agencies were hit with unprecedented levels of internet traffic. Damien McGuinness, a correspondent reporting for the BBC, described the attack as follows:

> Massive waves of spam were sent by botnets and huge amounts of automated online requests swamped servers. The result for Estonians citizens was that cash machines and online banking services were sporadically out of action; government departments and officials were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news.[27]

Fortunately, these types of attacks do not typically result in the theft or the loss of information. Their primary purpose is to force the victim to spend time and money dealing with the outcomes.[28] As such, they are designed to create disruption, confusion and frustration for the intended victim(s). However, these actions did "effectively closed down the 'always on' nature of the digitally dependent state of Estonia."[29]

In the short-term, the attacks blocked access to information and services that the country depended on and this could have had profound economic and potentially social consequences. Had the attack gone on much longer, there could have also been a far greater consequence to Estonia and its reputation as a safe place to do business.[30]

A COORDINATED ECONOMIC EFFORT TO ACHIEVE MAXIMUM IMPACT

Although the cyber attacks took most of the international media spotlight, it was economic pressure that caused the greater amount of short-term damage to Estonia. Once work started on the monument, trade relations between the two countries deteriorated rapidly. And as time went on, the Russian Government continually increased its pressure on the Estonian economy. According to Anastasia Nevskaya of the Institute of World Economy and International Relations, the Estonian government ended up losing a great deal of Russia's business and investment because of the crisis. She revealed that the transit industry was one of the biggest losers as Estonia handled 25 per cent of Russia's petroleum product along with large amounts of coal, forest, chemical, and metallurgical industries exports to the European Union (EU).

It has been estimated that shipments moving through Estonia decreased by as much as 41 per cent between January-March 2008, compared to the similar period of 2007.[31] The full impact of Russian actions likely cost the Estonian economy close to eight million krooni (0.5 billion euros) per year. This amount is about 3 per cent of the country's GDP.[32] In addition to lost revenues there was also a mass exodus of both Russian companies and investors from the country. Much of this money re-orientated its focus to neighbouring countries while some simply moved back to the Russian side of the border.[33]

ESTONIA'S RESPONSE

Although there was little Estonia could do about the economic pressure it was facing, it was able to deal with the cyber attacks as they occurred. According to Major Max Gordon of the United States Air Force, "Many IT experts in the country had done an impressive amount of preparation in combating possible threats to web services."[34] He explained this was "due in part to the country's need for sophisticated security in the face of an early adoption of web-based voting."[35]

Nationally, a task force of cyber security experts, along with election authorities from the police, intelligence services, and other agencies had

been put together in preparation for the April 2007 elections. Fortuitously, this task force remained in place after the vote when different intelligence agencies started receiving mounting evidence of possible DDoS attacks on the government.[36]

Despite advance knowledge of the strikes, Estonia struggled in the face of both the sophistication and scale of the attacks. Thankfully, the DDoS attack methodology is very familiar to cyber security experts so they were quite easy to counter. The key was to identify the sources of attack so that the unwanted web traffic could be blocked. Due to the massive size of the attack, however, blocking all the sites took both time and resources.[37]

Another issue was that the country's front line cyber experts were struggling with the adaptability of the hackers. They were finding that as they attempted to defeated/stop incoming assaults by filtering out the botnet's brand of attack, a short while later it would get past the defenses after having been modified to bypass the new filters that had been put into place.[38] Gordon suggests, "This type of adaptability would indicate a very active, persistent, and sophisticated hacker/s carrying out the attack."[39] It did not help that the attacks were coming from all around the world. This meant that blocking all the attacks at their source would require significant international cooperation.

In the end, that is exactly what happened. In addition to its own resources, Estonia was able to garner the assistance of cyber experts from Finland, Germany, Israel, Slovenia and others to eventually restore all of their network operations. In the process, they also received help from the North Atlantic Treaty Organization's (NATO) Computer Emergency Response Team (CERTs), which provided additional assistance, as well as EU's European Network and Information Security Agency (ENISA) that produce technical assessments of the developing situations.[40]

LIKELY ATTRIBUTION FOR THE ATTACKS

Saboteurs typically try to conceal their identities and the 2007 cyber attacks on Estonia were no exception. Despite the extensive media coverage and very public form of the attacks, only one person was ever charged. And, although Moscow has always denied involvement in these

attacks, there is compelling circumstantial evidence to suggest high level government involvement.

For example, the demonstrations, concurrent economic disruption and overall sophistication of the actual cyber attacks, particularly in its later stages, all occurred in conjunction with the scheduled move of the Tallinn monument. The only country protesting the move at the time was Russia, so it is not difficult to conclude that these actions were likely a coordinated act of hostility on their part to stop the work.[41]

In addition to the timing and sophistication of the attacks, Estonian and international cyber experts were able to track the source of many of the individual attacks back to Russia. In fact, they were even able to trace one source from a computer within the Kremlin.[42]

It is also clear that the attacks were politically motivated, as many of the hacks contained messages related to the conflict surrounding the statue. It is difficult to accept that such actions would have occurred from inside Russia without at least "unofficial" government approval.

After the incident, there was a total lack of cooperation by Russian authorities with any investigations into the attacks. This refusal, despite the fact that the activity in Russian-based forums at the time of the assaults indicated a clear and widespread interest in attacking Estonia. Moreover, many of the copied scripts and instructions for the attack were described in detail on both Russian language forums and various websites, all of which were available to anyone interested in participating in the attacks.[43]

When taken together, it is not difficult to conclude that Russia's political elite were playing a leading role in the attacks. However, based on this assertion, the question remains, why would Russia be interested in conducting these attacks in the first place?

RUSSIAN RATIONAL BEHIND THE ATTACKS

In the context of the specific situation, analysts believe the attacks were carried out to convince the Estonian government to stop the relocation of a memorial. Using cyber warfare as the major line of attack was logical in

this case for two reasons. First, this type of attack provides near perfect deniability for the government.[44] Secondly, for a country that has been described as "The Most Wired in Europe," hitting the country's public digital services would have the greatest effect on the largest number of individuals, government agencies and businesses at the lowest cost.[45]

However, these actions were likely part of a march larger strategy aimed at maintaining Russian influence over the country and possibly to serve as a warning for others in the Baltic region. To achieve this strategic outcome, the attacks were likely an attempt to destabilize the Estonian social system and undermine the country's economy. In so doing, the Russians hoped to weaken Estonian ties to both the EU and NATO.[46]

Analysts have also suggested that Russia's influence campaign may have been seeking to demonstrate to Estonian citizens that their own government (and NATO) was unwilling and/or unable to protect them or to pursue the adversary, thereby weakening trust and confidence in both the national government, and the established international collective security structures protecting the Baltic region.[47]

It is possible that the Russians may have also wanted to test and refine the developing concept and capabilities of what they would later refer to as *New Generation Warfare*. This is the same concept the world would witness in 2014, with the Russian assaults on Crimea and Ukraine. In fact, this situation was an ideal opportunity to functionally test cyber weapons in coordination with other strategically ambiguous measures such as the protest potential of the population, and economic sanctions. Moreover, they would able be able to closely monitor and evaluate the responses to these measures.[48]

In looking at the emerging concept of Russia's *New Generation Warfare*, Dr. Rain Ottis, a professor and founder of the Centre for Digital Forensics and Cyber Security at the Tallinn University of Technology, provides an interesting link between these attacks and Chinese strategies regarding the concept of the People's War in the digital era. He states:

> In an article about possible Chinese strategies for invading Taiwan, it points out the possibility of using the information age equivalent of the concept of people's war. In the context of cyber

> attacks, this means that ordinary citizens of a state can be motivated to use the resources under their control to independently attack enemy systems in order to confuse the defenders…Amidst all the noisy and ill-coordinated attacks, more professional intrusions can then be carried out, supplemented with physical attacks to take out the command-and-control systems of the opponent. The beauty of people's war is that it provides near perfect deniability for the government or any other entity that is behind the attacks.[49]

This example is an interesting perspective because this is precisely what the mobilization of the "script-kiddies" accomplished during the Estonian attack.

Finally, another possibility is that 2007 was an election year in Russia so it is likely that the attacks could have also been a distraction and attempt to unite the Russian people against a common enemy before those elections occurred later that year. It is likely that Russian motives included a combination, or possibly all, of this rational.[50]

RUSSIAN STRATEGIC SUCCESS WITH ITS INFLUENCE OPERATIONS

If the main goal for Russia was to maintain influence over the country by attempting to destabilize Estonian society and weaken its ties to the EU and NATO, then the attacks were a failure. Estonia did not stop work on moving the monument, and it was able to hold off the onslaught and, in the process, achieve several political gains for itself. Specifically, it was able to establish closer ties with the West. According to Schmidt, "the attacks and the respective response turned Estonia into a household brand for all matters cybersecurity, which likely helped to secure the hosting of the NATO Cooperative Cyber Defence Centre of Excellence and EU Agency for large-scale IT systems." He added, "Its vanguard status was only increased by Estonia's provision of support in some international cyber-crime cases. Politically, Estonia managed to secure an increased commitment from NATO and the EU, thereby advancing its strategic foreign policy goal of strengthening integration into Western institutions."[51]

WESTERN POLICY AND STRATEGY RESPONSES SINCE 2007

Another area where the attacks had an impact was in highlighting to the international community the importance of cyber security. Saboteurs attempt to conceal their identities in part to avoid the consequences of their actions. By doing this, they hope to delay or prevent invoking effective counter measures to address their actions. In the case of the 2007, cyber attacks on Estonia the opposite occurred.

Both during and after the cyber attacks on Estonia, NATO and EU member states began to take a far more serious interest in cyber security than had previously been the case. To this end, the NATO Cooperative Cyber Defence Centre of Excellence was established in Tallinn, Estonia and became a NATO-accredited research and training facility focused on cyber defence education, consultation, lessons learned, and research and development.[52]

About a year later, at NATO's Bucharest Summit in April 2008, cyber security was a priority agenda item with discussions leading NATO to adopted a policy on Cyber Defence and to the establishment of the Brussels-based Cyber Defence Management Authority (CDMA) to "centralise cyber defence capabilities across the Alliance."[53] In August of that same year, Tallinn became home to NATO's cyber security headquarters.[54]

In November 2010, the EU released its cyber security strategy, calling for an integrated response to cyber security threats and significant expansion of the European Union Agency for Cybersecurity (ENISA's) duties beyond a purely analytical role. In addition, both NATO and the EU announced plans "to establish CERTs for EU institutions, hold multinational cyber defence simulations, and create a joint European cyber-crime platform," along with steps to develop strong, integrated internet defence capabilities.[55]

Since that time, the NATO Computer Incident Response Capability Technical Centre (NCIRC TC) has become operational.[56] It includes the NATO Communications and Information Systems School in Latina, Italy, as well as the NATO School in Oberammergau, Germany, which

also conducts cyber defence-related education and training to support Alliance operations, strategy, policy, doctrine and procedures. The NATO Defence College in Rome, Italy, also fosters strategic thinking on political-military matters, including on cyber defence issues.[57]

In February 2016, NATO and the EU concluded a Technical Arrangement on Cyber Defence to help both organizations better prevent and respond to cyber attacks. This Technical Arrangement provides a framework for exchanging information and the sharing of best practices between various emergency response teams.[58] Rather than delaying or preventing effective counter measures, the cyber attacks on Estonia actually became the stimulus for action on internet and cyber security worldwide.

IMPLICATIONS FOR THE FUTURE OF HYBRID WARFARE

So, what can the cyber attacks on Estonia in 2007 tell us about the future of cyber warfare as a weapon in the information age? For peer and near-peer adversaries wishing to cause obstruction, disruption, or destruction while having plausible deniability, cyber actions appear to provide an ideal solution moving forward. Moreover, they provide a great deal of flexibility as they can be very simple and focused, as was the case of the corrupt software operation that triggered the explosion in a Siberian natural gas pipeline. They can be focused and more complicated, as in the case of the Stuxnet computer worm, or they can be broad and complex such as the attacks on Estonia.

Primitive cyber attacks take very little time and effort to organize, while defending against them requires a major investment in both time and resources. Unfortunately, as countries continue to invest in highly developed network infrastructures, they will become increasingly vulnerable to digital sabotage.[59]

Of greater significance is the fact that Estonia has showcased to the world that cyber space is being rapidly militarized. With this militarization comes the dangers of both an increase in the acts along with a greater variety of attacks. In the event of war, all of a targeted country's critical systems could fall under a simultaneous concentrated cyber attack from thousands of professional, well trained and equipped cyber attackers

that control an army of cyber militia with just enough training to be dangerous.[60] In this regard, attacking a nations' cyber infrastructure will become easier and far more prevalent as the cyber domain continues to evolve.

CONCLUSION

Information age technology has provided the world with a great number of benefits, but with it come greater dangers. These include transnational sabotage, cyber terrorism, information warfare, and the outright attack on a nation-state's sovereignty in cyberspace.

The 2007 cyber attacks on Estonia have shown that states and autonomous transnational networks, or a combination of the two, have the capability to target a nation's digital networks with the ability to disrupt and/or cripple its social order and/or critical infrastructure through various acts of sabotage. Ironically, the more technically sophisticated the targeted nation-state or organization, the greater the impact. Unfortunately, the effect of the cyber attacks on Estonia will likely encourage other groups to do the same in the future, as everyone with an internet connection has access to the battle area in this domain.[61]

The challenge for democracies is to find the right balance between internet freedom and providing adequate monitoring, early warning and defensive systems. These systems will need to be combined with a far more aggressive concept of cyber security cooperation across all borders. Cooperation and a flexible approach to problem-solving were the keys to Estonian cyber success. This approach must remain the Western model for success against sabotage, cyber terrorism, information warfare and an all-out network attack in the future.[62]

CHAPTER 8

NON-STATE ACTORS: THE LINK BETWEEN TACTICAL OPERATIONS AND STRATEGIC OUTCOMES IN HYBRID WARFARE

An important aspect of modern Hybrid Warfare is the ability of peer nations to link a series of tactical operations with strategic outcomes. One way of doing this is to use surrogate organizations, particularly non-state actors. This trend was demonstrated during the 2007 cyber attack on Estonia, where unidentified hackers and hacker groups carried out much, if not all, of the day-to-day operations for the Russians. More importantly, such groups are not directly linked to the government, so they can provide that all-important plausible deniability. However, peer and near-peer adversaries often seek to employ such groups as a way to achieve national objectives at relatively low cost to themselves in both dollars and personnel.

Such demand for their services often gives non-state actors access to modern equipment, along with various other forms of national level support. For armed non-state actors, this often means the ability to access modern weapon systems. Although it is this access that gives armed non-state actors their greater reach and destructive power, it also allows them to create a more refined conceptual approach to the conduct of their military operations. This is done by incorporating these new capabilities into their established doctrine.[1]

Doctrine can be defined as the fundamental principles by which military forces guide their actions in support of specific objectives.[2] At the tactical level, it is the adherence to doctrine that has allowed armed non-state actors to quickly transition their war-fighting methods from an insurgency campaign to conventional operations, or to combine both forms of combat, seemingly with little or no effort. Moreover, it is doctrine

that gives these groups the necessary framework in which to develop additional reach and fully utilize newly acquired technical capabilities.

This combination of integrating on-going advances in technology with changes to force structure and doctrine is what has fundamentally changed the dynamics of the modern tactical fight for these organizations. Specifically, it has allowed armed non-state actors to mature at much faster rates, engage their enemy at greater ranges and create higher casualty ratios on their opponents in battle. Together, these factors have produced an extremely complex security challenge for nation states forced to confront such fighters on the battlefield.

Armed non-state actors can provide peer and near-peer adversaries with the ability to introduce proxy combat forces into a conflict and they can quickly transform the situation on the ground. Moreover, they give these adversaries a holistic and flexible capability within the context of Hybrid Warfare.

HEZBOLLAH: THE TEMPLATE FOR ARMED NON-STATE ACTORS IS CREATED

The rise of Hezbollah has provided many armed non-state actors with a contemporary template for gaining and maintaining political and military power. The group's success is deeply rooted in its adherence to the *People's War* doctrine, which has been modified and continues to evolve to meet the changing circumstances the group faces. More importantly, that doctrine remains the foundation on which it continues to evolve and expand its capabilities.[3]

This adaptability, along with support from both Iran and Syria, has allowed Hezbollah to unite minority Shiites within Lebanon, while taking control of the political agenda in that country. In the process, they have developed an extremely resilient organization that has survived numerous attempts at its destruction.[4] The rise of Hezbollah as a modern armed non-state actor also provides Western analysts with a case study into how these forces emerge and the keys to their success.

This case study will focus on the group and its military capabilities as this is what Western forces will encounter on the battlefield. In so

doing, it provides an overview of its performance in selected operations to establish key periods within its developmental process. Finally, it will highlight specific periods that have played a role in defining Hezbollah's way of war. To begin, it is important to furnish a brief overview of the group's conception and early history.

Early History of Hezbollah

The rise of Hezbollah had its origins in the political situation facing Lebanon at the end of the Second World War. The country had gained its independence from France in November of 1943. As part of its transition from French rule, which ended in 1946, the Lebanese National Pact was established. The idea of this pact was to create a framework for the orderly distribution of power within the country.[5] In essence, the framework called for an allocation of membership within the state's parliament and control of senior bureaucratic and political appointments based on the 17 recognized sectarian communities within the country.

Although the allocation was proportionately grounded on the size of each community, the key positions of the presidency and premiership were given to the Maronites and Sunnis respectively.[6] The Shiite, the third largest demographic group in the country, was given the position of speaker. Regrettably, that position had no authority within the governing structure and resulted in the Shiite community becoming politically marginalized within the system.[7]

Full independence in 1946 brought with it turmoil and conflict. Since that time, Lebanon has alternated between periods of political stability and prosperity, frequently interrupted by civil war and the occasional need to fight off invasion. Adding to the overall instability within the country was the fact that in the aftermath of the 1948 Arab–Israeli War, more than 110,000 Palestinian refugees moved into Lebanon. This influx further aggravated tensions in an already stressed situation and resulted in even more conflict.[8]

Haugbolle Sune, an associate professor in Arabic and Middle Eastern Studies at the University of Copenhagen, insightfully points out that the situation in Lebanon "revolved around some of the same issues that dominated regional politics in the Middle East during the latter

part of the 20th century, including the Palestine-Israel conflict, Cold War competition, Arab nationalism and political Islam.''[9] Sune asserts, ''Conflicts over these issues intersected with longstanding disagreements in the Lebanese political elite, and in parts of the population, over the sectarian division of power, national identity, social justice and Lebanon's strategic alliances.''[10]

Civil War in Lebanon

By 1975, many of these issues had coalesced sufficiently to push the country into civil war. Hezbollah, as we know it today, did not emerge as a structured organization until after the 1982 Israeli invasion of Lebanon.[11] At the time of the invasion, many Shiite leaders within the country belonged to the *Amal Movement*. Amal was the military and political wing of Lebanon's Higher Shiite Council, a religious grouping that represented a large number of Shiites in Lebanon and was supported by both Syria and Iran.[12] However, Amal's leadership was divided on how best to respond to the Israeli aggression.

Those that favoured the eventual creation of an Iranian-style Islamic republic for Lebanon, wanted to fight the incursion and were unwilling to accept the more moderate approaches being suggested by others in the movement.[13] This division eventually resulted in a split within the group and the creation of the Al Amal al Islamiya (or Islamic Amal) organization.[14]

Frequent clashes between the two groups continued for a period of time, until they were able to reach an understanding with Syrian mediation. However, by that time, the Islamic Amal had established itself as the clear leader of Shiite interest in the country and as the apex of the resistance movement in the South. In the process, they became the umbrella association for like-minded groups, and it is this organization that evolved into Hezbollah (Party of God) in 1985.[15]

As chaos was unfolding within Lebanon during the early 1980s, Iran was seeking ways to capitalize on the deteriorating situation and unite the various Shiite militant groups under its control.[16] The emergence of Hezbollah as a supporter of the Iranian Revolution and clear leader of the resistance in the South provided Iran with that opportunity. In addition

to accessing financing and equipment, the group received assistance from Iran's Islamic Revolutionary Guard Corps (IRGC) *Pâsdârân*.[17] The Guard Corps provided instructors/mentors, and weapons along with expertise in organizing the group's militia. They also provided support to both social and cultural activities.[18]

Hezbollah's Strategy

Like many aspiring insurgent groups, Hezbollah initially confined itself to fighting other militias and carrying out acts of terrorism. This included suicide bombings, kidnappings, and hijackings. However, by 1986 the group's leadership began to realize these actions were unfocused and achieving little of substance.[19] Moreover, during its early years, Hezbollah's belief system prevented it from creating political alliances or understanding the need to win over the local population. In fact, its lack of tolerance for any ideas but its own alienated many Lebanese as the group quickly moved to implement and enforce Islamic fundamentalism in areas it had secured. These measures quickly proved very unpopular and the group started losing much of its support among the people it was trying to protect.[20]

As the backing of the local population is an essential prerequisite to success in the *People's War* doctrine, Hezbollah eventually realized it needed to somehow regain that support.[21] To do this, the group decided to make critical concessions to its philosophical outlook. As Cambanis Thanassis, a senior fellow at The Century Foundation highlights, "Hezbollah issued an invitation to the Lebanese people… 'Support our resistance against Israel, and we will stop talking about an Islamic republic and stop telling you how to live your lives'."[22]

In addition to granting more freedoms, Hezbollah also started providing areas under its control with better governance and a host of social services. This change in mindset played a crucial role in winning back and maintaining control over much of the Lebanese Shiite population.[23] Eventually, the group expanded its services into a vast network of activities including infrastructure, policing, garbage collection, health-care facilities, schools, and different youth programs.[24] A key part of this programme was the reconstruction of damaged homes. Every home

damaged in Israeli raids between 1991 and 2000 was eventually repaired, and it is estimated that the total number of homes the group worked on was over 17,000.[25]

From a military perspective, Hezbollah's real fight was with Israel and the group realized that without political participation its resistance movement would have no legitimacy within the country. To deal with this vulnerability, the group's leadership decided to run candidates in the parliamentary elections of 1992. Their efforts paid off, as they were able to take eight seats in parliament during their first run. This victory gave them a strengthened claim to legitimacy but also provided them with nationalist credentials.[26] As Iver Gabrielsen in his article, "Hezbollah's Strategy and Tactics in the Security Zone from 1985 to 2000," points out, "Pragmatism, social services and political participation were important means for Hezbollah to reach their political aim of liberating Southern Lebanon. This approach secured popular support and increased the legitimacy of their struggle." He added, "these non-military means were arguably a crucial aspect of Hezbollah's grand strategy."[27]

There can be little question that non-military means were an important driver in Hezbollah's overall strategy, the group understood that if it wanted to accomplish its ultimate goal, that of eventually creating an Iranian-style Islamic republic for Lebanon, it would first need to force the Israel Defense Forces (IDF) and its proxy, the South Lebanese Army (SLA) out of Southern Lebanon. And, that was not going to be done using non-military means.

To achieve this desired end-state, the group went back to the basics of the *People's War* doctrine. They realized that they would need a far more holistic military campaign based on a pragmatic strategy. The group's leadership concluded that by attacking the Israeli public's aversion to casualties, there was a possibility of eventually undermining support for the war effort. They also understood that such a victory would likely be a long and bloody process but believed that regardless of the outcome, the conflict would position Hezbollah as the undeniable leader in the southern part of the country. Lisa Brennen in her thesis, "Hezbollah: Psychological Warfare Against Israel," reinforces this last point when she states, "Hezbollah carried out attacks in order to position themselves as

the protectors of the Lebanese (not just Shiite) population of southern Lebanon from the vicissitudes of Israeli occupation."[28]

Moving forward, Hezbollah decided on a long-term strategy of continuous attrition. However, this meant that it would have to constantly hit at its enemies.[29] Moreover, it had to do so while maintaining a sustainable casualty ratio for itself. Unfortunately for the group, in the early stages of its development, it lacked both the knowledge and experience to achieve such an outcome. Operations tended to be poorly executed and usually resulted in high casualty rates. A CIA report published in 1987 noted that before the spring of 1986, Hezbollah's attacks were more "undisciplined acts of desperation than military actions."[30] The report highlighted an attack by the group on 18 April 1986, when a force of approximately 100 fighters attacked two SLA positions where 25 of its fighters were killed in what was described as a clear defeat for the group.[31]

One of the main reasons for this poor performance were the tactics being employed. The primary method of attack was human wave assaults. This technique was employed simply because it was used by the Iranians at the time and was taught to the group by their advisors.[32] Matters were not helped by the fact that many of their early assaults were carried out in broad daylight against well-defended outposts or positions. The results of such attacks often proved extremely costly, regardless of the actual outcome of the operation.

As Gabrielsen emphasized, in order for Hezbollah's attacks to have a strategic impact, "they needed to improve their tactical performance compared to the costly human-wave assaults of the 1980s." However, this in and of itself was not going to fix the real problem. Gabrielsen concluded that the group still had to deal with the main strategic issue it was facing which was, "[i]nflicting a heavy and persistent casualty toll on the IDF and the SLA was necessary to crack Israeli public support for the occupation of the security zone."[33]

By the summer of 1986, the group had begun to overhaul their tactical procedures in order to better align them to its strategic objective. To do this, they started improving training and looking at alternative methods that could reduce casualties using standoff attacks. Under this concept

they switched their focus from direct assaults on fortified positions to using improvised Explosive Devices (IEDs), ambushes, and various types of attacks employing long-range or indirect fires. Over time, these changes had the desired impact on the overall situation. IEDs, in particular, proved to be so effective that by the late 1990s they were accounting for almost half of all the IDF casualties.[34]

Although, direct assaults on fortified positions continued to be an important element of the overall strategy, particularly against SLA positions, they were starting to be carried out based on the principles of fire and movement. The group began employing assault forces and fire support teams. Fire support usually included machine guns, mortars and eventually the addition of long-range direct fire from anti-tank weapons.[35] The group also started integrating indirect fire support (artillery and mortars) into their attacks. The 1987 CIA report acknowledged this progress, stating, "beginning in the spring of 1986, the group was conducting squad-size operations using guerrilla-style hit and run tactics. By last fall, Hizballah began what appeared to be carefully planned attacks on Army of South Lebanon strongpoints." It continued, "in September [1986], Hizballah had launched an unprecedented number of simultaneous attacks on positions throughout much of South Lebanon."[36]

There is little question that these tactical level improvements were starting to create a more adaptable and proficient force on the battlefield. According to Gabrielsen, "When the IDF and SLA employed fixed outposts, Hezbollah responded by frontal assaults. When the outposts were reinforced, Hezbollah responded with indirect mortar and rocket fire. When the IDF changed tactics and became a more mobile force with increased patrols, Hezbollah responded with ambushes and improvised explosive devices (IEDs)."[37]

As Hezbollah became increasingly successful on the ground, they started to expand the scope of their operations throughout all of Southern Lebanon. However, this expansion brought with it the need to improve operational security. In addition to implementing better operating procedures, the group cut out a number of their loosely affiliated reservists. In order to limit information leaking out, the group also removed most mid-level commanders from the chain of command.[38] Interestingly, this change

not only increased security but had the added benefit of improving the group's battlefield performance as it pushed greater authority down to local commanders.

Local commanders are often in the best position to take advantage of the evolving situation on the ground in real time. This change gave them greater authority to act in those situations, which enhanced the group's overall tactical adaptability and performance. Improvements at the tactical level were not the only reforms implemented by Hezbollah.

By the early 1990s, the group had created a dedicated military staff, which enhanced its overall planning and coordination abilities significantly. An important aspect of this addition included the establishment of a new and highly proficient intelligence organization. Over time this capability evolved to became responsible for intelligence, counter-intelligence, and internal supervision.[39]

There is little doubt that intelligence triumphs by Hezbollah played a role in eventually forcing IDF into withdrawal from South Lebanon.[40] Notable examples of intelligence success included, "the ambush of sixteen naval commandos from the elite Shayetet 13 unit near the town of Ansariyah in 1997, which led to the loss of 12 Israeli operatives while Hezbollah reportedly only suffered casualties of two slightly wounded."[41] Despite statements from the IDF that the operation's failure was attributed to bad luck, evidence suggests that Hezbollah had intercepted Israeli unmanned aerospace vehicle (UAV) video transmissions in real time and possibly had a double agent working for them. Regardless of the reason for the operation's failure, Israeli raids north of the security zone halted after the operation.[42]

One of the more important mandates for the group's intelligence organization was the infiltration of enemy organizations.[43] Gabrielsen notes that much of their intelligence activities were focused on the SLA. He states, "Hezbollah was able to encourage desertions with offers of amnesty, in addition to targeting individual officers for assassination."[44] For example, "SLA's second-in-command Aql Hashim was among the killed high-ranking SLA officers."[45]

In fact, the group was eventually able to neutralize the effectiveness of the SLA through a long running campaign of both intimidation and assassinations. This success was in part due to the fact that Hezbollah's intelligence service maintained records of all SLA members and when needed, would threaten them unless they deserted or served as informants.[46]

These tactics had the added benefit of increasing the group's collection capabilities against the IDF, something that created a great deal of distrust between the IDF and SLA. The infiltration and slow disintegration of the SLA was significant in that a key part of the initial Israel strategy in 1982 was to use the organization as a buffer between themselves and the various anti-Israel forces operating in southern Lebanon.[47]

Collectively, these reforms had the desired strategic impact, as the group's casualty rates started decline. For instance, prior to 1993, it is estimated that Hezbollah was losing about five fighters for every Israeli soldier killed. After 1993, that ratio was down to about 1.5 to 1.[48]

On the battlefield, a major improvement in the group's combat capability occurred in September of 1992, when it acquired the AT-3 Sagger anti-tank guided missile (ATGM). As time went on, the employment of this weapon steadily increased as the group continued to evolve its anti-tank tactics to deal with Israel's Merkava tanks.[49] Although the quality of the group's missiles could not match the Merkava's sophisticated reactive armor protection suite, ATGM gunners were trained in finding work-arounds using innovative tactics. For example, tank hunting teams were able to eventually defeat the armour by using swarming tactics. This method involved hitting the same spot on a tank, multiple times in quick succession to overwhelm and defeat the vehicle's defences.[50]

In response to Hezbollah's growing threat, Israel started to exert greater pressure on the group. This strain was done by increasing retaliatory attacks and launching large-scale counterterrorism operations targeting both the group's personnel and capabilities.[51] The first of these major operations occurred in July 1993, when Israel launched a major offensive into Southern Lebanon.

Operation Accountability and the Introduction of Katyusha Rockets

Operation Accountability took place between 25 and 31 July 1993. It occurred after months of sporadic clashes between the IDF and Hezbollah. According to the IDF, the goals of the operation were "to strike the terrorist organization Hezbollah and other Lebanese terror organizations and to stop them from turning southern Lebanon into a base for terror."[52] To achieve this outcome, Israel used a combination of air raids; artillery strikes and commando operations against specific targets in an attempt to eliminate the group's capabilities.[53] The operation concluded after a week of heavy fighting with little or no impact on Hezbollah.[54] Despite a clear lack of success by either side, the operation did prove significant in that it saw the first large-scale and prolonged use of unguided Katyusha rockets being fired into Northern Israeli settlements by the group.

Hezbollah first fired these rockets into Northern Israel in retaliation for the assassination of Abbas al-Musawi in 1992.[55] However, it was not until Operation Accountability that the extensive use of rocket attacks over a prolonged period was employed by the group as a critical part of ongoing operations. More importantly, the success of these attacks during this action resulted in the rocket's employment becoming a standard operating practice for Hezbollah moving forward.[56]

The reason these attacks proved so effective was due to the indirect effects they created, rather than the casualties they produced. The range of these weapons could put almost one million people living in Northern Israel at risk. These people would need to seek refuge in bomb shelters every time there was an attack.[57] More importantly, during periods of sustained shelling people living in the impacted areas were forced to relocate, creating significant additional problems for government officials already dealing with the demands of an ongoing operation. Finally, from a psychological perspective, it was quickly realized that these attacks had a major impact on the Israeli public's confidence in the ability of their politicians and the IDF to keep them safe.[58]

Thus, the introduction of Katyushas into the conflict with Israel provided Hezbollah with an important weapon in helping the group achieve its

strategic objective, that of undermining support for the war effort. It also gave the group a significant deterrence capability against its enemy. In fact, it is likely that this development helped to shorten the Operation Accountability campaign and led to an understanding between the two sides, "Hezbollah would not launch rockets, if Israel did not launch attacks that caused Lebanese civilian casualties."[59] This understanding, however, did not last long as sporadic clashes continued between Hezbollah and Israel. These actions eventually culminated with Israel once again launching a major assault on the group in 1996 under what was called Operation Grapes of Wrath.

Operation Grapes of Wrath

Operation Grapes of Wrath was the second major offensive carried out by the Israelis specifically targeting Hezbollah. It occurred between 11 and 27 April 1996. Its stated goal was to neutralize rocket attacks into northern Israel. The methods employed in attempting to achieve this outcome, however, were at best questionable. At the start of the operation, Israeli aircraft and artillery hit a number of Shiite villages in South Lebanon.[60] The purpose of these attacks was to create a humanitarian crisis by forcing the civilian population out of their homes and having them evacuate towards Beirut.[61] The Israelis hoped that the subsequent crisis would put sufficient pressure on both the Lebanese and Syrian governments to finally put an end to Hezbollah. At the very least, it was assumed that the operation would degrade the group somewhat as it would hit the infrastructure being used by the organization.[62]

Although the sixteen-day campaign was marked by intensive rocket and artillery strikes and heavy ground fighting, Hezbollah suffered little overall from the operation. In fact, it is telling that the group was able to continue launching rockets into Israel for the entire period of the operation. The campaign ended with the negotiated written "Grapes of Wrath Understandings." This agreement barred cross-border attacks on civilian targets, as well as the use of villages to launch attacks.[63]

After the operation, fighting lulled briefly as Hezbollah took time to recover from the effects of the fighting. The group dramatically escalated its level of activities in the subsequent months and years.[64] Arguably,

the group appeared to become stronger as time went on. For example, Hezbollah carried out 100 attacks from 1985–1989 and 1,030 attacks in the six-year period from 1990–1995. However, from 1996–2000, it launched over 4,928 attacks.[65]

Moreover, by 1997, Hezbollah was displaying capabilities normally found in advance insurgency armies or conventional military forces, as many of the reforms of the early 1990s were now being combined with more advanced equipment and experience. According to Major Christopher E. Whitting, in his thesis, "When David Became Goliath," a characteristic Hezbollah attack now:

> consists of a hit-and-run assault on an IDF or SLA position or patrol. It will normally involve two squads, each comprising three-to-four men. Typically, the first squad will attack a compound at any time of day at close range with light and heavy machine guns, rocket-propelled grenades and Sagger or 90 Spigot antitank missiles…At the same time, the second squad, acting as a fire support team, will fire 81-millimeter or 120-millimeter mortars. Attacks lasted only a couple of minutes and the Hezbollah, did not limited their attacks to one objective, but rather synchronize concurrent attacks against multiple positions that were spread over a wide area.[66]

In February of 1997, the group launched a total of 21 attacks on IDF and SLA positions simultaneously. In late December of that same year, Hezbollah repeated this scenario, launching 25 attacks on IDF and SLA positions simultaneously.[67]

Of greater significance is the fact that starting in 1997, combined Israeli and SLA casualties began to exceed those of Hezbollah. In 1990, Hezbollah was suffering 5.2 casualties per IDF/SLA casualty. In stark contrast, by 1998, that casualty gap was shrinking. In that year, Hezbollah suffered 37 and the IDF 23 killed in action respectively.[68]

On 24 May 2000, the first phase of Hezbollah's long-term strategy succeeded amid escalating violence, poor morale, and intense political pressure at home for the Israelis. The war in Lebanon simply became

too much for Israel. The IDF departed southern Lebanon after 18 years of occupation.[69] Not surprisingly, the SLA collapsed shortly after the withdrawal and Hezbollah took over control of the region.[70]

During the course of the insurgency, Hezbollah had evolved from a poorly trained militia group into a highly skilled guerrilla movement that was concurrently pursuing political, social, military and propaganda goals. According to Shmuel L. Gordon, a PhD in International Relations and Strategic Studies from the Hebrew University in Jerusalem:

> Its [Hezbollah's] development reveals a deep understanding of the theory and practice of guerrilla warfare. Central control of the different wings of the organization is a power multiplier that enhances the movement's integrity and unity…In the last few years Hezbollah fighters have acquired the knowledge and proficiency needed to exploit modern weapon systems such as anti-tank missiles, sophisticated mines, proximity and electronic fuses, communication, and intelligence gathering systems…The integration of guerrilla doctrine and tactics with modern systems has become a substantial factor in the movement's success against a modern, well-trained, well-equipped IDF.[71]

2006 Lebanon War

After the Israeli withdrawal from Southern Lebanon in 2000, Hezbollah realized that it would only be a matter of time before the two sides clashed once again. As a result, the group used that period to transform itself into a more effective fighting force. As it continued to monitor Israeli developments, it started adopting a number of lessons learned it had gain from its insurgency.[72]

Although, there were many minor alterations made to improve its overall tactical performance, a key change in the group's strategy was its decision to transition from a guerrilla army into a regular military force.[73] This transformation was done within the aforementioned doctrine by splitting guerrillas into two capabilities: regular and guerrilla forces. Within this context, the strategic role of guerrilla warfare is to support regular military operations and to provide replacements for the regular force. According to the doctrine, regular forces can still be used to carry out

guerrilla warfare when needed, however, their primary military focus remains the conduct of mobile and positional warfare.

From a geographic and security perspective, these changes in force structure were coupled with an operational imperative onto positional warfare or what Western experts often denote as the operational defensive. As such, Hezbollah would fight a defensive battle while attempting to maximize opportunities for the tactical offence. In the process, it would evolve its fighting methods into what Western analysts now refer to as a hybrid force. Hezbollah's strategy for its future defence was based on the idea of area-denial using a "Complex Web Defense" (CWD) concept. This concept also incorporates the use of integrated standoff fires along with an active defence component on the ground.[74]

CWD was based on a series of well-defended villages and small built-up areas that were interconnected to natural terrain features. When they were brought together, they became a series of integrated and mutually supporting defensive positions. These interconnected positions included well-sited strong points, redundant communications, overlapping fields of fire and large stockpiles of supplies.[75]

The active defence component was characterized by launching rocket attacks into Israel and employing mobile light infantry forces organized into small self-sufficient units. These units carried out ambush patrols and anti-tank hunting operations. Once hostilities started, these forces provided a constant rate of attrition on advancing IDF forces until they hit the main defensive positions.[76]

Not surprisingly, the idea behind Hezbollah's overall concept for defence is similar to China's concept for active defence. This similarity is likely due to the fact that both military capabilities evolved from Mao's *People's War* fighting concept. Captain Scott J. Tosi, highlights in his article, "Xi Jinping's PLA Reforms and Redefining 'Active Defense,'" that the concept was actually "First coined by Mao Zedong during the Chinese Civil War for the strategy of the Red Army (the precursor to the PLA)."[77] He states, "the term emphasized a strategically defensive posture characterized by tactically and operationally offensive actions, primarily within the confines of China's geographic borders."[78]

This basic idea is reinforced by Major Timothy A. Ornelas in his article, "China's Active Defense Military Strategy," where he acknowledges, "Following the Chinese Civil War, China's primary military strategy was influenced heavily by Mao Zedong's approach to guerilla warfare, which sought to draw an adversary deep into Chinese territory then reclaim any lost territory through a long-protracted war of attrition using China's geography and population to its advantage."[79]

By 2006, Hezbollah's defensive posture included an operational level mobile component/reserve that remained north of the Litani River. However, the concept appeared to emphasize a desire to defeat or at least significantly wear down the IDF in a series of defensive battles at or near the border. If this was not possible, they would allow the Israeli attack to continue into Lebanon before starting to reclaim lost territory through a protracted war of attrition using the active defence component of its force structure.

To this end, the group started a massive buildup in the early 2000s that involved the construction of defensive positions interconnected by tunnels. In addition, they were able to increase both the number and sophistication of their weapons holdings. This arsenal included more advanced anti-tank missiles like the AT-14 Kornet and their first holdings of UAVs.[80]

In the lead up to the war, the situation remained strained between the two sides. Things took a drastic change on 12 July 2006, near Zarit, when Hezbollah ambushed an Israeli patrol just inside Israel. During the attack three Israeli soldiers were killed and two others were captured as leverage for the release of incarcerated Hezbollah prisoners. Unexpectedly, Israel responded to this attack with a full-scale invasion, sparking what would become the 34-day 2006 Lebanon War.[81]

Within hours of the Hezbollah attack, Israeli authorities retaliated with a bombing campaign that targeted various objectives within South Lebanon and Beirut including the Beirut airport. The main focus of the initial Israeli response was an air and artillery campaign with the Israeli Air Force flying 11,897 missions and firing some 170,000 artillery shells.[82] Israel also launched a limited ground attack into South

Lebanon. The stated aim of this offensive was to push Hezbollah away from the Israeli border.[83]

Hezbollah retaliated to the airstrikes by firing rockets into Israeli territory. In fact, over the course of the conflict it is estimated that the group fired between 3,970 and 4,228 rockets in total.[84] On the ground, Hezbollah's new defensive strategy work extremely well as the group was able to disrupt the Israeli offensive using its newly established active defence concept almost as soon as it started.

As the IDF assault force advanced, it found itself facing well-organized Hezbollah militias both in the countryside and in every town and village they approached.[85] It did not help matters that the region they were attacking was ideal for defensive operations, so the terrain negated many of Israel's advantages in armoured and manoeuvre warfare. As a result, combat outcomes focused on the importance of highly developed infantry skills, where Hezbollah proved to be superior.[86]

The 2006 conflict between Israel and Hezbollah ended after 34 days of fighting by United Nation (UN) Resolution 1701. The resolution was approved by the United Nations Security Council (UNSC) and was accepted by both sides. As a result, the cease-fire took effect on 14 August 2006.[87]

The Concept of Hybrid War at the Tactical Level

Not surprisingly, the 2006 war garnered significant interest from Western analysts as it was clear that Hezbollah had performed extremely well against the IDF onslaught. More importantly, the group was something more than the purely guerrilla organization it had been in 2000. During operations it showed it could switch between guerrilla and conventional (mobile) warfare or use both forms simultaneously depending on the situation. Moreover, it now had the ability to absorb significant damage during prolonged periods of high-intensity fighting. Outside of the context of the Israeli–Hezbollah conflict, this new form of warfare had the potential to become a major threat to Western militaries and therefore needed to be better understood.

In his analysis after the war in 2007, Frank Hoffman, a Research Fellow at the Marine Corps Warfighting Laboratory, produced a monograph entitled, *Conflict in the 21st Century: The Rise of Hybrid Wars*. This book was primarily based on Hezbollah's performance in the war.[88] In it, Hoffman laid out the key principles that have come to define Western perceptions on tactical Hybrid War. In this work, he defined Hybrid Wars as incorporating "a range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorism acts including indiscriminate violence and coercion, and criminal disorder."[89] He described this form of warfare as blurring the lines between different types of conflict, those who fight them, and the technologies that are used.[90] In this respect, Hoffman saw the world entering a period when multiple types of warfare would be used simultaneously by flexible and sophisticated adversaries.[91]

Hoffman believed, "The future does not portend a suite of distinct challenges with alternative or different methods but their convergence into multi-modal or Hybrid Wars."[92] He emphasized that units operating in such an environment would be hybrid in both form and application. As an example, he pointed out that future conflict would include hybrid organizations like Hezbollah and Hamas, employing a diverse set of capabilities. Additionally, he envisioned states shifting their conventional units to irregular formations and adopting new tactics, as the Iraqi *Fedayeen* did in 2003.[93] Hoffman also highlighted the fact that although these activities could be carried out by the same, or separate units, they would usually be operationally and tactically coordinated within the main battlespace by a higher headquarters to achieve synergistic effects.[94]

One of Hoffman's most critical observations pertained to how Hybrid Wars would function in terms of the interaction between regular and irregular elements. He revealed that historically, many wars had seen both regular and irregular elements fighting; however, these elements traditionally operated in different theatres and/or in different formations. He hypothesized that in the future, this may no longer be the case. In fact, he declared that it would not be unusual for the irregular element to become operationally decisive, rather than just being relegated to the traditional role of a secondary player.[95]

Hoffman's ideas regarding the simultaneous use of multiple forms of warfare, the employment of state level Hybrid War, hierarchical political structures employing decentralized cells, and the emergence of the irregular element as a decisive, or at least equal, partner in conflict are in large part proving to be correct. It is important to remember that Hoffman was interpreting Hezbollah's actions and performance in 2006. As Hezbollah was developing its capabilities based on the prescribed evolution of Mao's *People's War* fighting doctrine, one could argue that Hoffman was simply interpreting Hezbollah's application of that doctrine, not something new. Regardless, Hoffman's analysis insightfully makes the connection between Hezbollah's application of Mao's *People's War* at the tactical and Colonels Qiao Liang and Wang Xiangsui's concept of state-level Hybrid Warfare in *Unrestricted Warfare*.

After the 2006 Lebanon War, Hezbollah again undertook an extensive after-action review of its performance, concluding that although its forces had performed well overall, some areas needed improvement. Specifically, there were weaknesses in the areas of marksmanship, small unit tactics, and the exposure of battlefield defences and weapons depots that needed to be addressed. However, its lack of air defence was considered a "serious problem" and an area that needed to be urgently dealt with.[96]

From an operational perspective, the war had weakened the group's overall position in Southern Lebanon, as the UNSC resolution that ended the war forced Hezbollah to abandon its vast network of underground bunkers and fortifications in southern Lebanon.[97] However, with help from Iran, Hezbollah was able to continue growing its weapons arsenal, manpower, and intelligence capabilities.[98] Moreover, after the war, the group started to evolve its practices and began exporting its knowledge and capabilities to other countries within the region.

Hezbollah's Involvement in Syria

In March 2011, the Syrian government faced a serious threat to its authority when pro-democracy protests began to erupt throughout much of the country. The Syrian government responded with force to suppress demonstrations, using police, military, and paramilitary forces in an attempt to regain and maintain order. Opposition militias began to

form from these uprisings and by 2012, the unrest and violence had expanded into a full-scale civil war.[99]

By the end of 2012, rebel groups had been able to achieve a number of tactical successes over government forces on the ground. These successes had forced the government to withdraw from many of the northern and eastern parts of the country. This retrograde included Aleppo, Syria's largest city, where rebels took control of part of the city. However, by early 2013, rebel forces had overextended themselves and were unable to make further progress. The situation was not helped by the fact that they lacked the heavy equipment, weaponry, and organization to capitalize on the situation. Government forces, on the other hand, had been weakened by defections, and were unable to retake any of the lost territory so the situation became stalemated. Daily fighting did continue, but the situation on the ground remained unchanged.[100]

Hezbollah's involvement in the civil war was the result of the strategic alliance between Iran, Syria, and Hezbollah. Specifically, Syria is a vital conduit between Iran and Hezbollah and neither Iran nor Hezbollah could afford to risk losing its access to that Syrian support. Moreover, the Assad regime had provided safe havens for Hezbollah's training camps and weapons storage facilities.[101] As Marisa Sullivan, a Fellow at The Institute for the Study of War (ISW), points out, it was through this relationship that Hezbollah entered the conflict and played a key role.[102]

There has been much speculation on the various contributions Hezbollah made to the overall war effort, however, there is little question regarding their impact on the battlefield, which was significant. At the tactical level, Hezbollah trained National Defence Forces (NDF) paramilitaries at military bases across Syria. This training proved instrumental in cultivating a light infantry force that helped the regime hold cleared terrain.[103] Hezbollah fighters also augmented Syrian forces, providing advice and training for Syrian military and paramilitary forces, either in an embedded or partnered capacity. The group also assumed a direct combat role alongside both Syrian military and paramilitary forces.[104]

In April 2013, Hezbollah's involvement in Syria shifted significantly when it was given direction to plan and lead the assault on al-Qusayr, a primarily

Sunni town in Homs province, not far from the border with Lebanon. This battle was noteworthy because Hezbollah not only operated within a much larger force structure than in its previous operations, but they were also responsible for almost all of the planning and conduct of the actual operation.[105]

Al-Qusayr itself was important because it served as a logistical conduit for the anti-Assad revolt, facilitating the movement of weapons and militants between Lebanon and Homs. Lebanon's northeast Bekaa Valley is home to a Sunni population, most of which sympathized with the Syrian opposition. Syrian rebels and Lebanese volunteers infiltrated Syria from Lebanon via the flat, arable Masharei al-Qaa district and the adjacent arid mountains to the east.[106] Moreover, the highway linking Damascus to the Mediterranean coastal port town of Tartus runs between Homs and Qusayr. Rebel control of Qusayr and parts of Homs threatened regime traffic.[107]

The Syrian government launched its offensive against al-Qusayr in May 2013, and after a period of bitter fighting was able to successfully push rebel troops from the town in early June of that same year.[108] What is interesting about the fighting in al-Qusayr is that it revealed a new approach to conducting operations for the government.

In this battle, government forces used a combination of conventional and hybrid fighters, and both were supported by heavy weapons and airpower. Tactics highlighted a sophisticated level of operations which included heavy preparatory bombardment, which covered the infiltration of irregular allied units. This penetration was followed up by armour-supported heavy infantry advances.[109] Moreover, the operation was achieved through the coordination of different chains-of-command, a difficult task even for the best militaries. What should make this operation of interest to Western analysts is the fact that government forces cooperated closely with Hezbollah leadership in combining regular, irregular, and allied units, each with very separate capabilities and functions.[110]

In the end, the victory at al-Qusayr marked an important turning point in the conflict. First, it dealt a major blow to rebel forces militarily and

psychologically. Al-Qusayr also began Hezbollah's overt involvement in Syria, which went on to play an important role in the Syrian government's success. Government forces quickly followed up this victory with offensives to regain the remaining territory in Homs, followed by Aleppo and areas around Damascus.[111]

Reports suggested that Hezbollah's forces were far better trained, disciplined, and experienced than any of their Syrian or Iraqi counterparts and that they tended to improve the overall combat effectiveness of the less-capable Syrian units when they were assigned to them.[112] In fact, many rebel commanders reported that fighting Hezbollah troops was much more difficult than fighting against regime troops because "they are better fighters" and "more professional" than the Syrian army.[113]

With the help of Hezbollah's leadership and fighters, along with those from Iran, and Iraq, Syrian government forces were eventually able to demonstrate a remarkable ability to adapt their military tactics on the battlefield and to become more effective fighting against the insurgency. Hezbollah's efforts in this regard likely helped to shift the local balance of power in the government's favour. According to Elizabeth O'Bagy, a senior policy advisor at the U.S. Senate, "Hezbollah has proven to be much more effective in confronting rebel forces as they have better experience in guerrilla tactics, unlike the ranks of Syria's conventional army." She continued, "moreover, Hezbollah has played a key role in the regime's development of effective irregular forces and knowledge of dealing with a combination with regular and irregular regime elements."[114]

During the course of the civil war in Syria, Hezbollah deployed a substantial amount of its manpower into the country, where it carried out both counterinsurgency and large-scale operations. Most sources tend to agree that this deployment has harmed Hezbollah's morale and public image, while improving the group's ability to conduct large-scale manoeuvres and better interoperability with allied forces.

As late as 2017, Hezbollah's military operations still included thousands of fighters deployed to Syria supporting the Assad government. It also had about 250-500 fighters in Iraq training the Shiite-dominated Popular Mobilization Forces. It is also believed that there are also about 50 fighters in Yemen on a covert train-and-support mission for Houthi rebels.[115] In

this regard, Hezbollah has taken over the role of providing training and advisors to other armed non-state groups supported by Iran.

The Next Stage in Hezbollah's Development

Clearly, Hezbollah transformed its military wing from a militia to a guerrilla army in the early 1990s and moved towards becoming a more mobile/conventional light force during the early 2000s. These transformations were at least part of the reason it performed so well in the 2006 conflict. Moreover, its regular military capability became significantly better with its experience in Syria, as its top commanders gained experience in operational command. So, given its development process to date, what is the group's most likely next move?

After 2006, the group's number one priority was to establish an effective air defence system in the south. As operations in 2024 play out, it is unlikely this priority has changed. Moreover, it is probable that significant investments in air defence systems will be attempted in order to reduce the IDF's ability to retaliate at will. This will remain a prime focus of Hezbollah's force development efforts into the foreseeable future.

Historically, whenever Hezbollah has improved its weapons capabilities, it has done so with the appropriate changes to its doctrine and tactics to maximize performance. This adaptation was the case when they adopted the *People's War* doctrine as a foundation on which to build their guerrilla army in the late 1980s and early 1990s. The group again used an adaptation of China's active defence concept in 2006 to develop its warfighting concept. As most of their capability development focus will likely now be on air defence and missile strike capabilities, it is reasonable to conclude that Hezbollah will attempt to develop its own version of an Anti-Access/Area Denial (A2/AD) strategy. Although, it is clear the group does not yet have that integrated and wide-ranging air defence system in place. Recent clashes between the group and IDF have shown evidence of progress in this area.

For example, the IDF has reported it intercepted surface-to-air missiles that were fired from Lebanon at Israeli UAVs on 25 & 28 October, 1, 12 & 18 November and 16 December 2023. In addition, Israel believes similar missiles may have been fired at Israeli helicopters on 20 December 2023.[116]

The overall success rate of both surface-to-air and surface-to-surface attack intercepts appears to be changing slowly as it is becoming more challenging for the Israeli system to deal with the higher technological missiles that are starting to be fired at its aircraft and into Israel. The improvement of Hezbollah's air defence capability, especially with the introduction of the 358 interceptors and the Sayyad-2 missile system, will not help the overall situation.[117] For instance, the Iranian Sayyad-2 can cover the medium range and high altitudes and has a combined guidance system. Interestingly, the launcher of the Sayyad-2 missile, which consists of four canisters in a two-on-two, configuration is similar in design to the American MIM-104 Patriot SAM system launchers.[118]

With a large stock of unguided missiles and a much smaller supply of guided systems, it is likely that Hezbollah is exploring and has started using the concept of a two-phase missile attack. Phase 1 would see hundreds of unguided systems used in "saturation attacks" to overwhelm Israel's Iron Dome system. As the systems within Iron Dome are reloading, Phase 2 would commence with guided systems (including drones) going after key targets such as surveillance installations, communications facilities and other high value targets. The main problem for Hezbollah in this situation is understanding the depth of the system they need to breach. This issue will take time to analyze in order to find the right/best solution.[119]

Once in place, an effective A2/AD system would become a game changer for Hezbollah. IDF air attacks would become less frequent and effective so unless ground forces move in to capture or destroy such systems, the IDF's options become limited. Moreover, should Israel decide to launch a ground attack, the IDF will be fighting a war on Hezbollah's terms.

Key Lessons from this Chapter

There are a number of lessons that can be taken away from this study on the development and continued existence of Hezbollah. These include:

- From its inception, Hezbollah had the advantage of receiving weapons, equipment training and support from a professional military force, Iran. Having these requirements fulfilled for them allowed the group to focus its efforts on increasing its battlefield performance, unhindered by resource or financial constraints.

- Hezbollah has put a lot of importance in having well-trained light infantry forces, with overmatch capabilities such as long-range AT weapons and mortars. This weaponry has given them the ability to hold off heavy forces in battle for a period of time.

- The group has adopted a form of mission command and has pushed command authority down to the lowest levels possible.

- Hezbollah has made significant advances in its combat capabilities such as the employment of long-range weapons, first with unguided rockets and then with AT weapons. This capacity has provided the group with the all-important standoff capabilities to effectively overmatch and hit at Israel and the IDF, thus helping to create a more level playing field with it enemy.

- Hezbollah has improved its weapons capabilities with the appropriate changes to doctrine in order to maximize it performance.

- Hezbollah understands the importance of long-term strategy and the need to stay focused on it goals. It has also proven to be a learning organization that has adapted to the changing circumstances it has faced.

- Hezbollah has developed and improved its overall capabilities by following Chinese doctrine. First with *People's War* and then with an adaptation of active defence. The evidence now suggests Hezbollah is likely in the process of moving to the next stage of Chinese doctrine evolution with the development of its own version of an A2/AD (Anti-Access/Area Denial) strategy.

Over the course of its existence, Hezbollah has evolved from a relatively small group of revolution-oriented conspirators into the most powerful organization in Lebanon. In the process, it has progressed from a small militant force into a guerrilla army and finally into a regional military actor with significant "hybrid" capabilities. Hezbollah's strategy combines a logical approach focused on long-term objectives to achieve its success. The main reasons for its success have been its continued resistance to Israeli occupation, combined with institution-building, the

development of social services and active political participation within the country. Arguably, its military capability has formed the foundation upon which much of its success in achieving political power, public support, and legitimacy has resulted. That being said, it is likely that little of this success would have been possible without the extensive support from Iran.

It has become popular for Western governments to classify organizations such as Hezbollah as little more then terrorist groups. Although, this depiction is useful in creating a simple picture of good and evil for public consumption, problems arise when governments and the people who advise them start to actually believe this to be the case. In reality, Hezbollah is a resilient, multifaceted and complex organization that has proven it can take whatever the IDF can dish out and survive. More importantly, it is not developing a new fighting construct, rather it is employing and evolving with an established doctrine.

Although Hezbollah has provided modern armed non-state actors with a template for long-term success using the *People's War* doctrine, actually gaining and maintaining that success is often more difficult than it appears. This paradox is due to the fact that adherence to its principles is critical for its success. For example, the movement did not grow beyond a small militia until it was able to win over the support of the people. Not winning over the people will eventually result in defeat. This outcome is precisely what happened to ISIL.

Despite impressive results of the battlefield, ISIL was unable to attain the most important objectives within the insurgency's framework. It failed to achieve the strategic requirement of winning the hearts and minds of the people. Moreover, it was never able or just unwilling to make long-term strategic alliances with other groups that could have aided its success, such as with the Kurds. These miscalculations eventually resulted in its downfall.

That being said, ISIL is an interesting case study from a military perspective of modern armed non-state actors. This is due to the fact that the group was able to progress to a hybrid force of guerilla and regular army units

without external support, and once they reached that capability were able to demonstrate exceptional abilities in the application of mobile warfare. They also showed a mastery of integrating conventional and irregular tactics into an overall campaign design. Moreover, its eventual defeat by the Iraqi military and coalition forces is evidence that these forces can be defeated if their weakness are well understood and exploited.

CHAPTER 9

THE ISLAMIC STATE OF IRAQ AND THE LEVANT (ISIL): TAKING ADVANTAGE OF VULNERABILITIES

The stunning success of ISIL between 2012 and 2014 in both Northern Syria and Iraq, along with similar performances by other such groups in the region, shocked the world and demonstrated the power and reach that such organizations can now achieve. The foundation of this success was also derived from the fact that ISIL used the tried and tested principles established within the *People's War* doctrine.

Like Hezbollah, the group was able to enhance this doctrine by integrating contemporary international trends such as globalization, the expansion of network-based approaches to organizational constructs, and advances in technology into their fighting techniques. Moreover, they benefited from direct assistance from decommissioned Saddam Hussein-era military commanders, specialized staff officers, training cadres and the acquisition of captured state-of-the-art weapons.

One of the main problems ISIL faced during its existence as a hybrid force was an inability to compromise its stance regarding Islamic fundamentalism and Sharia law. This lack of flexibility prevented the group from gaining the support of the people, so once military operations started to go wrong for them, they had nothing to fall back on. This section will examine the rise of ISIL and how it used the key elements of insurgency doctrine to establish itself in Iraq and Syria. It will then analyze its strengths and weaknesses in implementing that doctrine and how its shortcomings ultimately led to its defeat.

BACKGROUND AND HISTORY OF ISIL

The organization that eventually became known as ISIL had its genesis as *Jama'at al-Tawhid wal-Jihad*, a Jordanian Sunni insurgency group that

formed in 1999. The main purpose of the group was to overthrow the monarchy in that country. However, after the American invasion of Iraq in 2003, it became one of many decentralized militant networks fighting against the coalition forces and their Iraqi allies.[1]

Despite being one of many militant groups *Jama'at al-Tawhid wal-Jihad* stood out for its brutally. It viciously targeted Iraqi security forces and anyone else it perceived as supporting the occupation.[2] Its tactics varied, but initially included a mix of suicide bombings, kidnappings, beheadings, the planting of IEDs, and ambushes.[3]

In October 2004, Abu Musab al-Zarqawi, a long-time jihadist and leader of the organization, pledged allegiance to Osama bin Laden. As part of the al-Qaeda network, the group became known as *Tanzim Qaidat al-Jihad fi Bilad al-Rafidayn* (commonly referred to as al-Qaeda in Iraq or AQI).[4] It was under this group that Al-Zarqawi formulated his overall strategy to unhinge American operations in Iraq. To do this he attempted to draw coalition forces into a sectarian Sunni-Shiite war through the broad use of targeted terror attacks.[5]

One such attack occurred on 22 February 2006, when AQI bombed the Shiite Askariyah Shrine in Samarra. Although there were no casualties, the attack prompted outrage within the Shiite community and resulted in a number of retaliatory strikes against Sunni mosques. The attack achieved the desired result of increasing violence between Shiites and Sunnis. However, it also created significant backlash against the group within the Sunni community.[6]

On 7 June 2006, Zarqawi was killed in a coalition air attack and was replaced by Abu Ayyub al-Masri. Under al-Masri's leadership, AQI continued the unrestricted use of terror. Unfortunately for the group, these attacks increasingly targeted Sunnis. By the end of 2007, the backlash from these attacks against the Sunni community had become so severe that it pushed many tribes into cooperating with American coalition forces.[7]

This Sunni cooperation became known in the West as the Anbar Awakening and its support greatly increased the overall effectiveness of government security operations. Over time, AQI, which had now been

renamed the Islamic State of Iraq (ISI), was almost completely destroyed.[8] In fact, by early 2008, it was estimated that government security forces had killed approximately 2,400 ISI members and captured about 8,800 others.[9] On 18 April 2010, ISI's two top leaders, al-Masri and Omar al-Baghdadi, were killed in a coalition air raid near Tikrit, paving the way for Abu Bakr al-Baghdadi to become the group's new leader.[10]

Although the Iraqi government's success against ISI during the Anbar Awakening was significant, it proved to be temporary. The group was saved by the coalition withdrawal from Iraq in December 2011. In addition, the government's lack of inclusiveness towards Sunnis, as well as its clumsy attempts to put down unrest in Sunni dominated areas, resulted in a continual state of discontent.[11]

Al-Baghdadi took advantage of the American departure and government hostility towards the Sunnis to rebuild his organization. One of his first and most important steps was to recruit a number of ex-senior military officers from the former Saddam Hussein's Army. This move allowed him to build a professional organization with world-class intelligence, security, and military capabilities. Moreover, it laid the foundations for ISI to recreate itself from a terrorist group into a full-fledged insurgency organization. Incredibly, this process occurred within little more than a two-year span.[12]

ISI'S MOVE INTO SYRIA

While the group was still recovering from the effects of the Anbar Awakening, ISI's leadership decided to take advantage of the weakened central Government of President Bashar al-Assad and moved into Syria. Under the leadership of Abu Mohammad al-Golani, members of the group experienced in guerilla warfare crossed the border into Syria in late 2011. They called themselves *Jabhat al-Nusra l'Ahl as-Sham* (Support Front for the People of the Sham) and by the second half of 2012, had established a reputation as a highly disciplined and effective fighting force.[13]

As *Jabhat al-Nusra l'Ahl as-Sham* was fighting Syrian government forces under the direction of ISI, al-Baghdadi began establishing a political presence among the Sunni-majority areas within the northern provinces

of Ar-Raqqah, Idlib, Deir ez-Zor, and Aleppo.[14] ISI started its takeover of these provinces by targeting specific villages. Once a village had been selected, the group would open an Islamic missionary centre.

The official purpose of these centres was to provide humanitarian relief. However, their main activity was the recruitment and training of followers to act as spies. According to Christoph Reuter, a reporter for *Der Spiegel*, "Of those who came to listen to lectures and attend different courses on Islamic life, one or two men would be selected and then instructed to spy on their village or local area to obtain information."[15]

The information that these spies were expected to gather was wide ranging and included such things as: a list the powerful families, names of powerful individuals in these families, their sources of income, the names and the sizes of (rebel) brigades that were operating in the village, the names of the leaders who controlled the brigades and their political orientation.[16]

As soon as the group had identified sufficient spies, they would begin to expand their presence. This infiltration was done covertly at first by renting apartments in strategic locations where they could store weapons and house their men. Once ISI felt it had gained sufficient strength in an area it, would start openly displaying its presence using black flags and blocking off streets to mark off and secure its territory.[17]

The idea was to expand its power base while avoiding open resistance. As a result, infiltration, surveillance, and espionage were critical to their operational success. According to Anne Speckhard and Ahmet S. Yayla, ISI documents captured in Aleppo confirmed that ISI had developed a highly complex system of monitoring all the groups and individuals opposing it. They state, "In the captured ISIL archives from Aleppo were long lists identifying the informants installed in each rebel brigade and government militia. These lists even noted who among the rebels was a spy for Assad's intelligence service. The lists also confirmed instructions for ISI cadres to strategically marry into influential families ahead of overtaking villages, thereby gaining their loyalty and allegiance before ISIL would take full power."[18]

Once its presence was firmly established ISI was extremely brutal in its consolidation of power. It would systemically clear the area of all potential threats. Reuter explained, "the phase of infiltration was followed by the elimination of every person who might have been a potential leader or opponent."[19] These people would simply be kidnapped by masked men and killed while ISIL publicly denied any involvement in such activities.[20]

This pattern repeated itself in different towns, villages, and provinces until much of Northern Syria had been secured by the group. In many cases the process was so opaque that it completely surprised local residents. In fact, many did not realize what was happening until it was too late and ISI was already in control. This strategy allowed the group to avoid heavy battle losses as it attempted to consolidate and expand its strength. Speckhard and Yayla point out ISI was able to rely on "surveillance, espionage, murder, and kidnapping to pave the way for the creation of the powerful totalitarian state structure of the "Islamic State."[21]

As ISI was establishing its control over Northern Syria it chose Raqqa as the base of its insurgency in that country. According to insurgency doctrine the base is the political, economic and military hub of its existence. It is used to provide protection for its forces, a house for its supplies, and it becomes a platform from which to expand its power. As such, the placement of the base must consider a number of factors including the geographical conditions, the enemy's situation, the population, the ability to develop political power and mass, among others. In many of these criteria, Raqqa was a perfect fit for the group.

Before the start of the civil war, Raqqa had a diverse population of nearly 300,000 residents, with Sunni Arab tribes making up the majority of the citizens within and around the city. Once the rebel uprisings against Syrian President Bashar al-Assad started, Raqqa became the refuge for many anti-government protesters from different Syrian cities.[22] More importantly, it was located in a remote oil-rich province on the north bank of the Euphrates River far from the control of the central authority. Other important factors in Raqqa's favour were its proximity to the Iraqi border and the strong ties of its tribes to Iraqi clans. These links allowed ISI to freely operate back and forth between the two countries according to shifting operational needs.[23]

BUILDING UP A MILITARY CAPABILITY

Although the sophisticated use of tactics such as surveillance, espionage, murder, and kidnapping worked well against the population protected solely by fragmented rebel forces, they were not enough to defeat established authorities such as the governments of Syria or Iraq. For this ISI needed a combat force of its own.

On 8 April 2013, ISI leader Abu Bakr al-Baghdadi publicly announced that he had created *Jabhat al-Nusra* and was now merging it with ISI to form one organization under this command. This group now called themselves the *Islamic State of Iraq and the Levant* (ISIL), although most Western press and government spokespeople called the group Islamic State in Iraq and Syria (ISIS).[24] However, al-Golani rejected the merger and after a bitter conflict the two groups ended up going their separate ways.[25] With its designated fighting force in the country and *Jabhat al-Nusra,* no longer being part of the group, ISIL needed to regenerate a military capability for its operations in Syria almost from scratch.

Shortly after its arrival in the country ISIL had established several military training camps. By the end of 2012, these camps were set up and fully functioning.[26] Moreover, they were well organized, inconspicuous and located in remote areas to prevent anyone from getting too close and interfering with their operations. Unlike other rebel groups in the country, which relied on local recruits, ISIL focused all of its efforts on recruiting foreign fighters. Unfortunately, most of these newcomers arrived in country with little or no military experience.[27]

As a result, all newcomers were expected to undergo at least two months of military training and were drilled to be unconditionally obedient to the central command. Once they had completed their basic training, they were placed under the command of battle-tested Chechens and Uzbeks, which significantly increased their overall combat effectiveness.[28]

ISIL's strategy of avoiding open combat with local rebel brigades had initially worked well for the group. They had been able to expand rapidly, and although they had to fight often, they were never confronted by any type of a unified resistance.[29] This situation changed in December 2013. As rebel leaders began to appreciate the scope of the growing threat ISIL

represented, they decided it was time to act and neutralize the threat. As a result, they attacked them with a series of coordinated assaults that were able to push the group out of large regions of Northern Syria. It was only the timely arrival of 1,300 fighters from Iraq that stabilized the situation and saved the day for ISIL in Syria.[30]

THE MILITARY STRATEGY AGAINST THE ESTABLISHED AUTHORITY

Having firmly established and consolidated its base within the Sunni communities of both Iraq and Syria, ISIL turned its attention to extending its concept of an Islamic Emirate even further. Key to achieving this objective, at least in the short term, was the group's ability to continue destabilizing the political situation in both these countries. The group reasoned that as various anti-government factions were actively engaged in fighting Syrian government forces, they could focus their efforts on Iraq.[31]

In pursuing its strategy in Iraq, the group hoped to fragment the government to the point that it would never be able to fully recover its authority over the country. To this end, ISIL's military objectives for the campaign focused on destroying the government structure, degrading and possibly destroying the Iraqi Army, as well as ensuring that Baghdad could no longer remain a viable Shi'a capital.[32]

To achieve its initial objectives, ISIL required the ability to clear government forces from Sunni dominated areas, defend the newly created nation and have sufficient strength to pose a long-term viable threat to Baghdad and Southern Iraq. ISIL leadership reasoned that this plan could be accomplished through a combination of conventional and irregular military operations supported by an extensive campaign of intelligence gathering, espionage, and terror.[33]

DEVELOPING ITS CONVENTIONAL AND HYBRID MILITARY CAPABILITY

ISIL had already developed a significant level of expertise with irregular military operations and had in place much of the capabilities it needed

to carry out an effective campaign of intelligence gathering, espionage, and terror. However, the group had little or no experience with large-scale military offensive operations. In order to defeat the Iraqi Army, they would need to generate this capability. As such, ISIL started building toward this by conducting a series of small-scale attacks and working up to larger operations. In addition, it also created an extensive capacity to carry out sustained nation-wide attacks using Vehicle-Borne Improvised Explosive Devices (VBIED).[34]

The development and active use of this capability had the benefit of allowing the group to continue its pressure on the government while it created an effective infrastructure for the command and control over a distributed ground force.[35] Experimentation also allowed VBIED operations to become integrated into combined arms attack against fixed sites, such as prisons, checkpoints, and police buildings.

As part of its preparations for offensive operations, ISIL announced the start of the "Destroying the Walls" campaign on 21 July 2012. The main objectives of this campaign were to secure the release of Muslim captives and retake territory that had previously been controlled by the group. During the one-year period of this campaign, there were eight attacks on Iraqi prisons with an estimated release of 1,000 prisoners. In July 2013, the group successfully broke out approximately 500 prisoners from Abu Ghraib prison alone.[36]

Sam Wyer, from the Institute for the Study of War, commented, "The 'Destroying the Walls' campaign indicates the degree to which ISIL has grown in its ability to plan, coordinate, and execute attacks since the withdrawal of U.S. forces."[37] He added, "the attack wave demonstrates a nation-wide command and control capability to synchronize attacks from Mosul and Kirkuk in the north to Basra in the south."[38] In fact, Wyer concluded that by the end of 2013, "ISIL had likely developed military headquarters commanding operations in separate zones in northern Diyala, the Jazeera desert west of Tikrit, and the Thar region north of Abu Ghraib."[39]

Despite its ongoing successes against Iraqi government forces, there were setbacks for the group. For example, in mid-2013, ISIL began attacking three Kurdish enclaves that bordered their territory in northern Syria.

Strategically, the group needed control of the Kurdish regions near the border with Turkey in order to secure an uninterrupted flow of operatives, recruits and weapons into the areas it occupied. Possession of the area would also prevent its opponents from linking up with foreign supporters.[40] However, ISIL was unable to achieve any of its objectives in this area. In fact, over the next year the group launched repeated attacks against the Kurdish People's Protection Units (YPG) and the armed wing of the Syrian Kurdish Democratic Union Party (PYD), with little or no success.[41]

THE TRANSITION TO CONVENTIONAL MILITARY OPERATIONS

Despite these setbacks, by early 2014, it was clear that ISIL's move into Syria had paid off for the group. It had provided it the time, resources and the necessary experience to not only re-equip and recover, but also to expand its fighting strength and capabilities. As the group would soon demonstrate, this period of recovery had transformed the organization into a formidable military force. It was now capable of fighting and winning a variety of different types of tactical battles against forces from the established authority in Iraq. Moreover, the political conditions in Iraq were now also moving in ISIL's favour.

During late 2013 and early 2014, Sunni militias in central Iraq went onto the offensive, taking over much of Fallujah and Ramadi and pushing the Iraqi Army out.[42] Although government forces immediately began counter-offensives into the Anbar region, their ruthless methods did more to alienate the Sunni tribes and their peoples than it did to secure the province.[43] Taking advantage of this discontent, ISIL launched a major offensive, striking towards Mosul and three cities north of Baghdad: Baiji, Tikrit and Samara.[44]

The operation proved surprisingly swift and decisive as the Iraqi army collapsed under very little pressure and in many cases without firing a shot. This gave ISIL a rapid military and complete propaganda victory.[45] Mosul, the second largest city in Iraq and an important crossroads between Iraq, Syria, and Turkey, was quickly captured. With that victory, ISIL declared a 'Caliphate' that included parts of both Syria and Iraq.[46]

FIGURE 10: Map of ISIL Control in Iraq[47]

As conventional military (mobile) operations were unfolding around Mosul, ISIL intensified its irregular campaign. This offensive included carrying out coordinated attacks on government installations as well as on the Shi'ite population in areas still under the Iraqi regime's control. These attacks were specifically targeted at undermining the regime's authority and forcing the army to redeploy its units from the main area of operations to secure its rear areas and vulnerable points.[48]

During August and September of 2014, ISIL continued its offensive south, attempting to take control of Baiji and Samara, while also pushing to extend its control into northern Iraq. By this time, both Kurdish forces and the Iraqi army were benefitting from increased American

aerial support. This assistance allowed both groups to put up a far more determined resistance that effectively brought the ISIL offensive to a halt.[49]

In an effort to consolidate control over the remainder of Al-Anbar, ISIL renewed its attack in that Sunni province at the end of September 2014. The main targets of this offensive were the cities of Ramadi and Haditha, which were well defended by Iraqi army forces. During the fighting ISIL, was able to secure a series of victories including Camp Saqlawiya outside of Fallujah, Hit, Kubaisa, Muhammadawi, and finally Ramadi. These successes put ISIL into a position where it directly threatened western Baghdad.[50]

PLANNING FOR THE FUTURE

These victories became the high-water mark of ISIL's advances in Iraq. The last series of attacks in September 2014 were seen by many Western analysts as the group attempting to position itself for an eventual attack on Baghdad. According to Jessica D. Lewis, Research Director at the Institute for the Study of War (ISW), ISIL's urban campaign in Iraq had revealed its future objectives. These included:

- Permanently break down political boundaries in Iraq, Syria, and the region by cultivating conditions for government failure and/or sectarian civil war;
- Establish the Islamic Emirate by controlling terrain across Iraq and Syria, governing the population within, and defending against external threats;
- Bring like-minded people to fight alongside and settle within the Islamic Emirate; and
- Expand the territory of the Emirate and connect it to the wider Muslim community, or the Ummah.[51]

Despite its careful strategic positioning around the city, analysts do not believe that ISIL would have been able to successfully take Baghdad by military attack as they had done with Mosul. Many believe that ISIL was

more likely to have besieged the city and attempted to disrupt life to the point where it would eventually surrender. It is possible that this would have been done by cutting off the main roads leading into and out of the city.[52] Lewis, for example, believed that ISIL would have likely attempted to besiege the city by using a previous plan developed by AQI for the control of Baghdad, which called for securing its surrounding belts.[53] Regardless of the method it employed, had ISIL been able to blockade the city for an extended period, it would have likely gone a long way to achieving the group's goal of preventing Baghdad from remaining a viable Shi'a capital.

THE BATTLE WITH THE IRAQI AND SYRIAN KURDS

ISIL's June 2014 advance into northern Iraq drew Iraq's Kurdish population into the conflict, as they sent their forces into areas abandoned by the Iraqi army. In August of that year, ISIL launched an offensive against the Kurds who initially withdrew from several areas including Sinjar, but overall held firm.[54]

In September 2014, ISIL launched a direct assault into the Syrian Kurdish area, this time near the town of Kobane. Fighting forced thousands of people to flee across the Turkish border and after prolonged fighting between the two sides, Kurdish forces were able to regain control of the area. Strategically, these failures would prove extremely costly for ISIL. Their attacks forced the Kurds into an alliance with the American-backed Syrian Democratic Forces (SDF). Aided by U.S.-led coalition airpower, Kurdish forces were able to eventually drive the group out of much of Northern Syria. More importantly, it also allowed the Kurds to maintain firm control along the border area with Turkey.[55]

ISIL'S ADMINISTRATION OF OCCUPIED TERRITORIES

A key aspect of the political and social elements of any insurgency is the insurgent's ability to establish an alternative government structure in the areas they have taken over. Once ISIL had started its move into Styria, it needed to govern increasingly wider areas and larger populations. According to a RAND study, at its peak in late 2014, ISIL held almost 100,000 square kilometers of territory, which included a population of nearly 12 million.[56]

This span of control meant ISIL needed to set up a large government-type administration to replace those in both Syria and Iraq which had essentially collapsed during the fighting. Everything from education, law enforcement, and municipal services, to taxation and defence had to be put back into place. According to several sources, ISIL was able to maintain a relatively high level of local services simply by changing as little as possible in the areas it governed.[57]

This transition was aided by the fact that many of the civil servants that allowed the cities to function had remained at their jobs and were in fact still being paid by the government. In Raqqa for example, "school teachers, state telecoms company employees and municipal workers all remain at work, under ISIL control but paid by Damascus." In these cases, ISIL simply placed its own leadership at the top of existing institutions to make sure employees were following ISIL's directives.[58]

The group did add their own policies to the framework. For example, ISIL quickly started revising school curriculums, setting tariffs for waste disposal and banning litter. In one ISIL communiqué issued to residents of Mosul and the surrounding Ninawa province, it stated, "Waste is not to be thrown away and gathered in a strip of vacant land, and all who deliberately throw away waste thus will incur a fine of 25,000 dinars [around $22] or be held in custody in the event of refusal to pay the fines."[59] In an attempt to curb illegal fishing in Deir ez-Zor province, along the River Euphrates, "ISIL banned fishing during the spawning season and the use of dynamite for fishing." It also banned electric current fishing, whereby two electrodes deliver a current into the water, because, "it leads to extermination of many river/water creatures as well as congenital disfigurement for small fish and other river creatures."[60]

According to many reports, local populations that remained under the control of the group appeared to have come to terms with the occupation and occasionally even supported it. This reaction was likely due to the organization's ability to restore daily life to the status quo by providing basic services, and filling the administrative void that was created when the government structure collapsed.[61] According to Aymenn al-Tamimi, a researcher at the Philadelphia-based think tank Middle East Forum, "I wouldn't say on the whole it's a better quality of life than

most Arab states, but what they do bring, that gives them a one-up, is their totalitarian model." He added, "It brings this sense of order in a time of civil war."[62]

Although it created an efficient infrastructure to provide services, the main goal, like any totalitarian organization, was to control the people. To do this, ISIL imposed their version of Sharia Law on the population, who were forced to adopt the code or be severely punished.[63] More importantly, educational, judicial, policing and law enforcement networks were all developed under ISIL to not only provide services but also to enforce its ideology and keep the local population under close surveillance.[64] According to Reuter, the plan was to produce, "a caliphate run by an organization that resembled East Germany's notorious Stasi domestic intelligence agency…the goal was to have everyone keeping an eye on everyone else."[65] The group continued making extensive use of spies and implemented brutal measures against its opponents and any minorities unlucky enough to be living under its control.[66]

Under ISIL's occupations, brutal measures included the liberal use of executions that targeted the Iraqi army, government officials and ethnic and religious minorities that ISIL regarded as "infidels." The executions were publicized on the group's social network sites as a means of deterrence to enemies at home and abroad. They did achieve the desired effect, as targeted groups would leave their homes en masse ahead of any reported ISIL advance. Moreover, the mass exodus of residents added to the Iraq Government's problem of displaced persons.[67]

According to Metin Gurcan, a Turkish security analyst and columnist with *al Monitor*, such terror polices had a strategic purpose. He asserts, "Their use of violence is not indiscriminate one but a strategic one serving to the purpose of creating a sterile environment. Simply, their aim is to drive the unwanted out of the captured lands and building a 'sterile' human population in sectarian terms in the controlled territories." He added, "This strategy provides ISIL a submissive human population and thus makes the holding phase easier to realize. This strategic use of fear and intimidation not solely for propaganda purposes but also for controlling the territory captured is another dynamic we have not noticed since 9/11."[68]

As ISIL did not have external support, they had to find other sources of income to fund their military and administrative activities. To do this the group used a verity of means. As they had taken over much of the state infrastructure in Syria and Iraq including a number of oil fields, the export of petroleum products was a main source of the group's income estimated at several million dollars a day.[69] Other sources of income included profits from various criminal activities such as extortion, collecting ransom for abductees, and trading in antiquities, as well as collecting donations and imposing local taxes. ISIL's ability to generate revenue allowed it to fund its military infrastructure and operations while providing an effective alternative system of governance to occupied territories.[70]

FORCE COMPOSITION AND ATTRIBUTES OF ISIL

At its peak, ISIL's military presence in Syria and Iraq was estimated to be around 10,000 armed fighters. About one third of those were experienced combat veterans. In addition, analysts believe there were also about 5,000 ex-Baathist cadres, local Sunni tribal structures, some local and transnational criminal networks and some other Salafi-Jihadist and around 10,000 local Iraqis, most likely Sunnis, working for ISIL in the areas of logistics, governance, recruitment, training and indoctrination. The complete force was estimated to be around 25,000 to 30,000 people with about 15,000 of those being armed fighters.[71]

Critical to its success was the fact that ISIL had developed into a professional and highly disciplined organization with many of the attributes associated with Western military institutions. They proved to be extremely good at adapting to changing situations and new developments on the battlefield. This adaptation was largely due to the fact that while they had a centralized decision-making and planning process, the execution of operations was usually based on the initiative of the commanders on the ground.[72] This particular ability made them masters at coordinated distributed operations.

There is also general agreement that the professionalism, military campaign design, and fighting style of the organization were derived in large part from a cadre of former Senior Saddam Hussein-era military officers who were intimately familiar with the terrain and demographic

dynamics. Moreover, they had the knowledge to exploit these dynamics when planning and conducting operations. As Lewis points out, "The ISIL style of warfare hybridizes terrorism, guerilla warfare, and conventional warfare." She argues, "The presence of the last indicates that the ISIL likely possesses a cadre of former Saddam-era military officers who know the military terrain in Iraq as their own."[73]

Metin Gurcan, a Turkish security analyst and columnist with *al Monitor*, expanded on this idea of ISIL's professionalism stating, "the military campaign design exhibited by ISIL … consistently demonstrated scope, distribution, deception, and timing as overarching strategic characteristics.[74] Gurcan observed:

> ISIL has been pursuing a phased campaign design as well. It has skilfully achieved building a balance between the phased campaign designs and maintaining the tempo of warfare. This could only be achieved with increased tactical and situational awareness and with the implementation of centered planning and de-centered execution… This is a strong indication of a unified, coherent leadership structure that commands from the top down.[75]

Andreas Krieg, a professor at King's College London who was embedded with Iraqi Kurdish fighters, agrees with these assessments. He explained, "ISIL local commanders receive overall orders on strategy but are given freedom to operate as they see fit to achieve them. That's a sharp contrast to the rigid hierarchies of the Iraqi and Syrian militaries, where officers often fear acting without direct approval."[76]

TACTICAL OPERATIONS

At the tactical level, ISIL proved to be a highly organized and adaptable fighting force. It had the ability to switch its operating concept between conventional attacks and guerrilla warfare with little difficulty. At times it would combine both by using the latter technique to wear down their opponents while massing the remaining fighters for a major attack. As time went on, these attacks would involve the coordinated use of armoured fighting vehicles, Humvees, and at times artillery. The group also incorporated suicide bombings into the initial phases of an attack by

having them infiltrate through enemy lines and setting off explosions just before the start of the assault.[77]

According to Petri Makela, a Finnish Security and foreign policy analyst, "When ISIL was on the offensive it would use its insurgence cells, set up in advance, in an attempt to create chaos among rear area Iraqi security forces until it was ready to take over the territory with fast moving motorized units."[78] This concept is reinforced by Reuter who states ISIL's playbook, "called for the infiltration of areas to be conquered with spies who would find out as much as possible about the target towns."[79]

On a number of occasions, ISIL highlighted its proficiency in attacking Iraqi military positions with coordinated company and battalion-size formations in order to clear towns and urban settlements. When conquering territory, its main tactic was to attack, hold and rebuild the settlements it had secured. This process was like the tactics Western forces attempted to use in their counter insurgency operations.[80]

ISIL AND POSITIONAL WARFARE

Unquestionably, these offensive tactics did not work once ISIL was forced onto the defensive. However, ISIL again proved adaptable in modifying its tactics to meet specific circumstances on the battlefield. According to Makela, some of the organization's units were designated to operate as layback cells, "fading into the population to harass advancing Iraqi troops." Other elements were used to conduct delaying operations along the major lines of advance by attacking lead elements that were following up on the withdrawing force.[81] This tactic allowed the group more time to prepare major defensive positions that were always focused in villages, towns and major centres. In cases such as Mosul, the defence plan would incorporate the surrounding area of settlements into the overall defence.

ISIL's tactical defensives were based on a ring defence with less reliable jihadists manning the outer perimeter of settlements. "ISIL allowed the attacking force to take them over, with relatively light resistance. IED, VBIED, ATGMs and sniper attacks were used to cause attrition on the lead elements of Iraqi troops delaying them for as long as possible.[82]

Once the Iraqi army reached the main defensive positions, which were usually based on a built-up area, they would attempt to send motorized light units into the main streets, however, ISIL would always develop obstacle belts to funnel these troops into kill zones where they would be subjected to intense assaults using IEDs, VBIEDs, RPGs and small arms fire."[83]

After the failure of an Iraqi assault force, ISIL would launch relentless waves of counter attacks with platoon and company sized units that would contain suicide bombers and sappers. These assault units were usually extremely motivated, well rehearsed and very well versed in infantry Close Quarter Battle tactics.[84]

The description of ISIL's tactical operations is intriguing with relation to the character of future war. When one talks about such attributes as highly organized, adaptable, mission command, proficiency in attacking positions with coordinated company and battalion-size formations, and relentless platoonand company level counterattacks to retake lost positions one automatically thinks of German infantry during World War II, not an insurgent group in Iraq.

ISIL'S USE OF PROPAGANDA

From its inception as AQI in 2004, the group had an extensive online presence and had made effective use of propaganda. Its main purpose was getting its message out to the world and recruiting new members. It also used the internet to pass on instructions and teaching materials to its distributed cells. To coordinate its increasingly sophisticated propaganda efforts, the group initially established the Al-Furqan Foundation for Media Production in November 2006.[85] This organization produced CDs, DVDs, posters, pamphlets, and a plethora of other web-based products including the group's official statements. By 2013, ISIL had created a second media wing, the Al-I'tisam Media Foundation, along with the Ajnad Foundation for Media Production, specializing in nasheeds (chants) along with other forms of audio content. In mid-2014, ISIL established the "Al-Hayat Media Center, which focused on targeting Western audiences producing material in English, German, Russian and French."[86]

A key forum of Al-Hayat messaging was its online English-language magazine titled *Dabiq*, which included "in-depth reports called 'Insight into the Islamic State' that detailed ISIL strategy and updates on its 'successes'."[87] In addition to these outlets, the group also ran a "radio network called Al-Bayan, which aired bulletins in Arabic, Russian and English covering its activities in Iraq, Syria and Libya."[88]

Despite significant attempts to counter its online presences and propaganda efforts, Western governments made little progress in defeating this sophisticated information war. As it had great success, it is likely to become a key component of armed non-state actors in future conflicts.

ISIL'S PERFORMANCE WITHIN THE STRATEGIC FRAMEWORK OF THE PEOPLE'S WAR DOCTRINE

Despite impressive results on the battlefield, ISIL was unable to attain the key objectives outlined within the *People's War* doctrine. For example, although they were able to establish bases, train and equip their forces, and generate stunning tactical and operational military successes, they failed in a number of critical areas. First, they were unable to arouse and organize the people to the extent they needed for any long-term success. In fact, they often alienated the people they needed most, the Sunnis, through the practice of Sharia law and harsh punishments and reprisals. Moreover, they tended to recruit fighters from outside the country rather than developing the capabilities from with the local population. As a result, they were unable to develop a close relationship with the people and use that relationship to properly structure their guerrilla force or their control over the population.

Secondly, they were never able to achieve the military objectives needed for their strategic success. Specifically, they were unable to destroy their enemy's (the Iraqi government's) national strength or its military forces. This failure prevented them from gaining their own national strength through that process.

Finally, ISIL was never able to achieve internal unification politically. To do this in Iraq and Syria the group would have needed to bring the Iraqi and Syrian Kurds and some part of the Shi'ite population/

tribes onto their side. However, the group's philosophy, organizational culture and policies of reprisal made this almost impossible. This shortcoming, combined with the fact that they were unable to make long term strategic alliances with any group that did not see the world the way they did, eventually resulted in their downfall.

Overall, the transformation of ISIL from a terror group into an insurgency force and ultimately a hybrid capability was impressive. Its plan to do so was well thought out and for the most part extremely well executed. During the group's initial stages of rebuilding in Syria it did not have the strength or desire to openly take on competitors, so it adopted a strategy of seeking out vulnerability and relying on intelligence, espionage, kidnapping and murder to open the way for its infiltration into the region. As it was doing this, the group also developed as a professional military force. This force was aided by an experienced cadre of former Saddam Hussein-era military officers, who also helped the group develop the blueprints for the future state, along with the strategic plans needed to achieve its goals.

In terms of tactical operations to support the insurgency, ISIL was able to use and combine different styles of warfare that included terrorism, guerilla warfare, and conventional military operations. They adapted their fighting style to the operational situation. Over time, ISIL was also able to generate an ability to conduct large scale military offensives. It did this systemically by starting off with small scale attacks and working up to larger operations.

Despite impressive results on the battlefield, the group was unable to attain its most important objectives. This failure was due to the fact that they were unable or unwilling to compromise on their belief system, which resulted in strategic miscalculations that prevented them from translating military successes on the battlefield to its larger operational and strategic goals. Specifically, the group failed to win the hearts and minds of the people. Moreover, they were never able to, or did not want to, make long-term strategic alliances with other groups that could have aided their success, such as the Kurds. This failure eventually resulted in their downfall.

In the end, ISIL's experience reinforces a clear message that Western governments would do well to adhere to, namely, strategic mistakes cannot be corrected by tactical or operational successes on the battlefield, regardless of how spectacular those successes may initially be. ISIL's failure was helped along by the international coalition that had formed to fight against it, however, its real failure was its own strategic blunders.

What does ISIL's experience tell us about Hybrid Warfare and conflict? Clearly the concept of the insurgency along with the idea of the insurgent group is still evolving. This form of warfare is no longer just being used to overthrow an established authority but is now being used by minority groups as a form of cultural/religious group security within a state or a collection of states.

Ongoing examples of this trend include the Kurds, Hamas and Hezbollah. This trend is likely to continue into the future, as more armed non-state actors see the benefits of this type of construct for self-defence or to achieve political goals. However, if peer and near-peer adversaries wish to harness the full potential of this capability, they will need a force to undertake the training, organization and oversee the development and employment of such a capability. And, this is where SOF excel.

To date, SOF have played key roles in a number of Hybrid Warfare operations carried out by peer and near-peer adversaries. Specifically, they have facilitated operations by armed non-state actors and have conducted a series of independent operations of their own. These operations have included the occupation and installation of a pro-Russian government in Crimea and the start of a resistance movement in Eastern Ukraine. In order to understand how SOF are employed in this role, it is instrumental to examine that operation in more detail.

CHAPTER 10

STATE USE OF SOF AND NON-STATE ACTORS: A PRACTICAL APPLICATION IN CRIMEA

From the outset, the outbreak of the "Maidan Revolution" in Ukraine was viewed by the Kremlin as a Western-backed plot to topple a legitimate government from power. Fearing that the demonstrations could spill over into Russia and that the installation of a pro-Western government in Ukraine would eventually bring NATO to Russia's doorstep in the south, the Russians concluded that they had little option but to act quickly.[1]

However, before they could effectively deal with the crisis, they had a number of problems they needed to resolve. They wanted to regain direct control over Crimea and they wished to have Ukraine back under their influence. However, in so doing they did not want a direct confrontation with NATO or the possibility of having to deal with yet another nationalist-inspired insurgency campaign should they decide to invade.[2] To that end, a Hybrid Warfare approach to the problem appeared to provide the best solution. The country was in the process of breaking up, so the trick was to allow it to continue imploding but to orchestrate the confusion towards a pro-Russian leaning.

As the situation started to come apart in Kiev, the Russians had already put the various elements it needed to secure the Crimea into place. As things got worse, the only visible sign of Russian preparations was the fact that they began to deploy significant military forces along the Russia/Ukraine border area. This of course immediately captured, and for the most part, held NATO's interest. When Ukrainian president Viktor Yanukovich fled the country in late February 2014, NATO braced for a Russian invasion and waited to see what the Kremlin would do next. Incredibly, Russian military forces simply remained on the border. Instead, news networks starting reporting that well-armed and equipped pro-Russia separatist rebels wearing green military uniforms and wearing no insignia began

taking control of key points within the Crimean Peninsula. Moreover, they began establishing checkpoints in and around cities and government locations including airports and military bases.[3]

What NATO, along with the rest of the world, did not know at the time was that these events were signalling the closing stages of the Russian operation in Crimea rather than its beginning. As it turned out, the first five phases of Russia's "New Generation Warfare" doctrine had already occurred, and the events that followed the establishment of the control points exposed both the true extent of Russian preparations along with the potential of this new form of Hybrid Warfare.

Shortly after the Peninsula had been secured, the Head of the Ukrainian Navy, Admiral Berezovsky, along with about half of the Ukrainian military forces stationed in the region, defected to the Russians.[4] This treachery was followed by the seizure of the Crimean parliament, which was immediately dissolved and a new pro-Russian Prime Minister installed.[5] The new parliament lost no time declaring the Republic of Crimea to be an independent, self-governing entity, and quickly announced it would hold a referendum on the status of Crimea recommending succession from the Ukraine to join the Russian Federation. In a majority vote, held on 16 March 2014, Crimea decided to become part of Russia and a treaty to that effect was signed with the Kremlin on 18 March 2014.[6]

While Crimea was getting ready for its referendum, demonstrations by anti-government groups were already taking place in the Donetsk and Luhansk regions of Eastern Ukraine. These demonstrations followed a similar format to the events in Crimea. So-called civilians holding Russian flags along with pro-Russian separatist rebels stormed buildings of regional state administrations and when successful in getting inside, raised Russian flags on top of the buildings.[7] Their demands were the same as those in the Crimea: a referendum to join the Russian Federation. News media outlets in the region captured the scene of hundreds and sometimes thousands of Ukrainian residents waving Russian flags wishing to reunite with Russia. Not surprisingly, some local reports pointed out that many of the key personalities and organizations associated with this separatist movement were either Russians or people with identifiable connections to Russia.[8]

The speed and efficiency of these operations had much to do with Russia's ability to infiltrate the Ukraine's political and economic institutions by the various Russian agencies. Dr. Mark Galeotti, who writes a blog titled *In Moscow's Shadows*, believes that "the GRU (military intelligence) supported by regular military units took the lead in Crimea, while the Federal Security Service (FSB), directed operations in eastern Ukraine." He states, "The FSB had likely penetrated much of the Ukrainian security apparatus prior to Yanukovich's fall, where it was able to monitor Kiev's plans and encourage at least some of the defections. Members of the Interior Ministry (MVD) used its contacts within the Ukrainian establishment to identify potential agents and other sources of information."[9]

As these activities were ongoing, the military was being used in a show of force role, providing a distraction along the border area while supporting the ongoing operations as needed. Moreover, Russian media and diplomatic sources kept up a constant campaign to characterize the new government as illegitimate and brutal, while in cyberspace 'patriotic hackers' attacked Ukrainian banks and government websites causing additional confusion and damage.[10]

In Crimea, the underlying premise of this form of warfare has been validated. This includes the idea of collapsing a state onto itself through social upheaval, even before a declaration of war is made, along with the focus of using such methods as political, economic, informational, humanitarian, and other non-military measures in coordination with the protest potential of the population. As Gerasimov also predicated, the Russians effectively used their Special Forces to link up with internal opposition groups throughout the target country, which created an operating front extending throughout the entire depth of the enemy's territory. These actions were effectively combined with information operations, cyber warfare, legal warfare, economic war and other activities that were specifically linked to a strategic outcome of the campaign and were modified as needed to achieve the specific results they wanted.

In fact, some believe it is the single most important lesson to come out of the Ukraine conflict. Kristin Ven Bruusgaard, a Research Fellow at the Norwegian Institute for Defense Studies (IFS) states:

> Experts have focused on the military novelties in the Russian approach—the use of asymmetric, covert, and otherwise innovative military tools. However, the real novelty in Crimea was not how Russia used its armed might (in terms of new military doctrine), but rather how it combined the use of military with state tools.[11]

The devastating effectiveness of this new combination can be seen when looking at the larger context of the conflict and its impact on security thinking within NATO in the aftermath of the operation. Imants Viesturs Liegis, the Latvian Ambassador to Hungary and a Former Defence Minister, put the Ukraine situation into context when he said:

> Russia is conducting several parallel wars at the same time. There has been a military intervention by stealth into Ukraine's Crimea and Eastern territory. An economic war is taking place following sanctions imposed on Russia by the EU, U.S. and other Western powers. An information war is being conducted by Russia on a massive and asymmetrical scale…The toxic results are there for all to see in Ukraine.[12]

In this regard, the Russian operations in 2014 appear to have taken significant steps towards creating the "battlefield of battlefields."

This construct will have a major impact on future wars, as the idea of combining conventional militaries with armed non-state actors will eventually reintroduce variations of compound warfare back onto the battlefield. As a result, Western militaries will need to start looking at how their force structures and planning can be adapted to accommodate these changes. Specifically, how will Western governments and their militaries evolve to meet these changing circumstances. More importantly, the question of what changes in policy and doctrine will be needed to be addressed to better understand, employ and counter these different types of formations and their methods in combat.

PART III

COUNTERING THE HYBRID WARFARE THREAT

CHAPTER 11

COUNTERING THE HYBRID WARFARE THREAT

Countries seeking to employ Hybrid Warfare are attempting to shift the emphasis of conflict from the operational level, focused on military campaigns, into the strategic realms of national defence/national security. Therefore, the critical first step in adjusting to this new reality is for Western nations to move back into the strategic realm of thinking while creating resiliency at the tactical level.

The strategic realm is defined as the art and science of developing and using the political, economic, informational and psychological powers of a nation, together with its armed forces, during peace and war, to secure national objectives.[1] To achieve the necessary proficiency to win this type of conflict, Western nations will need to open debate on how best to carry out strategy formulation and more importantly how best to apply it to achieve their strategic goals.

Although such changes at first glance appear to be relatively simple, they may be very difficult to bring about. This paradox is due to the fact that strategy formulation and implementation has not been a strong point for the West for some decades. A recent RAND Corporation study, *Improving Strategic Competence Lessons from 13 Years of War*, found that strategy is the missing link in current operations. Among others, shortfalls included a deficit in the understanding of strategy, shortfalls in the process for formulating strategy, and a failure to incorporate the essential political element of war into strategy.[2]

A key finding noted, "The U.S. government has experienced a persistent deficit in understanding and applying strategic art. The blurry line between policy and strategy requires both civilians and the military to engage in a dynamic, iterative dialogue to make successful strategy, but that often failed to occur."[3] The report added, "Americans [Western nations] are very competent at fighting, but they are much less

successful in fighting in such a way that they secure the strategic and, hence, political rewards they seek."[4] This point is significant, as the focus of different forms of Hybrid Warfare such as "New Generation Warfare" is to specifically seek and attain those political rewards as part of an overriding strategic goal.

Western nations will need to become more strategic in their thinking and application, if they wish to neutralize the effects of this form of warfare in the future. However, this is only part of the answer. The ability to think is of little value without the appropriate tools to do the job that must be done. These tools need to include the creation of a strategic coordination agency, along with the production of a new doctrine for war. Finally, Western nations must overcome the stigma of using various state tools as the primary means of dealing with conflicts.

CREATING A STRATEGIC COORDINATION AGENCY

To defeat state-level Hybrid Warfare, Western nations will need to compete with an enemy operating at a tactical level but fighting within the strategic realm. To accomplish this, a coordination agency that can effectively process information and coordinate the necessary state tools will be necessary. Initially, the role of such an agency would be to define the end-state of the Hybrid War against any nation prosecuting such a conflict, articulate the means available to achieve that end-state, and produce a coherent plan to set the concept in motion to counter the designated activities.

Once this has been accomplished, the coordination agency would need to organize the necessary activities to bring about the chosen end-state for the defender. Such an organization would need the capacity to create a model of the nation's "extended domain" so that it could produce and coordinate a national version of the "battlefield of battlefields."

To this end, the agency would need to be able to monitor the military, political, informational and economic situation worldwide. More importantly, it would need the analytical power to anticipate, recognize and analyze threats to its national entity (as well as its alliance partners), both ongoing and emerging. It would also need the authority for control over

its national military forces, along with any other national bodies and national organizations needed for the overall security of the state. This includes intelligence, national police forces, national emergency measures troops, diplomatic affairs, and cyber warfare capabilities, to name but a few.

In essence, the Strategic Coordination Agency becomes a country's Hybrid Warfare planning and operations centre. In the case of an alliance such as NATO, a similar organization that connects the national coordination centres to the alliance would also be required. As there is arguably no longer a distinction between war, competition and peace, this centre would need to operate continuously on a high-readiness posture. The capabilities within the agency would need to be networked into national-level strategic coordination centres with similar abilities and functions in order to be truly effective.

CREATING A HYBRID WARFARE DOCTRINE USING THE CONCEPT OF POLITICAL WARFARE AS THE FOUNDATION

As Strategic Coordination Agencies are put into place, Western countries will need to develop a doctrine for the conduct of this new type of warfare. This process may not be as difficult as it first appears. A Cold War application of this concept was first introduced by George Kennan in 1948 under the idea of "Political Warfare".

Kennan was an American diplomat and historian best known for developing the concept of "Containment," an idea to limit Soviet expansion during the Cold War. John Lewis Gaddis, a Cold War historian and author of *George F. Kennan: An American Life*, observed that the genius behind the thinking regarding containment was that "Kennan laid out a third path between the extremes of war and appeasement." Kennan believed, "if the US and its allies could be patient and …develop a coherent strategy of non-provocative resistance, this third path would lead to a settlement … or even to the break-up of the Soviet Union."[5]

In a Policy Planning Memorandum, dated 4 May 1948, Kennan argued, "Political warfare was the means to achieve Western objectives and was in fact, the logical application of Clausewitz's doctrine in time of

peace." He asserted, "in [its] broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives." He added, "Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP [the Marshall Plan]), and 'white' propaganda to such covert operations as clandestine support of "friendly" foreign elements, 'black' psychological warfare and even the encouragement of underground resistance in hostile states."[6]

Kennan provided three broad areas of focus for Political Warfare's activities, Liberation Committees, Support of Indigenous Anti-Communist Elements in threatened countries of the Free World, and Preventive Direct Action in Free Countries. In 2014, the United States Army Special Operations Command (USASOC) updated these ideas to include a more detailed listing. These include:

- Economic sanctions against countries, groups, and individuals, as well as coercive trade policies;
- Diplomacy, including boycotting international events, establishing treaties or alliances to counter adversary UW, severing diplomatic relations, or excluding offending states from membership in international forums;
- Support for "friendly" insurgent groups to coerce, disrupt, or overthrow an adversary regime;
- Support for friendly governments to counter adversary political warfare activities;
- Support for foreign political actors and parties opposing adversarial regimes; and
- Strategic communications and information operations to expose adversary activities.[7]

The strategy of containment became the central pillar in the post-war concept for dealing with the Soviet Union. Although it had its detractors, it kept the Cold War in check for 41 years and did achieve Kennan's ultimate vision of ending with the break-up of the Soviet Union.

While Kennan was not interested in managing the transition from peace to war in broad terms, the other components of political warfare, particularly within the context of USASOC updated listing, are still relevant to developing an effective counter to Hybrid Warfare. These include finding the enemy's weaknesses, developing a long-term strategy to attack those weaknesses, and identifying and coordinating the necessary state tools to do the job effectively.

Interestingly, USASOC has already started to move in this direction. In their *SOF Support to Political Warfare White Paper,* they lay out the requirement for a suite of complementary options to counter Hybrid Warfare carried out by state and non-state adversaries. They feel that any effective response will need to "comprehensively mitigate the effect of subversion, UW [Unconventional Warfare], and delegitimizing narratives in partner countries targeted by adversaries. They also feel that it is important to dissuade adversaries from conducting Hybrid Warfare by increasing the cost of such activities to the point that they become unsustainable."[8]

To do this USASOC believes it can overmatch its adversaries. However, they understand that this can only be done through a whole-of-government approach that is expressed through an integrated strategy and a cohesive set of policy options that uses both overt and covert tools.[9]

SPECIAL OPERATIONS FORCES THE KEY MILITARY PLAYER IN THE FUTURE OF TACTICAL HYBRID WARFARE

The central idea behind the evolving character of state-level Hybrid Warfare is to de-emphasize the use of conventional military forces and if possible, eliminate their use altogether. Unfortunately, this will not always occur. During the Cold War, even though NATO and the Warsaw Pact never went to war in Central Europe, the strategy of containment, using Political Warfare as its means, produced a number of proxy wars between various Communist nations and the Americans including Korea, Vietnam, and Afghanistan to name a few.[10] In fact, central to the initial phases of Hybrid Warfare is the use of security services, intelligence and Special Operations Forces (SOF) operating in a covert manner or

with local forces in the form of irregular warfare. Therefore, even though the aim of Hybrid War is to reduce military conflict, it is reasonable to assume that military operations will be needed with the idea that they would be limited to as small a force as possible.

The most suitable and likely military intervention in the early stages of any future Hybrid War will likely be SOF and counter-SOF capabilities. This is due to the fact that such capabilities are the most capable physical component for transitioning between the strategic, operational and tactical levels of conflict and war. The major question that needs to be addressed is, do these forces fit into the realm of Political Warfare in such a way as to allow them to contain the situation or effectively destroy an enemy's capacity to carry out specific aspects of a Hybrid Warfare campaign? One possibility could be the use of an innovated concept being referred to as Special Warfare.

In a research paper, "Special Warfare: The Missing Middle in U.S. Coercive Options," published by the RAND Corporation in 2015, the authors argue that Special Warfare fills the missing middle for exerting influence between the costly commitment of conventional forces and precision-strike options provided by drones, aircraft, missiles, and SOF direct action. The idea is that Special Warfare campaigns are designed to "stabilize or destabilize a regime by operating "through and with" local state or non-state partners, rather than through straight unilateral action.

The authors have identified a number of campaigns that could support a Hybrid War capability. These include hybrid guerrilla warfare in the defence, support to conventional power projection, support to distant blockade, covert foreign internal defence for eliminating weapons of mass destruction, counter proliferation against a global network, foreign internal defence in a fractured state, building a regional security exporter, and counter genocide unconventional warfare. Most of these missions are directly applicable to three of USASOC's Political Warfare activities. As such they may provide a good foundation for deploying SOF on such operations.[11] The research paper adds that these Special Warfare campaigns have six central features:

- Their goal is stabilizing or destabilizing the targeted regime;
- Local partners provide the main effort;
- Military forces maintain a small (or no) footprint in the country;
- They are typically of long duration and may require extensive preparatory work better measured in months (or years) than days;
- They require intensive interagency cooperation; and
- They employ "political warfare" methods to mobilize, neutralize, or integrate individuals or groups from the tactical to strategic levels.[12]

Like the USASOC white paper, the RAND document emphasizes the need for strategic thinking and coordination. However, it cautions, "accepting this broader definition of war would then require a theory of victory to adequately account for that dimension." Moreover, political outcomes would be embraced as a principle and articulated specifically in each case.[13]

OVERCOMING THE STIGMA AND INSTITUTIONAL RESISTANCE OF USING HYBRID WARFARE

Although, there is sufficient evidence to support the need to adapt Hybrid Warfare doctrine as part of the West's security strategy, the idea will face a number of difficult obstacles. For example, despite the publicity and analysis surrounding the initial launch of the *Unrestricted Warfare* publication, there is little evidence that the Chinese People's Liberation Army (PLA) has adopted any of its core concepts. In 2003, the Chinese Communist Party (CCP) Central Committee and the Central Military Commission (CMC) did endorse the "three warfares" concept based on the need to integrate Psychological Warfare, Media Warfare, and Legal Warfare into its doctrine.[14] However, according to the Department of Defense's, *Military and Security Developments Involving the People's Republic of China for 2011, "*The Chinese concept of "three warfares" … reflects China's desire to effectively exploit these force enablers in the run-up to, and during, hostilities."

The term "force enablers" suggests little more than a supporting role for these capabilities within the context of conventional military operations. Something Qiao Liang and Wang Xiangsui specifically warned against. In fact, the evidence suggests that the PLA is very much on the road to developing a capability and doctrine to conduct a head-on conventional war against a high-technology conventional opponent. According to another Department of Defense review "China is investing in military programs and weapons designed to improve extended-range power projection and operations in emerging domains such as cyberspace, space, and electronic warfare." The report adds, "current trends in China's weapons production will enable the PLA to conduct a range of military operations in Asia well beyond China's traditional territorial claims."[15] This would clearly suggest that the PLA's views on future warfare appear to be very similar to Western ideas of integrating selected national capabilities to support operational level activities, rather than creating a specific hybrid doctrine or warfare components to support strategic operations.

Why have the Chinese adopted a more conventional approach to military modernization? As Dr. Andrew Scobell, Senior Political Scientist at RAND in Washington, D.C., points out, "it is likely that China's political leaders would find many of the concepts discussed in *Unrestricted Warfare* appealing as it would offer an alternative defense policy where strategic (government) control would be far greater and likely for far less money. However, the military establishment of the PLA would likely view such a reorientation as a threat to the defense budgets, manpower, bureaucratic clout, and a decline in prestige."[16]

Notwithstanding, this institutional resistance, the idea of state-level Hybrid Warfare is still very much viewed as the poor man's weapon and although effective in defending a weaker opponent, it is unable to provide the necessary power projection capabilities needed to become a real player on the international stage. In this respect, the Russians may have found the right balance; they have integrated Hybrid Warfare into their conventional warfighting doctrine, which demonstrates a transition from Hybrid War to conventional operations as required. But they still have a significant conventional military capability they can call upon. That being said, its success in places such as Crimea, Ukraine, Syria, South China Sea and Norway may start to change some perceptions.

TOWARDS A FUTURE OPERATING CONCEPT FOR DEALING WITH ARMED NON-STATE ACTORS

Undeniably, armed non-state actors will play a key role in state-directed Hybrid Warfare efforts. Moreover, these actors are also beginning to introduce different forms of warfare onto the battlefield. As a result, conventional military operations, irregular warfare, Hybrid War, acts of terrorism and criminal activities are now occurring simultaneously on the contemporary battlefield. To counter these new threats, Western military forces will need to become more flexible and adaptive. But how? One possibility is to integrate SOF into an Army's employment concept using UW to train, coordinate and direct the operations of irregular and hybrid forces.

Such a concept would formally bring these individual capabilities into the Western military's operating doctrine. Properly done, it would give Western nations a more holistic force structure with a flexible doctrine of battlefield saturation. It would also provide armies with the ability to transition between hybrid, conventional and counterinsurgency (COIN) operations simply by emphasizing different aspects of that doctrine and/or the forces available.

Historically, the idea of bringing a variety of forces together, or pairing conventional and irregular forces onto the same battlefield is nothing new. Such tactics have been used extensively throughout Western history with great success and are now being employed or being considered by a number of different militaries and armed non-state actors in the form of hybrid or compound warfare at the tactical level. In order to better understand what roles Western forces can play within this context, it is important to first comprehend the trends impacting the modern battlefield.

Frank Hoffman's ideas regarding the simultaneous use of multiple forms of warfare, the employment of state-level Hybrid War, and the emergence of the irregular element as a decisive, or at least an equal partner, in open conflict is slowly impacting conventional military thinking. Along with this concept is the idea that operations are becoming more distributed as the modern battlefield expands and fighting becomes more dispersed,

diverse and complex.[17] This process is forcing conventional military forces into various forms of distributed operations.

DISTRIBUTED OPERATIONS WAR-FIGHTING CONCEPT

As already noted, the modern Western concept of dispersion in war-fighting was researched and developed by the United States Marine Corps and initially published as a war-fighting concept, *Distributed Operations* (DO), in April 2005. This document was subsequently refined and adopted in various forms by other Western nations. The concept was specifically designed to deal with adaptive enemies operating in a complex environment by providing conventional forces with the ability to decentralize both decision-making and force distribution as necessary.

In order to maintain the ability to destroy the enemy or support other operations, distributed units need the capability to rapidly re-aggregate.[18] This ability to distribute and aggregate is necessary to provide commanders with the capability to operate using the fuller range of tactical employment methods that were complementary in character. For example, the initial concept envisioned sea-based forces projecting power using ship-to objective manoeuvre in an aggregated fashion, while being complemented by additional units that would continue using distributed operations.[19]

FINDING THE RIGHT EMPLOYMENT CONCEPT

Understanding this problem is one thing, finding a way to actually integrate and manage the various capabilities on the battlefield is another. Part of the answer lies not so much in attempting to find new capabilities as it does in finding new ways to bring current capabilities, such as well established heavy, medium, and light ground forces, together with SOF/irregular forces onto the battlefield within an integrated and flexible doctrine. In this case, the challenge is in finding the right tactics to effectively employ SOF/irregular forces by allowing them to be coupled to conventional units, while allowing the two groups to break apart when necessary. One option could be the integration of SOF/irregular and light forces into the part of the construct for disperse operations, while

maintaining medium and heavy forces to do the aggregate work, within a distributed construct.

In this case, SOF could be integrated into the employment of this concept using UW. This allows the further integration and employment of irregular forces into the larger operating doctrine. This construct, properly done, creates a holistic force structure operating from a common and flexible doctrine of battlefield saturation.

Such a doctrine and force structure would also give Western armies incredible flexibility to deal with the complexities of future conflict by allowing them to have the ability to quickly transition between hybrid, conventional and COIN operations simply be emphasizing different aspects of the doctrine and forces that are available.

Interestingly, the idea of bringing these different types of forces together is nothing new. It has been used extensively throughout history and with great success. Moreover, the idea of pairing conventional and irregular forces onto the same battlefield is also nothing unique and has sometimes been referred to as compound warfare.[20]

DEVELOPING COMPOUND WARFARE TO BETTER MEET WESTERN NEEDS

From a Western perspective, compound warfare has been defined as the simultaneous use of conventional and irregular forces against an enemy.[21] According to Thomas M. Huber, editor of *Compound Warfare: That Fatal Knot*, operations of the regular and the irregular forces are extremely complementary. He explains that the irregular forces can give important advantages to the regular force, such as developing superior intelligence information while suppressing enemy intelligence. They can also provide supplies and quick passage through territory that they occupy, while denying these to an enemy.[22]

Huber also believes that regular forces can give important advantages to irregulars. For example, they can pressure the enemy to withdraw, forcing them into or out of areas where irregulars are operating thus creating the conditions for greater freedom of action. "The main force can provide

strategic information, advising the guerrillas of when and where to act to accommodate the overall effort."[23]

From a historical perspective, Huber's thesis appears to have merit as there are numerous examples of armies employing various forms of compound warfare. The more famous cases include Wellington's use of irregulars in Spain (1808 and 1814), Mao Zedong in China's revolutionary wars (1927 to 1949), and Ho Chi-Minh in Vietnam's wars of Independence (1945-1975).[24] In fact, compound warfare was an integral part of the early Canadian "way of war" as both the English and French used conventional and militia units in North America that integrated irregular forces, such as native allies during much of the eighteenth and early nineteenth centuries.[25]

Interestingly, French Canadian militiamen adapted these tactics to the conditions of fighting in the North American wilderness faster and better than their English counterparts, and for this reason they usually had a tactical advantage. Eventually, the British discovered that they could overcome this very effective form of warfare by adopting similar tactics.[26] Michael Pearlman, associate professor of history at the United States Army Command and General Staff College explains, "The British did more than slavishly copy the French. They domesticated irregular operations… [this was done] by substituting rangers for Indian auxiliaries, and then more reliable light infantry regulars for American rangers."[27] Ironically, once the British had developed a capacity for irregular warfare, they used it to great effect on their enemies, and even exported the idea to the Spanish theatre of war where they ravaged a far superior French force. The number of irregulars operating with Wellington's forces during the Spanish campaign provides some insight into effectiveness of compound warfare. Huber states that "France had 320,000 troops in Spain at the height of its presence in 1810 and…during their six-year campaign, French forces lost 240,000 men. Of these, 45,000 were killed in action against conventional forces, 50,000 died of illness and accident, and 145,000 were killed in action against guerrilla forces." By comparison, he estimates that "Wellington's army in Spain at its height had only about 40,000 troops, with some 25,000 Portuguese forces attached."[28] Incredibly, despite enjoying a conventional force advantage

of four to one the French were unable to achieve any type of measurable success let alone victory during the six-year campaign.[29]

The synergy derived by combining regular and irregular operations at both the tactical and operational levels makes compound warfare especially effective for operations by smaller forces over large areas and in difficult terrain. If properly developed, such operations would significantly enhance the flexibility and combat effectiveness of any Western nation's future doctrine.[30] However, for such a concept to be integrated into that doctrine, a capability would be needed that could organize, train, and employ irregular forces and conventional light forces within the framework of a nation's campaign plan and this is where SOF comes in.

As SOF are likely to play the central role in the initial phases of any future conflict, their operations would also set the battlefield framework for any escalation and subsequent move to conventional force operations. The key capability SOF would need to bring to the table for this modern version of compound/Hybrid Warfare to be effective is Unconventional Warfare.[31]

UNCONVENTIONAL WARFARE AND THE MERGING OF DIFFERENT FORCES

In its most basic terms, UW can be defined as the ability to organize, train, equip, advise, and assist indigenous and surrogate forces in military and paramilitary operations. According to the American *Joint Special Operations Joint Publication 3-0517,* Unconventional Warfare are operations "that involve a broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces that are organized, trained, equipped, supported, and directed in varying degrees by an external source."[32] The publication explains that "UW is unique in that it is a SO [special operation] that can either be conducted as part of a geographic combatant commander's overall theater campaign, or as an independent, subordinate campaign. When conducted independently, the primary focus of UW is on political-military objectives and psychological objectives."[33]

Incredibly, UW has not been well received or understood by conventional military commanders, which may be the reason it originated outside of the armed forces establishment. Despite this lack of interest on the part of the military, the American and British Governments devoted significant effort to such activities during the Second World War, as both the British Special Operations Executive (SOE) and American Office of Strategic Services (OSS) were set up to coordinate various UW activities in occupied countries in Europe and Asia. These activities included the insertion of teams to support and coordinate existing resistance movements.[34] One such organization was based on a three-man liaison team, commonly referred to as a Jedburgh team. These teams consisted of a British or American officer, a French officer, and a radio operator, who would be deployed into areas known to have active resistance movements with sufficient arms to supply about one hundred men.[35] In addition to the Jedburgh teams, the OSS developed and successfully employed the idea of operational groups (OGs).

OGs were unique as they were deployed on missions that required a wider range of capabilities than could be provided by the three-man Jedburgh teams. As a rule, an OG had between fifteen and thirty men and included two specialists, a medical technician, and a radio operator.[36] These groups were organized and trained to work independently or in cooperation with either the Jedburghs or partisans. They also undertook a variety of activities that ranged from ambushing enemy columns, cutting lines of communications, blowing up railroad lines and bridges, and providing supplies to various resistance groups. According to Patrick K. O'Donnell, an expert on Second World War espionage and special operations, "The typical OG team was described as a small self–sufficient band of men who might be required to live and fight in the manner of guerrillas."[37]

During the war, the success of the OSS validated the concept of UW and provided SOF with a unique mission. The idea was refined in post-war analysis as members of the OGs indicated that their extensive training was effective but felt that some adjustments needed to be made. Specifically, greater emphasis was required on such things as the operation and maintenance of foreign weapons and vehicles, methods of instruction, French military nomenclature, and on radio maintenance and repair.[38] Members of the groups realized that any type of team functioning

behind enemy lines for extended periods needed highly developed skills in critical areas, such as communications, medical procedures, weapons knowledge, and vehicle and equipment maintenance and repair.[39]

UNDERSTANDING WESTERN EMPLOYMENT OF THE UNCONVENTIONAL WARFARE CAPABILITY POST WWII

At the end of the Second World War, the OSS was disbanded and most of its operational intelligence activities were handed over to the newly created Central Intelligence Agency (CIA). Initially, the United States Army did not see a need to develop an UW capability; however, a growing Soviet threat resulted in the activation, albeit reluctantly, of the 10th Special Forces Group (Green Berets) in 1952. From the beginning, the group's main mission was to conduct guerrilla warfare behind any Soviet advance in the event of a Russian invasion of Western Europe.[40] The organization of the 1952 Special Forces (SF) operational detachment (OD) was very similar to the OGs that had deployed to France, with the addition of many of the post-war recommendations.[41]

ODs were authorized a strength of 15 men, which included a "detachment commander, an executive officer and 13 enlisted men. In theory, these teams could organize, support and direct a regimental-sized guerrilla unit. The functional specialties used to carry out this mission included medical, demolitions, communications, weapons, [and] operations and intelligence."[42] During the Vietnam War (1959-1975), the Americans had the opportunity to again prove and refine this concept as the Green Berets were tasked to employ indigenous troops using many of the same small-war methods the enemy was using.[43] For much of the war "the 5th Special Forces Group trained and led Civilian Irregular Defense Groups (CIDGs), which included Mobile Strike Forces ("Mike Forces") and reconnaissance companies that were manned by ethnic minority tribes from the mountain and border regions."[44] These forces carried out reconnaissance along the border regions and provided security for their home bases. The idea of having CIDG forces was to broaden the COIN effort; by asserting security over much of the tribal-minority-populated areas of the highlands and remote districts of the Mekong Delta to provide a buffer against Viet Cong infiltration.[45]

Controlling the region allowed the Americans to set up a system of "indigenous trail watchers, whose mission was to locate and report Viet Cong movements near the border. The trail watcher program was significant in that it was the precursor to the border surveillance program, where area development and border surveillance combined to create one of the more valuable components of the CIDG program."[46] Over time, these forces developed an offensive capability and by 1964 they were carrying out operations against Viet Cong safe havens and interdicting infiltration routes into Vietnam. By 1965, these operations had developed into more aggressive search and destroy missions using larger forces.[47] Other CIDG-type forces included mobile guerrilla teams, which raided enemy base areas using hit-and-run tactics against regular enemy units.

To put these operations into perspective, 2,500 Special Forces soldiers raised, trained, and led an army of 50,000 tribal fighters that carried out operations in some of the most difficult areas in Vietnam. This force patrolled the border areas, provided intelligence, and developed a security force in areas that otherwise may have been controlled by the enemy.[48]

The adaptability and employment of the UW capability has remained valid in the contemporary operating environment. In fact, in the aftermath of 9/11, SOF have played increasingly important roles in military operations throughout the world. As in the case of Afghanistan, they proved they could quickly adapt to changing circumstances. Despite having as few as 300 soldiers on the ground, SOF teams were able to successfully rally unorganized and rival anti-Taliban-opposition groups within the country to form a Northern Alliance that defeated Taliban forces. These well-planned operations included very intense and precise bombing campaigns that used state of the art equipment coordinated by SOF soldiers. However, what is even more astonishing than the effectiveness of these operations was the speed at which they were accomplished. Only 49 days were needed from the time they became directly involved with operations on the ground to the fall of Kandahar.[49]

EMBRACING THE UNCONVENTIONAL WARFARE CAPABILITY

UW has proven to be a versatile operational capability, however, in order to be a successful, part of the force structure would have to be devoted to

working within the irregular construct of compound warfare. This means that, at the operational level, UW activities would be focused on establishing and/or maintaining the overall framework for dispersed operations around which conventional forces could manoeuvre. This would allow OD forces employing UW to provide tactical support to conventional forces operating in theatre on an ongoing basis.

Such a change would significantly alter the current relationship that has historically existed between SOF, irregular and conventional units. Once these issues have been worked out, the possible combinations of UW and conventional forces could be as numerous as the situations they would be expected to encounter. Moreover, it is this flexibility that is at the heart of compound warfare's true strength, and it is this flexibility that will allow Western nations the ability to deal with increasingly larger threats in the future security environment.

Another issue that would have to be addressed when considering the development of an UW capability for ODs is the need to closely align SOF operations with the Western nation's conventional forces doctrine. To achieve the necessary coordination, SOF would have to become an integral component within their operations and this new emphasis would require a major cultural shift for many militaries and their SOF. In developing such a capability, Western nations could better tailor their operational needs to meet the specific requirements of ODs and Hybrid War rather than trying to make employment compromises that could reduce ODs' full potential.

THE FINNISH ARMY'S INTERPRETATION OF COMPOUND/ HYBRID WARFARE CONCEPT

Many of these ideas have already, to some extent, been incorporated into the Finnish military's modern force structure and doctrine.[50] The country's defence doctrine is to hold vital ground and key points with regional forces while destroying attacking forces using a combination of irregular and conventional mobile forces. This is done within the context of a deep territorial defence based on a force employment concept similar to that of compound warfare.

As mentioned earlier, the synergy derived by combining regular (light, medium, and heavy) and irregular operations at both the tactical and operational levels makes this type of warfare especially effective for operations by smaller forces. As with the Finnish Army's experience in the Winter War in 1939-1940, when properly employed, such operations can significantly enhance the flexibility and combat effectiveness of an army.

Finnish forces achieve this level of fighting efficiency by breaking down their force structure into general forces, local forces, and support forces. General forces are based on brigades and are the best equipped units within the Army. As such, they are the elements most suited for decisive massed attacks at key points along the battle front.[51]

The Finns use local forces to supplement this conventional military capability. These units consist of a professional cadre, older reservists, and newly raised conscripts. Their primary function is to carry out guerrilla operations in areas that have been overrun by the enemy. When necessary, these local forces are combined with general forces for conventional attacks against a weakened or encircled enemy. Support forces assisted the other two forces with logistics, supplies, and other requirements.[52]

In peacetime, the Finn's standing forces are concentrated in areas where they can be deployed to provide the greatest flexibility at hitting back at potential threats in the most likely areas of attack. Any attacking force would have to go through a "deep zone" defence that would take advantage of both geographical features and climatic conditions. Tactics of delay and attrition would be employed to the extent possible to prevent an attacking force from reaching vital areas.[53]

As the attacker's lines of communication lengthen, concentrated counterattacks would be launched under conditions favouring the more lightly armed Finnish units. In areas seized by an invading army, local forces would continue to conduct guerrilla-type operations, such as ambushes, limited raids on the enemy's supply lines, mining of roads, and carrying out strikes against logistics centres.[54]

These local defence forces would also be expected to operate as self-contained units in relative isolation. The object of such operations is to

sap the strength of an attacker as they moved deeper into the country, denying them the use of roads and facilities to slow down progress. After enemy combat units have been cut off from supplies and reinforcements, segmenting the fighting, it is expected that local and general forces would be concentrated to deliver strikes against the enemy before dispersing into the wilderness to repeat the process.[55] After suffering costly damage over a protracted period, the Finns hope that the attackers would find it more expedient to abandon their original objectives and accept some type of negotiated settlement.[56]

Within the context of modern conflict, the idea of using local defence forces as self-contained units supporting larger manoeuvre elements to sap the enemy's strength and deny them freedom of movement goes back to the British 1808-1814 Peninsular War. However, it is now being modified and refined by the United States Marine Corps to support future American maritime operations.

THE UNITED STATES MARINE CORPS' MOVE TOWARDS COMPOUND/HYBRID WARFARE CONCEPT

Introduced in March 2020, Force Design, is the Marine Corps' effort to reshape its fighting capabilities to better meet the demands of future conflicts and support naval operations.[57] The main focus of this concept is to counter an enemy's area denial and access strategy, within the context of littoral settings. Central to its vision is the ability of small but well-equipped forces to operate within an enemy's protective zone of air, missile, and naval power. Something the Marines refer to as the weapons engagement zone (WEZ). To accomplish this, the Marines will provide the Navy with "stand-in forces" (SIF). These forces are specifically designed and trained to operate as irregular forces within the WEZ.[58]

SIF's main mission is to support the U.S. Navy's fleet operations by disrupting enemy forces. This will be done by fighting within a contested area as the forward edge of a maritime defense-in-depth strategy. Their primary function will be to help the fleet win the reconnaissance/strike and counter reconnaissance/strike battles before and during the initial stages of a conflict. To do this they will attempt to identify and monitor potential adversary's sensor systems. Should armed conflict

erupt, SIF will be expected to carry out a host of additional missions including:

- conduct sea denial operations in support of fleet operations, especially near maritime chokepoints;
- sea denial through the use of organic sensors and weapon systems to complete kill webs, but also by integrating organic capabilities with naval and joint all-domain capabilities; and
- In support of sea denial operations, SIF will be expected to gain positional advantage in the area by seizing, and controlling key maritime terrain.

The idea is that SIF forces will become so much of an operational problem for an enemy that the problem must be addressed if the enemy is to achieve their war aims. However, this outcome can only be achieved if units have operationally relevant capabilities that cannot be ignored.[59]

The basic idea is to turn large bodies of water into anti-ship missile engagement zones, with layers of various anti-ship missile defenses ranging out to hundreds and even thousands of miles from shorelines. As Tyler Rogoway, points out in his article, "HSV-2 Swift Destroyed Off Yemeni Coast by Anti-Ship Missile: A horrific reminder of how anti-ship missiles are falling into the hands of non-state," he explains, "Even relatively dated anti-ship missiles, or, in more rare circumstances, anti-tank missiles, are especially dangerous to vessels operating close to shore in the so-called littoral combat environment." He adds, "In such an environment, these weapons can emerge from seemingly nowhere and impact in a matter of seconds, giving a crew little time to react. This is a reality that even the world's most advanced surface combatant will have to come to terms with."[60]

In order to work, the concept will require major structural changes within the Corps. For example, it will need to become a more amphibious and somewhat irregular light striking force if it wants to dominate the littoral setting in key areas. To do this the Marine Corps is looking to create a new baseline "formation called the littoral regiment." These regiments will consist of infantry, rocket artillery, logistics, and an anti-

air battery, all of which will be highly mobile and have a long-range precision strike capability.[61]

Littoral regiments will also be equipped with a variety of missiles and drones and will be able to form smaller highly mobile teams able to moved quickly from island to island using various types of amphibious vessels, to assist the Navy with attacking enemy ships and keeping sea lanes open.[62]

This added agility and firepower will come at a cost. Structural changes to make this happen will need to include the shedding of all tanks and the replacement of most cannon artillery with rocket artillery. It will also see the number of UAV squadrons, missile artillery batteries, and C-130 transport squadrons increasing, while removing almost all cannon artillery batteries, and all tank and bridging companies. Moreover, the numbers of other units, "including infantry battalions, tilt-rotor aircraft squadrons, and helicopter squadrons, are being slightly reduced."[63] A key element of the new concept will be reintroduction of the "distributed operations" concept.

As already noted, distributed operations were developed by the Marines to deal with adaptive enemies operating within a more complex battlefield environment. Their primary purpose was to provide conventional forces the ability to decentralize their capabilities, including both decision-making and force distribution as necessary. More importantly, distributed operations were intended to provide commanders with the ability to employ tactical units across the entire depth and breadth of the non-linear battlespace.[64]

As the Marine concept paper at the time explained, "Distributed Operations describes an operating approach that will create an advantage over an adversary through the deliberate use of separation and coordinated, interdependent, tactical actions enabled by increased access to functional support, as well as by enhanced combat capabilities at the small-unit level." It goes on to state, "The essence of this concept lies in the capacity for coordinated action by dispersed units, throughout the breadth and depth of the battlespace, ordered and connected within an operational design focused on a common aim."[65]

This approach allows forces to reduce their vulnerability to enemy observation and fire. However, forces still need to possess significant combat power to close with, and destroy the enemy as necessary.[66] Within Force Design, it appears that the Marines are attempting to address this issue, as a major departure from the initial concept recognizes that future SIF units will require significantly more organic combat power, not just the capacity to call on supporting fires.[67]

The Marine Corps has taken a number of lessons from history to justify further research. For example, they point out that to "strategically defend the Sinai coast, Israeli Red Sea Naval Forces conducted a tactical offensive using a variety of aggressive small unit actions to confuse the Egyptians and keep them close to their bases, focused on defending themselves." Their studies point out that, "Through a combination of navy commando raids, hit and run attacks, complemented by an understanding of how to evade and defeat Egyptian sensors, the Israelis were able to destroy Egyptian missile boats and much of their transport fleet." They conclude, "the Israelis were able to do all of this even though their army and air force were fully engaged in other parts of the theater of operations."[68]

When facing a near-peer threat such as China, the Marine Corps' Force 2030 will see small Marine forces deployed around the islands of the first island chain and within the South China Sea. Each element will have the ability to contest the surrounding air and naval space using medium and long-range anti-air and antiship missiles. Collectively, it is hoped that these units will attrite Chinese forces, inhibit them from moving outward, and ultimately, as part of a joint campaign, squeeze them back to the Chinese homeland.[69]

In the end, analysis and experimentation are showing the Americans that SIF can generate technically disruptive, tactical stand-in engagements that can confront enemy naval forces with an array of low signature, affordable, and risk-worthy platforms and payloads.[70] In this respect, we are seeing a reintroduction of old but proven concepts that validate the idea that not all forces need to be going into battle as conventional capabilities within the Western context.

CONCLUSION

Peer and near-peer adversaries are seeking to move the center of gravity for conflict from the operational level, where conventional military forces play a predominant role, into the strategic realm, where the integration of strategic planning and the coordination of state tools becomes the critical denominator. This is achieved by converging different methods, battlefields, and force structures into a holistic doctrine that blurs various capabilities into a single force operating within a battlespace dominated by information management.

This concept comes from the Chinese idea of creating the "extended domain," which is done by integrating information from national interests and national security requirements onto the larger strategic situation map. Once this has been completed, one can produce the "battlefield of battlefields," which, if coordinated correctly, will be a major step towards reducing the impact of a potential enemy's overwhelming advantage in conventional military operations.

The Russians have proven that they are well on their way to developing this concept in the form of "New Generation Warfare." Based on the theory of Unlimited Warfare, they will only become more effective over time as experience creates sophistication of both process and reaction. As a result, Western countries must seek to better understand this form of warfare in order to effectively counter its devastating results.

To counter these types of operations Western countries will need to have the appropriate concepts, tools and organizations in place so that they can plan, act and coordinate the strategic capabilities within the nation. In the future, Western countries will still be required to fight and win conventional wars; however, they must also be able to fight on the "battlefield of battlefields" that globalization, technology and the evolution of the future security environment are now creating. In order to win the various conflicts, whether through the media battle, the cyber battle, the political battle, or on the irregular/conventional military battle, the West must make the following changes to their current practices:

- The first and most important is to move from operational to strategic level thinking;
- Create a Strategic Coordination Agency;
- Create a Hybrid Warfare capability using the concept of Political Warfare;
- Bring Special Operations Forces to the forefront of Hybrid Warfare by integrating Political Warfare with Special Warfare; and
- Lose the stigma of fighting Hybrid War.

In order to bring all of these things together, Western nations will need to have a unifying doctrine for conflict from the tactical to national strategic level. They will have to deal with the problems associated with the idea of the "Whole of Government" approach, which is more show on a PowerPoint presentation than a work in progress. Finally, it will have to plan for and develop resiliency within the elements of national power. The one issue that events in the Ukraine, Syria and the South China Sea have shown the West is that, should peer nations wish to take on a Western country, they will do so by avoiding the West's military and high technology strengths. The West must be ready to counter this approach.

More importantly, current trends in the international security environment suggest a continued use, by both regional and major powers, of non-state actors as proxies. In practice, this is currently being done by supplementing such forces with small SOF or other specialists, which can access Intelligence, Surveillance, Reconnaissance (ISR)/strike capabilities along with other types of selected conventional military support. This additional support is usually in the form of training, logistics and advance equipment. Recent examples of this approach have been seen with the Russian use of such forces in the Crimea, Ukraine and Syria, as well as with the American/Coalition's use of similar forces in both Iraq and Syria. More recently, Iran has also begun employing such forces against various governments within the Middle East. Given the increasing capabilities of these forces, it is likely their importance and influence will only continue growing on both the irregular and conventional battlefields of the future.

As the emphasis of major conflict between peer nations slowly shifts to a focus on targeting social stability rather than the destruction of military capabilities, it is likely this type of conflict will continue to evolve with both state and armed non-state actors employing different aspects of Hybrid Warfare depending on the specific situation they face. Moreover, armed non-state actors will likely serve as the future building blocks for a more modular and flexible state military doctrine that can allow such forces to be integrated into SOF or conventional units to better meet specific national policies and battlefield circumstances.

In order to counter armed non-state actors using Mao's doctrine, it is important to understand that they are as much a political force as they are a military threat. As such, their focus is at the strategic and tactical levels of conflict. This construct allows them to circumvent the established authority's strength in military capability at the operational level. When armed non-state actors get to the point where they are openly displaying capabilities that challenge the operational level of war, or are being provided with that capability by an outside nation state, it is a sign that they are in a position of strength relative to the established authority. Defeating such groups militarily does little except to force them back into a posture of guerrilla warfare, as is the case currently with the remnants of ISIL, so they must also be defeated politically as well to achieve decisive results.

To defeat such forces as a political entity, they must be isolated from their base of support and from any external help they may be receiving. If this cannot be done, victory cannot be achieved. However, if the armed non-state actor can be isolated politically, they can be defeated. More importantly, conventional military operations alone will not be able to achieve victory. If Western nations want to be successful in the battlespace of the armed non-state actor, they will need a doctrine that is as flexible and adaptive as the one they must face. Doctrine that seeks to find and fight the decisive battle will not work with this type of enemy.

ENDNOTES

INTRODUCTION TO PART I

1 Department of the Army, *Multi-Domain Battle: Combined Arms for the 21st Century* (Washington D.C.: TRADOC, 24 February 2017), 2, http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_WhitePaper.pdf, accessed 12 October 2017.

CHAPTER 1

1 Dennis M. Drew and Donald M. Snow, *Making Strategy: An Introduction to National Security Processes and Problems*, (Alabama: Air University Press, Maxwell Air Force Base, 1988), 205. For the purposes of this work, nuclear warfare will not be considered. This section was taken from Tony Balasevicius, "Adapting Military Organizations to Meet Future Shock," *The Canadian Army Journal*, Vol. 12, No. 2 (Summer 2009).

2 In January 2001, the Canadian Army adapted the NATO vision of this construct, when it published *Future Army Capabilities* and addressed a future operational environment that imagines two forms of conflict.

3 Definitions & Translations, *Definition of conventional warfare,* http://www.definitions.net/definition/conventional%20warfare, accessed 15 November 2017.

4 Ibid.

5 Department of National Defence (DND), Director Land Strategic Concepts (DLSC) Report 01/01. 2. *Future Army Capabilities* (Kingston: Fort Frontenac, Directorate of Land Strategic Concepts, January 2001), 4.

6 Wikipedia, "Asymmetric warfare," https://en.wikipedia.org/wiki/Asymmetric_warfare, accessed 15 November 2017. Asymmetric warfare "is in contrast to *symmetric warfare*, where two powers have similar military power and resources and rely on tactics that are similar overall, differing only in details and execution. The term is also frequently used to describe what is also called 'guerrilla warfare,' 'insurgency,' 'terrorism,' 'counterinsurgency,' and 'counterterrorism,' essentially violent conflict between a formal military and an informal, less equipped and supported, undermanned but resilient opponent. Asymmetric warfare is a form of irregular warfare."

7 DND DLSC Report 01/01, 2. Ibid., 4.

8 DND, *Land Operations 2021: Adaptive Dispersed Operations* (Kingston: Directorate of Land Concepts and Design, 2007), 6.

9 Wikipedia, "Nuclear warfare," https://en.wikipedia.org/wiki/Nuclear_warfare, accessed 15 November 2017.

10 DND DLSC Report 01/01, 2-4.

11 Francis G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, Va.: Potomac Institute for Policy Studies, 2007), 28, http://www.projectwhitehorse.

com/pdfs/HybridWar_0108.pdf, accessed 1 May 2015. At the time he wrote the paper, Hoffman was an employee of the Potomac Institute for Policy Studies and working for the USMC.

12 Ibid., 29.

13 Tony Balasevicius, "Adapting Military Organizations to Meet Future Shock," *The Canadian Army Journal,* Vol. 12, No. 2 (Summer 2009).

14 In a 2011 presentation for the Annual Security Review Conference, Janusz Bugajski, of the Center for Strategic and International Studies, Washington D.C., outlined three components to intra-state conflicts. These were: "a. civil conflicts precipitated by deepening political cleavages; b. economic distress, and growing inequalities, which in worst case scenarios can lead to the erosion of government legitimacy; and c. a breakdown of law and order, and escalating ungovernability. State weakness can spawn the creation of armed criminal gangs and armed vigilante groups, provoke inter-ethnic conflicts, anti-immigrant pogroms, separatist movements, and significant refugee outflows. Such developments will also stimulate the growth of organized crime and smuggling operations transcending national borders." For inter-state conflicts he noted: "These may include conflicts over the status of disputed territories and the treatment of ethnic kindred in which intra-state conflicts can pull neighboring powers into the fray. They can also involve energy conflicts and other resource disputes stemming from the short and long-term impact of climate change." Finally for trans-state conflicts he observed: "these could include international terrorism, economic sabotage, and cyber attacks that precipitate state paralysis, undermine national security, or provoke international conflicts with sponsoring states." Online at http://www.osce.org/cio/80530?download=true, pp. 1-2, accessed 15 November 2017.

15 Keir Giles, *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power* (London: Chatham House, The Royal Institute of International Affairs, 2016), 2, https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf, accessed 15 November 2017.

CHAPTER 2

1 TRADOC, *Multi-Domain Battle*, 1.

2 Stephen J. Blank, "Imperial Ambitions: Russia's Military Buildup," *World Affairs* (May/June 2015), http://www.worldaffairsjournal.org/article/imperial-ambitions-russia%E2%80%99s-military-buildup, accessed 1 October 2015.

3 Xiabing Li, *A History of the Modern Chinese Army,* (University Press of Kentucky, June 2007), 271. This section appeared in an article in Vol. 17, No. 3 of the *Canadian Military Journal,* Tony Balasevicius, "Looking for Little Green Men: Understanding Russia's Employment of Hybrid Warfare," *Canadian Military Journal,* Vol. 17, No. 3 (July 2017), http://www.journal.forces.gc.ca/Vol17/no3/page17-eng.asp, accessed 15 January 2018.

4 Dean Cheng, "Chinese Lessons from the Gulf Wars," in Andrew Scobell, David Lai, and Roy Kamphausen, eds., *Chinese Lessons from Other Peoples' Wars* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2011), 159.

5 Ibid., 159.

6 Ibid., 159.

7 Ibid., 159.

8 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare,* (Beijing: PLA Literature and Arts Publishing House, February 1999), 189, http://www.c4i.org/unrestricted.pdf, accessed 01 May 2015.

9 Ibid., 118.

10 Ibid., 190. This approach superimposes both national interests and national security requirements onto the larger strategic situation map.

11 Ibid., 190.

12 Ibid., 181.

13 Ibid., 181.

14 Major John A. Van Messel, USMC, *Unrestricted Warfare: A Chinese doctrine for future warfare?* (Quantico, VA: United States Marine Corps School of Advanced Warfighting), 7, http://www.dtic.mil/dtic/tr/fulltext/u2/a509132.pdf. The author provides a good overview of both the combinations and principles.

15 Liang and Xiangsui, *Unrestricted Warfare,* 206.

16 Ibid., 207.

17 Ibid., 207.

18 Ibid., 206-209.

19 Ibid., xx.

20 Ibid., 140. By "combined well" the authors meant the winner was able to coordinate and synchronize the different forces they had available to them to enable victory.

21 Ibid., 140.

22 Ibid., xx.

23 Ibid., 145-146.

24 Ibid., 38-43.

CHAPTER 3

1 As Richard H. Shultz, Douglas Farah, and Itamara V. Lochard, Armed *Groups: A Tier-One Security Priority,* (Colorado Springs, CO: USAF Institute for National Security Studies USAF Academy, INSS Occasional Paper 57, September 2004), 20.

2 Francis G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* (Arlington, VA.: Potomac Institute for Policy Studies, 2007), 14, http://www.projectwhitehorse.com/pdfs/HybridWar_0108.pdf, accessed 1 May 2015.

3 Ibid., 28.

4 Ibid., 29.

5 The idea of irregular warfare, referred to within the framework of the Army's notion of the future security environment is little more than a modern adaptation of the classic insurgency strategy developed and refined by Mao Zedong. In the most basic terms, Mao's insurgency, commonly referred to as the People's War, can be viewed as an uprising against an established form of authority such as a government or occupying force. Historically, insurgencies have been successful because they have evolved to meet the specific conditions of their environment and circumstances. Mao's contribution to this process was to integrate political, social and economic elements into what had been essentially a military activity. Moreover, Mao was able to solidify and refine his core ideas regarding insurgency during a period of almost continuous conflict between 1927 and 1949, where he fought wars against the Kuomintang, China's Nationalist Party, and the Japanese. Mao believed that military strategy had to be directly connected to the economic and political ideology it was seeking to establish. However, Mao's greatest influence on the development of modern insurgency lays in his innovative solution for overcoming his position of weakness. Mao understood that he did not have the material resources to defeat the Nationalists, so he redefined the rules for political and military success. In redefining these rules Mao "argued that there was a broader set of resources available on which to build power-the most important of them being the will of man..." Mao reasoned that victory could be attained as long as the struggle remained within the parameters of what the "human will" was capable of achieving. In this respect, Mao was able to shift the centre of gravity from possessing military capability to controlling the people. Major William L. Cogley, the former Chief of the Asian Studies at the USAF Special Operations School, explains, "Failure to recognize, or refusal to accept, [this] different nature of armed struggle…has been the major stumbling block for those attempting to counter it…" William L. Cogley, *A New Look at People's War*, *Air University Review*, July-August 1977, http://www.airpower.maxwell.af.mil/airchronicles/aureview/1977/jul-aug/cogley.html, accessed 12 January 2008.

6 Bard E. O'Neill, *Insurgency & Terrorism: Inside Modern Revolutionary Warfare* (Washington, DC: Brassey's, 1990), 13. O'Neill, a recognized expert on the subject, articulates this concept as a "struggle between a non-ruling group and the ruling authorities in which the non-ruling group consciously uses political resources (e.g., organizational expertise, propaganda and demonstrations) and violence to destroy, reformulate, or sustain the basis of legitimacy." It should be noted that over the past few years, Western nations have come to recognize the trans-national nature of modern insurgencies and now refer to insurgency as, "a competition involving at least one non-state movement using means that include violence against an established authority to achieve political change (Definition as developed by a COIN study group during USMC Joint Urban Warrior 2005. Taken from National Defence, *Canadian Army Counter-Insurgency Operations* (Draft) (Kingston: LFDTS, 2005).

7 O'Neill, *Insurgency & Terrorism*, 17.

8 The concept of insurgency is not new to military operations. In fact, insurgencies have been around for almost as long as organized warfare. Examples of such struggles

can be found in ancient Egypt and China, while the Roman, Ottoman and Napoleonic empires each had to deal with various types of insurgencies throughout their histories. More recently, there have been numerous insurgencies in response to European colonial expansion into Asia and Africa. Interestingly, conventional military forces have also used elements of insurgency doctrine through the use of Special Forces in support of conventional operations since the First World War.

9 C. P. Fitzgerald, *Mao Tse-tung and China,* (New York: Holmes & Meier Publishers, 1976), 16, 26, 38. Also see Chang, Jung, and Jon Halliday, *Mao The Unknown Story* (New York: Knopf, 2005.), 350-365.

10 Mao Tse-tung, *On Protracted War,* (Reference Archive: marxists.org, 2000.), http://www.marxists.org/reference/archive/mao/works/1937/guerrilla-warfare/index.htm, accessed 10 March 2008.

11 Mao Zedong, *On Practice: On the Relation between Knowledge and Practice, Between Knowing and Doing (July 1937),* (Peking: Foreign Languages Press, Selected works of Mao Tse-Tung, 1967), 299. Mao believed knowledge also came from what he refers to as indirect experience, or "all knowledge from past times and foreign land." That being said, he was quick to point out that it was only reliable if during the course of their direct experience the requirement of "scientific abstraction" had also been fulfilled. Mao validates this theory by suggesting "the reason why Marx, Engels, Lenin and Stalin could work out their theories was mainly that they personally took part in the practice of the class struggle and the scientific experimentation of their time." He asserts, "Lacking this condition, no genius could have succeeded. The saying, "without stepping outside his gate the scholar knows all the wide world's affairs", was to him mere empty talk.

12 Edward E. Rice, *Mao's Way,* (Berkeley: University of California Press, 1972), 55.

13 "Get Organized!" (November 29,), Selected Works, Vol. III, 153, http://www.marxists.org/reference/archive/mao/works/red-book/ch09.htm, accessed 15 March 2008.

14 Han Suyin, *The Morning Deluge; Mao Tsetung and the Chinese Revolution, 1893-1954,* (Boston: Little, Brown, 1972), 197. This control was absolute. To oversee army-political indoctrination it was decided that a ratio of one-Party member to two non-Party members in the Army would now be the norm. As a result, "Mao would always consider the Red Army as the training ground for Party cadres, since armed struggle [not combat operations] was the dominant factor in the Revolution in China."

15 Philip Short, *Mao: A Life*. (London: Hodder and Stoughton, 1999), 211.

16 Ibid., 197.

17 Ibid., 197.

18 Suyin, *The Morning Deluge,* 175-176.

19 Mao Tse-tung, *On Guerrilla Warfare,* 2. Within the context of today's military Campaign Planning Process these steps would be referred to as Decisive Points.

20 Ibid.

21 Mao Tse-tung, *On Protracted War*, 21.

22 Ibid., 21.

23 Ibid., 21. Mao understood that it is only through this phase that the enemy can ultimately be defeated.

24 John J. McCuen, *The Art of Counter – Revolutionary War: The Strategy of Counter-Insurgency*, (London: Faber and Faber, 1966), 30. Part of McCuen's quote was taken from Mao Tes-tung, *Strategic Problems in the Anti-Japanese guerrilla War*, Vol II, Selected Works (New York: International Publishers, 1954), 125.

25 Julian Paget, *Counter-insurgency Campaigning* (London: Faber and Faber Limited, 1967), 23.

26 Fitzgerald, *Mao Tse-tung and China,* 26.

27 A report, entitled *How to Hold On To and Consolidate the Anti-Japanese Democratic Base Areas*, carried in Party Life, published by the Northern Bureau of the CPC Central Committee on January 15, 1943, http://english.peopledaily.com.cn/dengxp/vol1/text/a1070.html, accessed 10 December 2007. It is important to remember that Mao distinguishes the difference between defending and securing an area or base. The task of defending was the responsibility of the Red Army. On the other hand, securing the area was the task given to the Red Guards, all of whom were drawn from the local inhabitants and formed the backbone of the Communists' guerrilla forces.

28 McCuen, *The Art of Counter,* 196-206. Within the construct of the people's war, only when such units were initially not available did the task fall to the Red Army.

29 Michael Elliott-Bateman, *Defeat in the East: The Mark of Mao Tse-Tung on War* (London: Oxford U.P., 1967), 124.

30 Robert Taber, *The War of the Flea: A Study of Guerrilla Warfare Theory and Practice* (New York: L. Stuart, 1965), 52-53.

31 Ibid., 48-49.

32 William L. Cogley, "A New Look at People's War," *Air University Review* (July-August 1977), http://www.airpower.maxwell.af.mil/airchronicles/aureview/1977/jul-aug/cogley.html, accessed 12 January 2008.

33 Mao Tse-tung, *On Guerrilla Warfare*, 3.

34 Mao Tse-tung, *On Protracted War*, 52. Mao did go on to state, "The principle of the Eighth Route Army [18th Group Army] is, 'Guerrilla warfare is basic, but lose no chance for mobile warfare under favorable conditions.'"

35 Mao Tse-tung, *On Guerrilla Warfare*, 37.

36 Ibid., 37. This emphasis was due to the fact that such forces may be the only ones available to the insurgent during the initial stages of the conflict.

37 Ibid., 21.

38 Ibid., 30.

39 Ibid., 30. He added, "I do not mean that every guerrilla group can have, at its inception, officers of such qualities. The officers must be men naturally endowed with good qualities which can be developed during the course of campaigning. The most important natural quality is that of complete loyalty to the idea of people's emancipation. If this is present, the others will develop; if it is not present, nothing can be done."

40 Cogley, *A New Look at People's War*.

41 Ibid.

42 Mao Tse-tung, *On Protracted War*, 49.

43 Ibid., 49-53.

44 Ibid., 38.

45 Ibid., 38. In fact, most battles initiated by the Red Army usually last a few minutes.

46 Ibid., 38.

47 Peter Paret, Craig Gordon Alexander, and Felix Gilbert, *Makers of Modern Strategy: From Machiavelli to the Nuclear Age,* (Princeton, N.J.: Princeton University Press, 1986), 839.

48 Mao Tse-tung, *On Protracted War*, 24.

49 Ibid., 24.

50 Ibid., 24.

51 Mao Tse-tung, *On Guerrilla Warfare,* 30.

52 Ibid., 238.

53 Thomas M. Huber, ed., *Compound Warfare That Fatal Knot,* (Fort Leavenworth: U.S. Army Command and General Staff College Press, 2002).

54 Ibid., 2.

55 Ibid., 2-5. Huber does qualify this by stating, "Although the model of compound warfare offered here has been kept simple in hopes that it will serve as a convenient framework for analysis, readers should remember that enormous variety exists in the historical cases of compound warfare. As in most other realms of military thought, the theory is simple but the reality is complex. The CW model assumes that one side in a CW conflict uses CW methods and the other does not. In reality, both sides may use CW methods. In most historical cases of compound warfare, one side uses CW methods predominantly; the other side deliberately uses them to the extent it is able. The model assumes two kinds of force, regular or conventional force, and irregular or guerrilla force. Several types of mobile regional militias may fall between these two poles and may contribute importantly to the leverage of the CW operator. In other words, various intermediate types of force are possible between the regular and irregular models promulgated here for simplicity."

56 Huber, *Compound Warfare,* 92. "For example, the number of irregulars operating with Wellington's forces during the Spanish campaign provides some insight into effectiveness of compound warfare. Huber states that "France had 320,000 troops in Spain at the height of its presence in 1810 and…during their six-year campaign, French forces lost 240,000 men. Of these, 45,000 were killed in action against conventional forces, 50,000 died of illness and accident, and 145,000 were killed in action against guerrilla forces." By comparison, he estimates that "…Wellington's army in Spain at its height had only about 40,000 troops, with some 25,000 Portuguese forces attached." Also see David G. Chandler, *On the Napoleonic Wars* (London: Greenhill, 1994), 155-174.

CHAPTER 4

1 Dean Cheng, "Unrestricted Warfare: Review Essay II," *Small Wars & Insurgencies* (Spring 2000): 123, http://www.tandfonline.com/doi/abs/10.1080/09592310008423266?journalCode=fswi20&, accessed 3 May 2015.

CHAPTER 5

1 Lothar Ibrügger, *The Revolution in Military Affairs Special Report*, (NATO Parliamentary Assembly, November 1998), http://www.iwar.org.uk/rma/resources/nato/ar299stc-e.html#1, accessed 6 December 2017. Ibrügger states, "Some analysts maintain that there have been only three and that these have been linked to the nature of the societies: agrarian, industrial, and information. Others have identified as many as fourteen. There is agreement, however, that technology alone is insufficient to bring about a true revolution in military affairs. For example, almost five centuries elapsed between the invention of gunpowder and its large-scale employment on the battlefield; and in the early stages of the Second World War, Germany's innovative operational concept that using communications technologies to integrate land and air forces enabled it to defeat French and British forces equipped with very similar technology. In other words, an appropriate operational concept is just as important as technological invention in bringing about a revolution in military affairs."

2 Elinor Sloan, *Military Transformation: Key Aspects and Canadian Approaches* (Ottawa: Canadian Defence & Foreign Affairs Institute, December 2007), 1, https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/41/attachments/original/1413661346/Military_Transformation.pdf?1413661346, accessed 21 December 2017.

3 Ibid., 1. Over the last 27 years these systems have continued to advance with experience and ongoing experimentation being gained from the wars in Afghanistan, Iraq and the War on Terror.

4 Ibid., 1.

5 Ibid., 1.

6 Ibid., 1.

7 John L. Romjue, *TRADOC Annual Command History 1994: Chapter 4 Doctrine*, (Washington D.C.: TRADOC, 1994), http://www.tradoc.army.mil/historian/pubs/chap4.htm, accessed 27 December 2017.

8 Ibid.

9 Ibid.

10 Ibid.

11 Ibid.

12 Ibid.

13 Department of the Army, *Force XXI Operations A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century – TRADOC Pamphlet 525-5* (Washington D.C.: TRADOC, 1 August 1994), 2-9, http://www.dtic.mil/dtic/tr/fulltext/u2/a314276.pdf, accessed 12 March 2017.

14 Ibid., 3-10.

15 Ibid., 3-12.

16 Ibid., 3-12.

17 Sloan, *Military Transformation*, 2.

18 Global Security.org, "Chapter 6 Conducting Full Spectrum Operations," http://www.globalsecurity.org/military/library/policy/army/fm/3-0/ch6.htm, accessed 28 October 2017.

19 Ibid.

20 Ibid.

21 Ibid.

22 Department of the Navy, *A Concept for Distributed Operations* (Washington, D.C.:, Headquarters U.S. Marine Corps, 25 April 2005), 1-2, http://indianstrategicknowledgeonline.com/web/A%2Concept%20for%20Distributed%20Operations.pdf, accessed 28 October 2017.

23 Ibid., 1-2.

24 Ibid., 2-4.

25 Ibid., 1-2.

26 Ibid., 2.

27 Robert E. Schmidle, *Distributed Operations: From the Sea,* (Quantico: Marine Corps Association and Foundation, July 2004), https://www.mca-marines.org/leatherneck/distributed-operations-sea, accessed 21 October 2017.

28 Ibid.

29 United States Army, *Multi-Domain Battle: Combined Arms for the 21st Century* (Washington D.C.: TRADOC, February 2017.), http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_WhitePaper.pdf, accessed 20 June 2017.

30 Ibid., 1.

31 Ibid., 3.

32 Ibid., 3.

33 Ibid., 3.

34 Ibid., 3.

35 Ibid., 1.

36 Wikipedia, "Deep operation," https://en.wikipedia.org/wiki/Deep_operation, accessed 18 January 2018.

37 Ibid.

38 Dr. Richard Harrison, "Architect of Soviet Victory in World War II: The Life and Theories of G.S. Isserson," Lecture given to the USAHAC, November 17, 2010, https://www.youtube.com/watch?v=56N9iPjQDIU, accessed 22 January 2018.

39 Ryan Patrick Hopkins, "The Historiography of the Allied Bombing Campaign of Germany," unpublished Electronic Theses and Dissertations Paper, 2008, 6-14, http://dc.etsu.edu/etd/2003, accessed 18 January 2018.

40 Colonel John A. Warden III, "Air Theory for the Twenty-First Century," in Karl P. Magyar, ed., *Challenge and Response: Anticipating U.S. Military Security Concerns* (Maxwell AFB, AL: Air University Press, August 1994), 311-332, https://media.defense.gov/2017/Mar/31/2001725260/-1/-1/0/B_0056_MAGYAR_CHALLENGE_RESPONSE.PDF, accessed 20 January 2018.

41 Gary M. Jackson, *USAF Warden's Five-Ring System Theory: Legitimate Wartime Military Targeting or an Increased Potential to Violate the Law and Norms of Expected Behavior?* (Maxwell Air Force Base, AL: Air Command and Staff College Air University, April 2000), 3-4, http://www.dtic.mil/dtic/tr/fulltext/u2/a425331.pdf, accessed 18 January 2018.

42 Warden, "Air Theory for the Twenty-First Century," 317.

43 Lewis Ware, "Some Observations on the Enemy as a System," *Airpower Journal*, Vol. 9, No. 4 (Winter 1995): 87-93.

44 David Jablonsky, "National Power," in Joseph R. Cerami, and James F. Holcomb, Jr., *U.S. Army War College Guide To Strategy* (Carlisle, PA: U.S. Army War College, February 2001), 87, http://www.au.af.mil/au/awc/awcgate/ssi/00354.pdf, accessed 18 January 2018.

45 Ibid., 88.

46 Ibid., 88.

47 Ibid., 90.

48 Ibid., 90.

49 Ibid., 90.

50 R Hopkins, *The Historiography of the Allied Bombing Campaign of Germany,* 14.

51 Ibid., 30.

52 Ibid., 30.

CHAPTER 6

1 Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington D.C.: Institute for the Study of War, 2015), 11, http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf, accessed 1 October 2015.

2 Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear," *In Moscow's Shadows* (Blog), ND, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/, accessed 16 November 2024. Many authorities on Russia believe that the article may have been written by someone else. Also, the same briefing was presented by the Chief of the Russian General Staff, Army General Valeriy Gerasimov, in January 2013 at the Russian Academy of Military Sciences' annual meeting; key elements of the Gerasimov Doctrine have since been integrated into the new edition of the Russian Military Doctrine, as approved in December 2014.

3 Ibid.

4 Ibid.

5 Ibid.

6 Colonel (Reserve) S.G. Chekinov and Lieutenant General (Retired) S.A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought*, No. 4 (2013): 13, http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf, accessed 5 July 2015.

7 Ibid.

8 Galeotti, "The 'Gerasimov Doctrine.'"

9 Ibid.

10 Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga: National Defense Academy of Latvia, Center for Security and Strategic Research; Policy Paper No. 02, April 2014), 6.

11 Ibid., 6.

12 Chekinov and Bogdanov, *The Nature and Content*, 13.

13 Galeotti, "The 'Gerasimov Doctrine.'"

14 Ibid.

15 Ibid.

16 Chekinov and Bogdanov as quoted in Janis Berzins, *"Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,"* Policy Paper 2, Center for Security and Strategic Research, National Defence Academy of Latvia, 6 April 2014.

17 Ibid.

18 It is important to note that other activities could be included such as economic warfare, legal warfare, … Also, it is interesting to note that four of the six activities on this list do not fall under the traditional idea of war and these four would be the most likely activities to be employed by Russia against Arctic Council members.

19 Murimi Stephen, "Cyber Warfare Assess of Russia," (Academia, Aug 2014,) p. 1, post online at http://www.academia.edu/9689387/Cyber_Warfare_Assess_of_Russia, retrieved 7 October 2015.

20 Ibid.

21 Jason Richards, "Denial-of-Service: The Estonian Cyber war and Its Implications for U.S. National Security," *International Affairs Review*, http://www.iar-gwu.org/node/65, accessed 7 October 2015.

22 Stephen, "Cyber Warfare Assess of Russia," 14.

23 Keir Giles, "Information Troops: A Russian Cyber Command?" (3rd International Conference on Cyber Conflict, C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011 © CCD COE Publications), 46, https://ccdcoe.org/ICCC/materials/proceedings/giles.pdf, retrieved 5 October 2015.

24 Ibid.

25 In Internet slang, a "troll" is a person who sows discord on the Internet by starting arguments or upsetting people, by posting inflammatory, extraneous, or off-topic messages in an online community (such as a newsgroup, forum, chat room, or blog) with the deliberate intent of provoking readers into an emotional response. Taken from "Definition of troll," *Collins English Dictionary*, http://www.collinsdictionary.com/dictionary/english/troll, accessed 4 October 2015.

26 Pierluigi Paganini, "Russia and Ukraine: Information Warfare," (INFOSEC Institute 17 June 2014), http://resources.infosecinstitute.com/russia-ukraine-information-warfare, retrieved 4 October 2015.

27 Ibid.

28 Andrew Davenport, "The Agendas of State-Owned Enterprises Raise Foreign Policy, Not Just Domestic, Concerns," (Canadian Global Affairs Institute, December 2014), http://www.cgai.ca/agendas_of_state_owned_enterprises#SOE%20Activity, retrieved 4 October 2015.

29 Tom Porter, "Gangs of Russia: Ruthless mafia networks extending their influence," *International Business Times*, 9 April 2015, http://www.ibtimes.co.uk/gangs-russia-ruthless-mafia-networks-extending-their-influence-1495644, retrieved 14 October 2015.

30 Luke Harding, "WikiLeaks cables condemn Russia as 'mafia state'," *The Guardian*, 1 December 2010, http://www.theguardian.com/world/2010/dec/01/wikileaks-cables-russia-mafia-kleptocracy, retrieved 11 October 2015.

31 Alexey Eremenko, "Blackwater.ru: The Future of Russian Private Military Companies," *The Moscow Times*, 12 November 2012, http://www.themoscowtimes.com/news/article/blackwater-ru-the-future-of-russian-private-military-companies/511056.html, retrieved 11 October 2015. Note: in fact, a bill has already been filed with the Russian parliament, the State Duma, to legalize PMSCs in that country.

32 Mark Galeotti, "Russia and 'elastic power': will the burgeoning private security industry lead to private military companies, too?," *In Moscow's Shadows* (Blog), https://inmoscowsshadows.wordpress.com/2013/06/16/russia-and-elastic-power-will-the-burgeoning-private-security-industry-lead-to-private-military-companies-too/, retrieved 7 October 2015.

33 Ibid.

34 Ibid.

INTRODUCTION TO PART II

1 Ben Taub, "Russia's Espionage War in the Arctic," *The New Yorker*, 9 September 2024, https://www.newyorker.com/magazine/2024/09/16/russias-espionage-war-in-the-arctic, accessed 8 October 2024.

2 Ibid. For years, Russia has been using the Norwegian town of Kirkenes, which borders its nuclear stronghold, as a laboratory, testing intelligence operations there before replicating them across Europe.

3 Ibid.

4 Ibid.

5 This project was in press at the time of Israel's invasion of Lebanon in October 2024. Therefore, it will not include results of that conflict.

CHAPTER 7

1 Office of Strategic Services, *Simple Sabotage Field Manual (Provisional)*, (Washington, D.C.: OSS, 17 January 1944), 1-6.

2 Howard L. Douthit, III, *The Use and Effectiveness of Sabotage as A Means of Unconventional Warfare - An Historical Perspective from World War I Through Viet Nam*, (Wright Patterson AFB, OH: Air Force Institute of Technology, Air University, September 1987), 100-104, https://apps.dtic.mil/dtic/tr/fulltext/u2/a188034.pdf, accessed 10 December 2020. Also see Wikipedia, "Sabotage," https://en.wikipedia.org/wiki/Sabotage.

3 OSS, *Simple Sabotage Field Manual*, 1-4.

4 Ibid., 1.

5 John Markoff, "Old Trick Threatens the Newest Weapons," *The New York Times*, 26 October 2009; "Secure Sources Lacking for Weapons Electronics," *The New York Times*, http://www.nytimes.com, accessed 1 December 2020. According to Markoff, "In 2004, Thomas C. Reed, an Air Force secretary in the Reagan administration, wrote that the United States had successfully inserted a software Trojan horse into computing equipment that the Soviet Union had bought from Canadian suppliers. Used to control a Trans-Siberian gas pipeline, the doctored software failed, leading to a spectacular explosion in 1982." Also see Wired Staff, "Soviets Burned by CIA Hackers?" *WIRED*, 26 March 2004, https://www.wired.com/2004/03/soviets-burned-by-cia-hackers/.

6 McAfee, "What is Stuxnet?," https://www.mcafee.com/enterprise/en-ca/security-awareness/ransomware/what-is-stuxnet.html#:~:text=Share%3A,used%20to%20automate%20machine%20processes, accessed 12 November 2020. According to McAfee, "Over time, other groups modified the virus to target facilities including water treatment plants, power plants, and gas lines." The website states, "Stuxnet was a multi-part worm that traveled on USB sticks and spread through Microsoft Windows computers. The virus searched each infected PC for signs of Siemens Step 7 software, which industrial computers serving as PLCs use for automating and monitoring electro-mechanical equipment." It goes on to say, "After finding a PLC computer, the malware attack updated its code over the internet and began sending damage-inducing instructions to the electro-mechanical equipment the PC controlled. At the same time, the virus sent false feedback to the main controller. Anyone monitoring the equipment would have had no indication of a problem until the equipment began to self-destruct."

7 David E. Hoffman, "Reagan Approved Plan to Sabotage Soviets." *The Washington Post*, 27 February 2004, https://www.washingtonpost.com/archive/politics/2004/02/27/reagan-approved-plan-to-sabotage-soviets/a9184eff-47fd-402e-beb2-63970851e130/, accessed 12 November 2020.

8 Government of Canada, "A Comparative Assessment of Electronic Voting, Part IV: European Trials, Estonia," (Elections Canada, archived file on the web), https://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote/comp&document=euro&lang=e, accessed 12 November 2020.

9 Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2018), https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf, accessed 15 November 2020.

10 Encyclopedia Britannica, "Cold War International Politics," https://www.britannica.com/event/Cold-War, accessed 12 November 2020.

11 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security*, Vol. 4, No. 2 (2011): 50, https://www.jstor.org/stable/26463926, accessed December 15, 2020.

12 Ibid., 50.

13 Andreas Schmidt, "The Estonian Cyberattacks," in Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association,

2013), 2, https://www.researchgate.net/publication/264418820_The_Estonian_Cyber attacks, accessed 12 November 2020.

14 Ibid., 2.

15 Ibid., 2.

16 Damien McGuinness, "How a cyber attack transformed Estonia," *BBC News*, 27 April 2017, https://www.bbc.com/news/39655415, accessed 12 November 2020.

17 Ottis, *Analysis of the 2007 Cyber Attacks*.

18 NATO Strategic Communications, "2007 Cyber Attacks on Estonia," Stratcomcoe.org, 55, https://www.stratcomcoe.org/download/file/fid/80772, accessed 12 November 2020.

19 Paloalto Networks, "What is a Denial-of-Service Attack (DoS)?" https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial-of-Service%20(DoS)%20attack%20is%20an%20attack%20meant,or%20sending%20it%20information%20that%20triggers%20a%20crash. According to the website, the main purpose of a DoS attack is to, "prevent legitimate users (i.e., employees, members, or account holders) from accessing the service or resource they use. This normally includes the targeting the web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations."

20 Ibid.

21 Max Gordon, *Lessons from The Front: A Case Study of Russian Cyber Warfare,* (Montgomery, AL: Air Command and Staff College Air University, December 2015), 8-9. Also see Ottis, *Analysis of the 2007 Cyber Attacks*.

22 Dan Verton, "Black Hat Highlights Real Danger of Script Kiddies, Reckless probing by amateurs could actually be helping cybercriminals," *Computerworld*, July 23, 2001, https://www.computerworld.com/article/2581986/black-hat-highlights-real-danger-of-script-kiddies.html, accessed 21 November 2020.

23 Schmidt, "The Estonian Cyberattacks," 9.

24 Akamai, "What is a Botnet Attack," https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp#:~:text=A%20botnet%20is%20a%20collection,data%20theft%20and%20DDoS%20attacks, accessed 15 November 2020.

25 Schmidt, "The Estonian Cyberattacks," 9.

26 Ibid., 9. Schmidt points out that "among the most significant attacks during this second phase were the attacks on Hansabank[,] Estonia's largest bank…"

27 McGuinness, "How a cyber attack transformed Estonia."

28 Paloalto Networks, "What is a Denial-of-Service Attack (DoS)?"

29 NATO Strategic Communications, "2007 Cyber Attacks on Estonia," 60.

30 Ibid., 59.

31 Anastasia Nevskaya, "Russian-Estonian Economic and Investment Cooperation During the Crisis: Dynamics and Possibilities," (Institute of World Economy and International Relations, Russia, Moscow, ResearchGate, May 2015), 38, https://www.researchgate.net/publication/285043517_Russian-Estonian_Economic_and_Investment_Cooperation_During_the_Crisis_Dynamics_and_Possibilities/link/5d26104ca6fdcc2462d325c1/, accessed 15 November 2020.

32 Ibid., 38.

33 Ibid., 39. Nevskaya estimates that about 10 transit companies had to stop operations completely and about 200 employees were laid off because of Russian actions.

34 Gordon, *Lessons from The Front*, 8-9.

35 Ibid., 8-9.

36 Ibid., 8-9.

37 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *WIRED*, 21 August 2007, https://www.wired.com/2007/08/ff-estonia/, accessed 23 November 2020.

38 Gordon, *Lessons from The Front*, 8-10.

39 Ibid., 8-9.

40 Schmidt, "The Estonian Cyberattacks," 8. Also see Republic of Estonia, Information System Authority, the Computer Emergency Response Team (CERT-EE), https://www.ria.ee/en/cyber-security/cert-ee.html, accessed 18 November 2020. According to its website Estonia's CERT "is to assist Estonian Internet users in the implementation of preventive measures to reduce possible damage from security incidents and to help them in responding to security threats. CERT-EE deals with security incidents that occur in Estonian networks, start there, or which it has been notified about by citizens or institutions either in Estonia or abroad."

41 NATO Strategic Communications, "2007 Cyber Attacks on Estonia," 60.

42 Gordon, *Lessons from The Front*, 10; and NATO Strategic Communications, "2007 Cyber Attacks on Estonia," 59.

43 Ottis, *Analysis of the 2007 Cyber Attacks*.

44 Ibid.

45 Gordon, *Lessons from The Front*, 8-9.

46 NATO Strategic Communications, "2007 Cyber Attacks on Estonia," 59.

47 Ottis, *Analysis of the 2007 Cyber Attacks*.

48 Ibid.

49 Ibid.

50 Luke Harding, "Russian Election Unfair and Biased Towards Putin, Observers Say." *The Guardian*, 4 December 2007, https://www.theguardian.com/world/2007/dec/04/russia.lukeharding, accessed 14 November 2020.

51 Schmidt, 17.

52 Herzog, "Revisiting the Estonian Cyber Attacks," 54. For an official breakdown of the policy changes see the NATO Cyber Defence Factsheet, 20160627_1607-factsheet-cyber-defence-eng.pdf (nato.int), accessed 14 November 2020. Also, although it is not part of the NATO Command Structure, the Centre offers recognised expertise and experience on cyber defence.

53 Herzog, "Revisiting the Estonian Cyber Attacks," 54-55.

54 Ibid., 55.

55 Ibid., 55.

56 Ibid., 55.

57 North Atlantic Treaty Organization, *NATO Cyber Defence Factsheet* (Brussels: Public Diplomacy Division (PDD) July 2016), 20160627_1607-factsheet-cyber-defence-eng.pdf (nato.int); and NATO, "News: NATO and the European Union enhance cyber defence cooperation," 10-Feb-2016, accessed 14 November 2020.

58 Ibid.

59 Ottis, *Analysis of the 2007 Cyber Attacks*.

60 Ibid.

61 Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," 56.

62 Ibid., 54-56.

CHAPTER 8

1 Francis G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 14, http://www.projectwhitehorse.com/pdfs/HybridWar_0108.pdf, accessed 01 May 2015.

2 *Commander Shannon Wells*, "In A World Without Doctrine, Chaos Reigns Supreme" (NATO Website), https://www.jwc.nato.int/newsroom/warfare-development-focus/world-without-doctrine-chaos-reigns-supreme#:~:text=NATO%20defines%20doctrine%20as%2C%20%22Fundamental,but%20requires%20judgement%20in%20application.%22, accessed 17 January 2024. It is important to note that although it is authoritative, it does require judgement in application.

3 Ambassador Chas W. Freeman, Jr., USFS (Ret.), "Mao Zedong: Nationalist in Spite of Himself," (Remarks to the SAIS China Forum, Middle East Policy Council), https://mepc.org/speeches/mao-zedong-nationalist-spite-himself/, accessed 14 January 2024.

4 Stephen Watts, Bryan Frederick, Nathan Chandler, Mark Toukan, Christian Curriden, Erik E. Mueller, Edward Geist, Ariane M. Tabatabai, Sara Plana, Brandon Corbin, and Jeffrey Martini, *Proxy Warfare in Strategic Competition: State Motivations and Future Trends* (Santa Monica, CA: RAND Corporation, 2023), 1-6 https://www.rand.org/pubs/research_reports/RRA307-2.html, accessed 20 August 2024.

5 Kali Robinson, "What is Hezbollah?" (Council on Foreign Relations, Backgrounder, last updated 30 July 2024), https://www.cfr.org/backgrounder/what-hezbollah, accessed 17 January 2024.

6 Andrew Dalack, *Hezbollah: A localized Islamic resistance or Lebanon's premier national movement?* (Ann Arbor, MI: University of Michigan, 2010), 6-7, https://deepblue.lib.umich.edu/bitstream/handle/2027.42/77609/ajdalack.pdf;sequence=1, accessed 17 January 2024.

7 Dr. Yusri Hazran, *The Shiite Community in Lebanon: From Marginalization to Ascendancy,* (Waltham, MA: Brandeis University, Crown Center for Middle East Studies, June 2009), https://www.brandeis.edu/crown/publications/middle-east-briefs/pdfs/1-100/meb37.pdf, accessed 14 January 2024.

8 Hala Jaber, *Hezbollah: Born with Vengeance* (New York, Columbia University Press, 1997), 14. Also see Encyclopaedia Britannica, "Lebanese Civil War summary," https://www.britannica.com/summary/Lebanese-Civil-War#:~:text=The%20factions%20fought%20fiercely%20through,had%20begun%20to%20lose%20ground, accessed 9 January 2024.

9 Haugbolle Sune, *The Historiography and Memory of the Lebanese Civil War 1975-1990* (25 October 2011), https://www.sciencespo.fr/mass-violence-war-massacre-resistance/fr/document/historiography-and-memory-lebanese-civil-war.html, accessed 21 January 2024.

10 Ibid.

11 Nicholas Blandford, *Lebanon: The Shiite Dimension*, 13 July 2022, https://www.wilsoncenter.org/article/lebanon-the-shiite-dimension, accessed 2 May 2024.

12 CIA, "The Amal Movement in Lebanon," (National Foreign Assessment Center, 20 November 1981), https://www.cia.gov/readingroom/docs/CIA-RDP83M00914R000300020014-6.pdf, accessed 1 February 2024.

13 Casey L. Addis, Christopher M. Blanchard, *Hezbollah: Background and Issues for Congress* (Washington D.C.: Congressional Research Service, 3 January 2011), 7, https://sgp.fas.org/crs/mideast/R41446.pdf, accessed 12 February 2024.

14 Ibid., 7.

15 Ibid., 7.

16 Catherine Bloom, "The Classification of Hezbollah in Both International and Non-International Armed Conflicts," *Annual Survey of International & Comparative Law*, Vol. 14, Issue 1 (2008): 62-69, https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1121&context=annlsurvey, accessed 1 February 2024.

17 Jewish Virtual Library, "A Project of Aice, Hezbollah: History and Overview," https://www.jewishvirtuallibrary.org/history-and-overview-of-hezbollah#tactic, accessed June 2024.

18 Dominique Avon, Anaïs-Trissa Khatchadourian, Jane Marie Todd, *Hezbollah: A History of the "Party of God"* (Cambridge, MA: Harvard University Press, 2012). See also Ashley Lane, "Iran's Islamist Proxies in the Middle East," Wilson Center, http://www.wilsoncenter.org, accessed 11 February 2024.

19 Lisa Brennen, *Hezbollah: Psychological Warfare Against Israel* (Monterey CA: Naval Postgraduate School, 2009), https://apps.dtic.mil/sti/tr/pdf/ADA496916.pdf, 17, accessed 12 January 2024. Around this time, Syria had intervened to bring about an understanding between the two main Shiite groups, Hezbollah and its rival Amal. This action eventually allowed the group to stop its infighting to focus its efforts on improving capabilities, and fight the occupation.

20 Thanassis Cambanis, *A Privilege to Die: Inside Hezbollah's Legions and Their Endless War Against Israel* (New York: Free Press, 2011), 111.

21 Ibid., 111.

22 Ibid., 112.

23 Iver Gabrielsen, "Hezbollah's Strategy and Tactics in the Security Zone from 1985 to 2000," *Small Wars Journal*, 11 July 2013, https://smallwarsjournal.com/jrnl/art/hezbollahs-strategy-and-tactics-in-the-security-zone-from-1985-to-2000#_edn5, accessed 12 February 2024.

24 Kali Robinson, "What is Hezbollah? What to know about its origins, structure and history," *PBS News*, 16 October 2023, https://www.pbs.org/newshour/world/what-is-hezbollah-what-to-know-about-its-origins-structure-and-history, accessed 14 February 2024.

25 Naim Qassem, *Hizballah: the Story from Within* (London: Saqi, 2005), 83. See also Iver Gabrielsen, "Hezbollah's Strategy and Tactics."

26 Robinson, *What is Hezbollah?*

27 Gabrielsen, "Hezbollah's Strategy and Tactics."

28 Brennen, *Hezbollah: Psychological Warfare Against Israel*, 16. She goes on to state, "Consequently, the group was careful when conducting military operations to avoid causing unnecessary collateral damage."

29 Shmuel L. Gordon, *The Vulture and The Snake Counter-Guerrilla Air Warfare: The War in Southern Lebanon* (Ramat Gan: Begin-Sadat Center for Strategic Studies Bar-Ilan University, 1998), 9, https://smallwarsjournal.com/documents/gordon1.pdf, accessed 17 February 2024.

30 Directorate of Intelligence, CIA, "Lebanon–Israel: Hizballah's Strategy and Capabilities," *Near East and South Asia Review,* 23 January 2017, 18, https://www.cia.gov/readingroom/docs/CIA-RDP05S02029R000300940004-7.pdf, accessed 21 February 2024.

31 Ibid., 18.

32 Hala Jaber, *Hezbollah* (New York, Columbia University Pres,1997), 37.

33 Gabrielsen, "Hezbollah's Strategy and Tactics."

34 Ibid.

35 Christopher E. Whitting, *When David became Goliath*, (Carlisle, PA: U.S. Army Command and General Staff College, 2001), 86, https://apps.dtic.mil/sti/tr/pdf/ADA397303.pdf, accessed 21 February 2024.

36 Directorate of Intelligence, "Lebanon-Israel," 19.

37 Gabrielsen, "Hezbollah's Strategy and Tactics."

38 Ibid.

39 The Institute for National Security Studies, "Strategic Assessment: Intelligence Agents in Israel: Hezbollah's Modus Operandi Research Forum," July 2022, https://www.inss.org.il/strategic_assessment/intelligence-agents-in-israel-hezbollahs-modus-operandi/, accessed 23 February 2024.

40 Gabrielsen, "Hezbollah's Strategy and Tactics."

41 Alex Fishman, "What really went wrong in botched 1997 Shayetet 13 operation?" *Ynet News.com*, 21 June 2017, https://www.ynetnews.com/articles/0,7340,L-4977429,00.html, accessed 18 February 2024.

42 Ibid.

43 Matthew Levitt, "Hezbollah: A Case Study of Global Reach," Remarks to a conference on "Post-Modern Terrorism: Trends, Scenarios, and Future Threats," September 8, 2003, https://www.aclu.org/wp-content/uploads/legal-documents/ACLURM001616.pdf, accessed 2 March 2024.

44 Gabrielsen, "Hezbollah's Strategy and Tactics."

45 Ibid.

46 Whitting, *When David became Goliath*, 92.

47 Brennen, *Hezbollah: Psychological Warfare Against Israel*, 72.

48 Marc Devore, "Exploring the Iran-Hezbollah relationship: a case study of how state sponsorship affects terrorist group decision-making," *Perspectives on Terrorism*, Vol. 6, No. 4-5 (2012): 95, https://pt.icct.nl/sites/default/files/2023-09/Article%205.pdf, accessed 12 January 2024.

49 Second Lieutenant Noah Kanter, "Employing Armor in Low-intensity Conflicts: Some Lessons for the U.S. Armor Force," *Armor Magazine*, PB 17-02-1 (January–February 2002): 9-11.

50 Nicholas Blanford, "Hezbollah and the Next War with Israel," Speech, Middle East Institute, 24 May 2010, https://www.youtube.com/watch?v=ayyQApYwenA, accessed 2 March 2024.

51 Brennen, *Hezbollah: Psychological Warfare Against Israel*, 17.

52 IDF Website, "Wars and Operations, Operation Accountability," https://www.idf.il/en/mini-sites/wars-and-operations/operation-accountability/, accessed 4 March 2024.

53 Ibid.

54 Ibid.

55 Naim, *Hizballah: The Story from Within*, 109.

56 Andrew McGregor, "Hezbollah's Rocket Strategy Terrorism Monitor," *The Jamestown Foundation*, 21 August 2006, https://web.archive.org/web/20060821195430/http://jamestown.org/terrorism/news/article.php?issue_id=3830, accessed 2 June 2024.

57 Ibid.

58 Whitting, *When David became Goliath*, 86.

59 Gabrielsen, "Hezbollah's Strategy and Tactics."

60 IDF Website, "Wars and Operations, Operation Grapes of Wrath," https://www.idf.il/en/mini-sites/wars-and-operations/operation-grapes-of-wrath/, accessed 2 June 2024.

61 Human Rights Watch, "Israel/Lebanon 'Operation Grapes of Wrath'," Vol. 9, No. 8(E) (September 1997), https://www.hrw.org/reports/1997/isrleb/Isrleb.html, accessed 7 June 2024.

62 "Operation Grapes of Wrath, *Ynetnews,* 1 August 2006, https://www.ynetnews.com/articles/0,7340,L-3284744,00.html#:~:text=Operation%20Grapes%20of%20Wrath%20was,to%20the%20Lebanese%2DIsraeli%20border, accessed 7 June 2024.

63 Israel Ministry of Foreign Affairs, "Cease-fire understanding in Lebanon- and remarks by Prime Minister Peres and Secretary of State Christopher," 26 April 1996, https://web.archive.org/web/20070310234701/http://www.israel-mfa.gov.il/MFA/Foreign%20Relations/Israels%20Foreign%20Relations%20since%201947/1995-1996/Cease-fire%20understanding%20in%20Lebanon-%20and%20remarks%20b, accessed 15 June 2024.

64 United Nations, *Report of The Secretary-General on The United Nations Interim Force in Lebanon* (Security Council for the period from 22 January 1996 to 20 July 1996, dated 20 July 1996), 5-8, https://documents.un.org/doc/undoc/gen/n96/180/47/pdf/n9618047.pdf, accessed 15 June 2024.

65 Wikipedia, "Hezbollah armed strength," https://en.wikipedia.org/wiki/Hezbollah_armed_strength, accessed 12 January 2024.

66 Whitting, *When David became Goliath*, 89-90.

67 Ibid., 89-91. According to Whitting, "at 0525 hour on 2 July 1998, Hezbollah launched a coordinated attack on eighteen separate IDF and SLA positions simultaneously using approximately 125 guerillas."

68 Gabrielsen, "Hezbollah's Strategy and Tactics." It is noteworthy that these numbers do not include the 73 IDF soldiers killed when two helicopters crashed in 1997, a sudden death toll that increased Israeli opposition to the war.

69 Brennen, *Hezbollah: Psychological Warfare Against Israel*, 72.

70 Whitting, *When David became Goliath,* 92.

71 Gordon, *The Vulture and The Snake,* 17.

72 Gabrielsen, "Hezbollah's Strategy and Tactics."

73 Lieutenant Colonel S.C. Farquhar, ed., *Back to Basics: A Study of the Second Lebanon War and Operation Cast Lead* (Carlisle, PA: Combat Studies Institute Press, 2009), 6.

74 Lieutenant Colonel Kenny D. Harper and Colonel (Retired) William R. Betson, "Complex Web Defense Experiment," *Armor Magazine* (January–February 2010), https://www.moore.army.mil/armor/eARMOR/content/issues/2010/JAN_FEB/ArmorJanuaryFebruary2010web.pdf, accessed 22 June 2024. The term "complex web defense" (CWD) refers to "an array of tactical practices a future enemy might employ against U.S. forces, which denies the United States advantages of using high technology sensors, massive firepower, and protected mobility, and exploits the enemy's ability to hide in complex/urban terrain, using civilians as shields. Although many possible future enemies could employ variations of these tactics, one example of "CWD-like" tactics is how Hezbollah fought the Israelis in Lebanon during 2006. CWD has no approved U.S. Army doctrinal definition, but it is characterized by mutually supporting defensive positions, interconnected with resilient, redundant communications, and sustained by stockpiled and hidden supplies. Enemy fighters are often irregulars but are well trained and very well equipped with top-of-the-line antitank and antipersonnel weapons. This enemy is capable of executing flexible, prearranged plans and demonstrates agility at the lower tactical levels. He rarely conducts large-scale maneuver and may attempt to contest the advance of U.S. forces only when it is to his advantage. He often allows U.S. combat elements to pass and then attempts to strike follow on support or sustaining forces."

75 David E. Johnson, "Minding the Middle: Insights, from Hezbollah and Hamas for Future Warfare," *Strategic Insights*, Vol. 10, Special Issue (October 2011): 124-137 and "New Actors and Belligerents", 125-127, https://calhoun.nps.edu/server/api/core/bitstreams/c0ac27f9-8a7b-4070-9f2e-881a61b06589/content, accessed 22 June 2024.

76 Harper and Betson, "Complex Web Defense Experiment."

77 Captain Scott J. Tosi, "Xi Jinping's PLA Reforms and Redefining "Active Defense," *Military Review* (September-October 2023), https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2023/Active-Defense/, accessed 12 January 2024. Tosi states, "More simply, the PLA adopted a strategy of mobile warfare in which ground forces would conduct a strategic defense before transitioning to a counterattack to overwhelm an adversary with numerically superior forces."

78 Ibid.

79 Timothy A. Ornelas, "China's Active Defense Military Strategy," *Marine Corps Gazette* (October 2021): 57, https://www.mca-marines.org/wp-content/uploads/57-Chinas-Active-Defense-Military-Strategy.pdf, accessed 2 July 2024. However, Ornelas also notes that in 1980, "China adopted a new concept that no longer called for the ceding of territory to an invading force but rather sought to actively repel an invasion and use counter-attack forces to remove any remaining occupying force." And this shift was the foundation of the current active defense strategy.

80 Farquhar, *Back to Basics,* 6.

81 Ibid., 6. By the time the IDF commenced its attacks, Hezbollah had completed much of its doctrine and force structure transition, and was now a well-organized, highly-trained and well-equipped defensive (positional warfare) force.

82 Avi Kober, "The Israel defense forces in the Second Lebanon War: Why the poor performance?" *Journal of Strategic Studies*, 1 February 2008, https://www.tandfonline.com/doi/pdf/10.1080/01402390701785211, accessed 6 July 2024.

83 Jeremy Sharp, Christopher Blanchard, Kenneth Katzman, Carol Migdalovitz, Alfred Prados, Paul Gallis, Dianne Rennack, John Rollins, Marjorie Browne, Steve Bowman, and Connie Veillette, *Lebanon: The Israel-Hamas-Hezbollah Conflict* (Washington D.C.: CRS Report for Congress, 15 September 2006). https://www.files.ethz.ch/isn/118864/2006-09-15_Israel_Hezbollah.pdf, accessed 6 July 2024.

84 Uzi Rubin, "Hizballah's Rocket Campaign Against Northern Israel: A Preliminary Report," *www.jcpa.org*, Vol. 6, No. 10 (August 31, 2006), https://jcpa.org/article/hizballahs-rocket-campaign-against-northern-israel-a-preliminary-report/, accessed 10 July 2024.

85 Martin van Creveld, "The Second Lebanon War: A Re-assessment," *Infinity Journal*, Issue No. 3 (Summer 2011): 4-7, https://www.militarystrategymagazine.com/article/the-second-lebanon-war-a-re-assessment/, accessed 12 July 2024.

86 Farquhar, *Back to Basics,* 9-12.

87 United Nations Peacemaker, "Security Council Resolution 1701: The situation in the Middle East," https://peacemaker.un.org/israellebanon-resolution1701, accessed 15 July 2024.

88 Hoffman, *Conflict in the 21st Century*, 28.

89 Ibid., 29. Over the years, he has modified this initial definition.

90 Ibid., 14.

91 Ibid., 28.

92 Ibid., 28. Hoffman states, "In such conflicts, future adversaries (state, state-sponsored groups, or self-funded actors) will exploit access to modern military capabilities including encrypted command systems, man-portable air to surface missiles, and other modern lethal systems, as well as promote protracted insurgencies that employ ambushes, improvised explosive devices (IEDs), and coercive assassinations. This could

include states blending high-tech capabilities, like anti-satellite weapons, with terrorism and cyber-warfare directed against financial targets."

93 Ibid., 28.

94 Ibid., 14.

95 Ibid., 29. Hoffman stated that normally these units would be used to prolong the conflict, provoke overreactions or siphon off resources from the enemy.

96 Nicholas, *Hezbollah and the Next War with Israel*.

97 Gene Green, "A Terrorist Group Rearms," Congressional Record – House. 153 (Pt 2): H862–H863, https://www.govinfo.gov/content/pkg/CREC-2007-01-23/pdf/CREC-2007-01-23-pt1-PgH863.pdf, accessed 16 July 2024.

98 Ibid.

99 Encyclopaedia Britannica, "Syrian Civil War History," https://www.britannica.com/event/Syrian-Civil-War (Last Updated: 17 August 2024), accessed 17 July 2024.

100 Marisa Sullivan, *Hezbollah in Syria. Middle East Security Report 19* (Washington D.C.: The Institute for the Study of War, April 2014.), 10, https://www.understandingwar.org/sites/default/files/Hezbollah_Sullivan_FINAL.pdf, accessed 17 July 2024.

101 Ibid., 10.

102 Ibid., 10.

103 Ibid., 10.

104 Ibid., 10.

105 Ibid., 10.

106 Nicholas Blanford, "The Battle for Qusayr: How the Syrian Regime and Hizb Allah Tipped the Balance," *Combating Terrorism Center Sentinel*, Syria Special Issue, Vol. 6, Issue 8, https://ctc.westpoint.edu/the-battle-for-qusayr-how-the-syrian-regime-and-hizb-allah-tipped-the-balance/, accessed 20 July 2024.

107 Ibid.

108 Elizabeth O'Bagy, "The fall of al-Qusayr," *Institute for the Study of War*, Backgrounder, 6 June 2013, https://www.understandingwar.org/backgrounder/syria-update-fall-al-qusayr, accessed 20 July 2024.

109 Ibid.

110 Ibid.

111 Sullivan, *Hezbollah in Syria*, 16-17.

112 Ibid., 24-26.

113 O'Bagy, "The fall of al-Qusayr."

114 Ibid.

115 DW News, "What you need to know about Hezbollah," 28 July 2024, https://www.dw.com/en/what-you-need-to-know-about-hezbollah/a-67093061, accessed 20 July 2024.

116 *Yair Ramati and Yaakov Lappin,* "The growing air defense capabilities of Hezbollah and Iranian proxies – An emerging threat to Israel and the West," 21 December 2023, https://israel-alma.org/2023/12/21/the-growing-air-defense-capabilities-of-hezbollah-and-iranian-proxies-an-emerging-threat-to-israel-and-the-west/, accessed 20 July 2024.

117 Ibid.

118 Mohamad El Chama and Samuel Granados, "What to know about Hezbollah weapons as Israel awaits retaliatory strikes," https://www.washingtonpost.com/world/2024/07/10/hezbollah-weapons-israel-war-border-nasrallah/, accessed 20 July 2024.

119 Ibid.

CHAPTER 9

1 Peter Grier and Faye Bowers, "Iraq's bin Laden? Zarqawi's rise," *Christian Science Monitor,* 14 May 2004, https://www.csmonitor.com/2004/0514/p03s01-usfp.html, accessed 22 June 2018.

2 Aaron Y. Zelin, *The War between ISIS and al-Qaeda for Supremacy of the Global Jihadist Movement* (Washington D.C.: Washington Institute for Near East Policy, June 2014), 1-2, http://www.washingtoninstitute.org/uploads/Documents/pubs/ResearchNote_20_Zelin.pdf, accessed 14 February 2018. This included Iraqi interim officials, Iraqi Shia and Kurdish political and religious figures, Shia civilians, foreign civilian contractors, humanitarian workers, and when necessary, Sunni Muslims.

3 In what would become a trademark tactic, they also started beheading Iraqi and foreign hostages.

4 Stanford University, "Mapping Militant Organizations: The Islamic State," 23 October 2017, http://web.stanford.edu/group/mappingmilitants/cgi-bin/groups/view/1, accessed 20 May 2018. Abu Musab al-Zarqawi had run a paramilitary training camp in Afghanistan.

5 The Meir Aralt Intelligence and Terrorism Information Centre, *ISIS: Portrait of a Jihadi Terrorist Organization,* (Glilot: Israeli Intelligence & Heritage Commemoration Center, 26 November 2014), https://www.terrorism-info.org.il/en/20733/, accessed 10 May 2018. He had no hesitation at using the same tactics against Sunnis when they were perceived to be helping the enemy.

6 Ellen Knickmeyer and K.I. Ibrahim, "Bombing Shatters Mosque in Iraq," *The Washington Post,* February 23, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/02/22/AR2006022200454.html, accessed 12 March 2018. In an attempt to improve its image after the attack, Zarqawi joined the Majlis Shura al-Mujahidin (MSC) coalition. Unfortunately, the MSC was little more than a coordinating agency, and

although it did give the group a more Iraqi flavour, it had little or no control over what the AQI actually did.

7 Bill Roggio, "Al Qaeda's Grand Coalition in Anbar," *Long War Journal*, 12 October 2006, https://www.longwarjournal.org/archives/2006/10/alqaedas_grand_coali.php, accessed 11 May 2018. On 12 October 2006, MSC united with three smaller groups and six Sunni tribes to form the Mutayibeen Coalition, pledging "To rid Sunnis from the oppression of the rejectionists (Shi'ite Muslims) and the crusader occupiers … to restore rights even at the price of our own lives … to make Allah's word supreme in the world, and to restore the glory of Islam." In October of that year, the MCS declared the establishment of the Islamic State of Iraq (ISI).

8 Joe Klein, "Is al-Qaeda on the Run in Iraq?" *Time Magazine Online*, 23 May 2007, https://web.archive.org/web/20070706191851/http://www.time.com/time/nation/article/0%2C8599%2C1624697%2C00.html, accessed 12 April 2018.

9 Cameron Glenn, "Timeline: the Rise, Spread and Fall of the Islamic State," *Wilson Center online*, 5 July 2016, https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state, accessed 17 April 2018.

10 Ibid.

11 Audrey Kurth Cronin, "ISIS Is Not a Terrorist Group Why Counterterrorism Won't Stop the Latest Jihadist Threat," *Foreign Affairs* (March/April 2015 issue), https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group, accessed 17 May 2018. The group also refocused its efforts on exploiting the country's sectarian strife, which continue to intensify after U.S. combat forces withdrew.

12 Isabel Coles and Ned Parker, "How Saddam's men help Islamic State rule," *Reuters Investigates*, 11 December 2015, https://www.reuters.com/investigates/special-report/mideast-crisis-iraq-islamicstate/, accessed 17 April 2018.

13 Rania Abouzeid, "The Jihad Next Door," *Politico*, 23 June 2014, https://www.politico.com/magazine/story/2014/06/al-qaeda-iraq-syria-108214, accessed 17 April 2018.

14 Ibid.

15 Christoph Reuter, "The Terror Strategist: Secret Files Reveal the Structure of Islamic State," *Spiegel Online*, 18 April 2015, http://www.spiegel.de/international/world/islamic-state-files-show-structure-of-islamist-terror-group-a-1029274.html, accessed 9 April 2018.

16 Ibid. It also included any illegal activities local power brokers were into that could be used to blackmail them, should that become necessary.

17 Ibid.

18 Anne Speckhard and Ahmet S. Yayla, "The ISIS Emni: Origins and Inner Workings of ISIS's Intelligence Apparatus," *The Terrorism Research Initiative (TRI), Perspectives on Terrorism*, Vol. 11, No. 1 (2017), http://www.terrorismanalysts.com/pt/index.php/pot/article/view/573/html, accessed 23 April 2018.

19 Reuter, "The Terror Strategist."

20 Ibid. Reuter also notes that during the infiltration, control, and consolidation phase of their operations ISI fighters would remain inconspicuous, being used for specific activities only when they were needed. Crucial to the success of these operations was the making of temporary alliances with key power brokers and rebel militias in the region. This tactic allowed the group to isolate and in turn eventually push out or destroy each of the rebel brigades in turn.

21 Speckhard and Yayla, "The ISIS Emni."

22 Rikar Hussein, "Why Islamic State Chose Raqqa as Its Syrian Capital," *VOA News*, 14 June 2017, https://www.voanews.com/a/islamic-state-raqqa-de-facto-capital/3900333.html, accessed 23 April 2018.

23 Ibid.

24 ISIL is the more correct form, but Western convention has predominantly used ISIS since 2012, when the group became active in Syria.

25 Abouzeid, "The Jihad Next Door."

26 Reuter, "The Terror Strategist."

27 Ibid.

28 Ibid. The big advantage of using foreign fighters was that they had no "knowledge of the societal terrain in which they operated and therefore had little reason to show mercy to the locals."

29 Ibid.

30 Ibid.

31 Cronin, "ISIS Is Not a Terrorist Group."

32 Jessica D. Lewis, "ISIS Battle Plan for Baghdad," *Institute for the Study of War*, June 2014, 1, http://www.understandingwar.org/sites/default/files/ISIS-not-culminated.pdf, accessed 27 April 2018.

33 Ibid., 1.

34 Sam Wyer, "The Islamic State of Iraq and the 'Destroying the Walls' Campaign," *Institute for the Study of War*, 21 September 2012, http://www.understandingwar.org/backgrounder/islamic-state-iraq-and-destroying-walls-campaign, accessed 2 February 2018.

35 Joel Wing, "Iraq's Security Forces Collapse as the Islamic State Takes Control of Most of Anbar Province," *Musings on Iraq*, 6 October 2014, http://musingsoniraq.blogspot.ca/2014/10/iraqs-security-forces-collapse-as.html, accessed 7 February 2018.

36 Wyer, "The Islamic State of Iraq." ISIL had been able to regain its strength largely because it had a secure base and recruiting centre in its safe-haven in Syria. However, it was also able to replenish its ranks with veteran manpower through prison breaks.

37 Ibid.

38 Ibid.

39 Ibid.

40 "Who are the Kurds?" *BBC Middle East Division*, 31 October 2017, http://www.bbc.com/news/world-middle-east-29702440, accessed 12 February 2018. Al-Baghdadi announced the merger of ISI with the al-Nusra Front and the renaming of the group to the Islamic State of Iraq and the Levant (ISIL). However, both the leaders of al-Nusra and al-Qaeda rejected the merger. After an eight-month power struggle, al-Qaeda cut all ties with ISIL on 3 February 2014, citing its failure to consult and "notorious intransigence."

41 Ibid.

42 Michael Knights, "The ISIL's Stand in the Ramadi-Fallujah Corridor," *Combating Terrorism Center Sentinel*, Vol. 7, Issue 5 (May 2014), https://ctc.usma.edu/the-isils-stand-in-the-ramadi-falluja-corridor/, accessed 10 February 2018.

43 "Iraq's Fallujah falls to 'Qaeda-linked' militants," *Daily Star, Middle East Section*, 4 January 2014, http://www.dailystar.com.lb/News/Middle-East/2014/Jan-04/243100-fallujah-outside-iraq-government-control-security-official.ashx, accessed 11 February 2018.

44 Ahmed Habshi, "Inside ISIS' battle strategy, use of Special Forces," *Ynet News.com*, 7 August 2015, http://www.ynetnews.com/articles/0,7340,L-4677761,00.html, accessed 7 February 2018.

45 The Meir Aralt, *ISIS: Portrait of a Jihadi Terrorist Organization*, 58.

46 "Sunni rebels declare new 'Islamic caliphate." *Al Jazeera, Middle East*, 30 June 2014, http://www.aljazeera.com/news/middleeast/2014/06/isil-declares-new-islamic-caliphate-201462917326669749.html, accessed 15 February 2018. The group also declared Abu Bakr al-Baghdadi as the Caliph and leader of all Muslims.

47 Evan Centanni, "War in Iraq: Map of Islamic State Control in May 2015," *Political Geography Now*, 22 May 2015, http://www.polgeonow.com/2015/05/war-in-iraq-map-of-islamic-state.html, accessed 7 February 2018.

48 Liz Sly and Ahmed Ramadan, "Insurgents seize Iraqi city of Mosul as security forces flee," *Washington Post*, 10 June 2014, https://www.washingtonpost.com/world/insurgents-seize-iraqi-city-of-mosul-as-troops-flee/2014/06/10/21061e87-8fcd-4ed3-bc94-0e309af0a674_story.html?utm_term=.5933e39cb0df, accessed 11 February 2018.

49 The Meir Aralt, *ISIS: Portrait of a Jihadi Terrorist Organization*, 62.

50 Wing, "Iraq's Security Forces."

51 Lewis, "ISIS Battle Plan for Baghdad."

52 The Meir Aralt, *ISIS: Portrait of a Jihadi Terrorist Organization*, 67. The report also states, "preventing supplies from reaching the local population and military reinforcements stationed in the city, damaging the infrastructure (by blowing up bridges,

for example), firing rockets and mortar shells at the city and its suburbs, and detonating car bombs inside the city (a modus operandi at which ISIS has shown itself skilled)."

53 Lewis, "ISIS Battle Plan for Baghdad."

54 The YPG and the Kurdistan Workers' Party (PKK) who have fought for Kurdish autonomy in Turkey for three decades and have bases in Iraq, also came to their aid.

55 Ibid.

56 Seth G. Jones, James Dobbins, Daniel Byman, Christopher S. Chivvis, Ben Connable, Jeffrey Martini, Eric Robinson, and Nathan Chandler, *Rolling Back the Islamic State* (Santa Monica, CA: RAND, 2017), xi, https://www.rand.org/pubs/research_reports/RR1912.html, accessed 9 February 2018.

57 Mara Revkin and William McCants, "Experts weigh in: Is ISIS good at governing?" *Markaz, Bookings Education*, 20 November 2015, https://www.brookings.edu/blog/markaz/2015/11/20/experts-weigh-in-is-isis-good-at-governing/, accessed 9 March 2018.

58 Thanassis Cambanis and Rebecca Collard, "How ISIS Runs a City," *Time Magazine Online*, 26 February 2015, http://time.com/3720063/isis-government-raqqa-mosul/, accessed 11 February 2018.

59 Ibid.

60 Ibid.

61 Ibid.

62 Ibid.

63 The Meir Aralt, *ISIS: Portrait of a Jihadi Terrorist Organization*, 72. In some cases Islamic law was put into place gradually in an attempt to prevent excessive alienation.

64 Ibid., 5.

65 Reuter, "The Terror Strategist."

66 Ibid.

67 The Meir Aralt, *ISIS: Portrait of a Jihadi Terrorist Organization*, 5.

68 Metin Gurcan, "ISIS Military Strategy," Presentation uploaded to www.academia.edu, 7, http://www.academia.edu/7632564/ISIS_MILITARY_STRATEGY, accessed 15 February 2018.

69 Profits fell in the wake of the aerial attacks carried out by the United States and its allies on its oil infrastructure.

70 The Meir Aralt, *ISIS: Portrait of a Jihadi Terrorist Organization*, 5.

71 Gurcan., "ISIS Military Strategy," 1.

72 Ibid., 2.

73 Lewis, "ISIS Battle Plan for Baghdad."

74 Gurcan., "ISIS Military Strategy," 3.

75 Ibid., 7.

76 Habshi, "Inside ISIS' battle strategy, use of Special Forces."

77 Ibid.

78 Petri Mäkelä, "Tactical Lessons from Mosul—Infantry Skills Matter." *Medium*, 10 November 2016, https://medium.com/@pmakela1/tactical-lessons-from-mosul-infantry-skills-matter-da3ced9ab8d6, accessed 11 February 2018.

79 Reuter, "The Terror Strategist."

80 Gurcan, "ISIS Military Strategy," 6-7.

81 Mäkelä, "Tactical Lessons from Mosul—Infantry Skills Matter."

82 Ibid.

83 Ibid.

84 Ibid.

85 Bill Roggio, "US targets al Qaeda's al Furqan media wing in Iraq," *FDD's Long War Journal Online*, 28 October 2007, https://www.longwarjournal.org/archives/2007/10/us_targets_al_qaedas.php, accessed 21 June 2018.

86 Wikipedia, *Islamic State of Iraq and the Levant*, https://en.wikipedia.org/wiki/Islamic_State_of_Iraq_and_the_Levant#cite_ref-Jihadologymedia_191-0, accessed 21 June 2018.

87 Olivia Becker, "ISIS Has a Really Slick and Sophisticated Media Department," *Vice News*, 12 July 2014, https://news.vice.com/article/isis-has-a-really-slick-and-sophisticated-media-department, accessed 21 June 2018.

88 The Daily Telegraph, "Islamic State launches English-language radio bulletins," *World News London*, 7 April 2015, https://www.telegraph.co.uk/news/worldnews/islamic-state/11519977/Islamic-State-launches-English-language-radio-news-bulletins.html, accessed 21 June 2018.

CHAPTER 10

1 Sergey Maidukov, "The Crimea Crisis -- Cui Bono?" *American Thinker* (daily internet publication), 5 April 2014, http://www.americanthinker.com/articles/2014/04/the_crimea_criss__cui_bono.html, accessed 17 June 2015. Critical to their planning was the status of Crimea, which is of special strategic interest to the Kremlin. Not only does Crimea hold the Russian Black Sea fleet, the peninsula serves as an economic thoroughfare connecting the Caucasus region and the Caspian Sea to central and Eastern Europe by way of the Dnieper River. Additionally, it is believed that the Crimea may hold a significant number of natural resources. According to the *American Thinker*, "Within 200 nautical miles of the Crimean shoreline there are an estimated 45 trillion cubic meters of gas reserves." It goes on to say, "Hydrocarbons in the Black Sea shelf could yield as much as 1.5 billion cubic meters per year."

2 Bērziņš, *Russia's New Generation Warfare in Ukraine*, 1.

3 Analysis, *Putting Russia's Crimean Intervention in Context*, *Stratfor Global Intelligence*, 12 April 2014, https://www.stratfor.com/analysis/putting-russias-crimean-intervention-context, accessed 15 June 2015. Russia's successes in the Ukraine were the result of a number of factors, only one of which included the employment of "New Generation Warfare." At the time of the intervention there was an overall weakness in the Ukrainian economy, wide spread corruption, a lack of investment in its military capabilities, and a fragile interim government in the capital. To this were added a number of advantages for Moscow, hich including the presence of Russian forces in Crimea, the high readiness of Russian military forces in southern Russia due to the Sochi Winter Olympic Games, and extensive use of the large pro-Russian speaking local population, particularly in Crimea and the East. In addition to exploiting these various weakness and strengths, the Russians also displayed an innovative use of a modern doctrine, employing a wide range of state tools, along with the ability to coordinate those tools in a complex multi-dimensional operation.

4 Bridget Kendall, "New head of Ukraine's navy defects in Crimea," *BBC News World*, 2 March 2014, http://www.bbc.com/news/world-europe-26410431, accessed 24 March 2015.

5 Marie-Louise Gumuchian, Laura Smith-Spark and Ingrid Formanek," *CNN*, 27 February 2014, http://www.cnn.com/2014/02/27/world/europe/ukraine-politics/, accessed 3 May 2015.

6 "Ukraine 'preparing withdrawal of troops from Crimea'," *BBC News*, 19 March 2014, http://www.bbc.com/news/world-europe-26656617, accessed 20 March 2014.

7 Oleksiy Matsuka, Vitaliy Sizov, "Russia's deep ties to Donetsk's Kremlin collaborators," *Kyivpost*, 10 April 2014, http://www.kyivpost.com/content/ukraine/russias-deep-ties-to-donetsks-kremlin-collaborators-342833.html, accessed 20 April 2015.

8 Ibid. In Russia and among pro-Russian activists in Ukraine, these events were called the Russian Spring.

9 Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows* (Blog), https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/, accessed 20 June 2015.

10 Ibid.

11 Kristin Ven Bruusgaard, "Crimea and Russia's Strategic Overhaul," *Parameters,* Vol. 44, No. 3 (2014): 81, http://www.strategicstudiesinstitute.army.mil/pubs/parameters/issues/Autumn_2014/11_BruusgaardKristin_Crimea%20and%20Russia's%20Strategic%20Overhaul.pdf, accessed 15 June 2015.

12 Imants Viesturs Liegis, "What does Hybrid Warfare mean to Europe? Three Experts Weigh in," http://www.europeanleadershipnetwork.org/what-does-hybrid-warfare-mean-to-europe-four-experts-weigh-in_2034.html, accessed 15 June 2015.

CHAPTER 11

1 Arthur F. Lykke, "Toward an Understanding of Military Strategy" in Joseph R. Cerami and James F. Holcomb, eds., *U.S. Army War College Guide to Strategy* (Carlisle, PA: U.S. Army War College, 2001), 117, http://www.au.af.mil/au/awc/awcgate/ssi/00354.pdf, accessed 20 June 2015. Specifically, nations should look into the possibility of conducting an analysis on how state-level hybrid warfare defence and how it should be designed and adapted to meet its specific national security and defence needs. A review of training is also required to produce better strategic thinkers. Finally, study is needed to identify what bureaucratic changes could be made to improve a country's strategic processing abilities along with how to make more efficient use of existing policy tools to counter specific threats from this form of warfare.

2 Linda Robinson, Paul D. Miller, John Gordon IV, Jeffrey Decker, Michael Schwille, Raphael S. Cohen, *Improving Strategic Competence Lessons from 13 Years of War*, (Santa Monica, CA: RAND Corporation, 2014), Summary xi, http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR816/RAND_RR816.pdf, accessed 10 June 2015.

3 Ibid., xi. The recommendation explains the decision to go to war in Iraq, the decisions to send a surge of troops to Iraq and then Afghanistan to bolster faltering war efforts, and the approach taken toward countering terrorism in the past two administrations all illustrate strategy deficits.

4 Ibid., 36.

5 The Economist, "George Kennan's cold war policy of containment: A conversation with Kennan's biographer John Lewis Gaddis," *Economist*, 28 November 2011, http://www.economist.com/Blogs/Prospero/2011/11/Quick-Study-George-Kennan%E2%80%99s-Cold-War-Policy-Containment, accessed 23 June 2015.

6 George Kennan, "Policy Planning Memorandum," 4 May 1948, National Archives and Records Administration, RG 273, Records of the National Security Council, NSC 10/2, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.html, accessed 23 June 2015.

7 United States Army Special Operations Command, SOF *Support to Political Warfare White Paper (Final)*, 10 March 2015), 127, http://www.soc.mil/swcs/ProjectGray/Support%20to%20Political%20Warfare%20White%20Paper%20v2.3-RMT%20(10MAR2015)%20%20%20.pdf, accessed 10 January 2018.

8 Ibid., 10.

9 Ibid., 11.

10 Ibid., 2.

11 Dan Madden, Dick Hoffmann, Michael Johnson, Fred T. Krawchuk, John E. Peters, Linda Robinson and Abby Doll, *Special Warfare: The Missing Middle in U.S. Coercive Options*, (Santa Monica, CA: RAND Corporation, 2014), 2, https://www.rand.org/content/dam/rand/pubs/research_rports/RR800/RR828/RAND_RR828.pdf, accessed 23 June 2015.

12 Ibid., 2.

13 Linda Robinson, Paul D. Miller, John Gordon IV, Jeffrey Decker, Michael Schwille, and Raphael S. Cohen, *Improving Strategic Competence: Lessons from 13 Years of War* (Santa Monica, CA: RAND, 2014), 98.

14 Department of Defense, *Military and Security Developments Involving the People's Republic of China for 2011,* (Washington D.C.: Government Publications, 2011), 26, https://www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf, accessed 23 June 2015.

15 Department of Defense, *Military and Security Developments Involving the People's Republic of China for 2014,* (Washington D.C.: Government Publications, 2014), 27, https://www.defense.gov/pubs/2014_DoD_China_Report.pdf, accessed, 23 June 2015. "Key systems that either have been deployed or are in development include ballistic missiles (including anti-ship variants), anti-ship and land-attack cruise missiles, nuclear submarines, modern surface ships, and an aircraft carrier."

16 Andrew Scobell, *Introduction to review essays on 'unrestricted warfare'* (Carlisle, PA: Strategic Studies Institute, US Army War College, 2007), 4, https://www.tandfonline.com/doi/pdf/10.1080/09592310008423264, accessed 10 July 2015.

17 Ibid., 29. Hoffman stated that normally these units would be used to prolong the conflict, provoke overreactions, or siphon off resources from the enemy.

18 Ibid., 1-2.

19 Ibid., 2.

20 For the purpose of this book, irregular forces are defined as militia, light infantry, and indigenous forces. Employment of light conventional forces could occur at the tactical level when indigenous forces are not available or have not been developed to the point where they can carry out operations. Conventional units are defined as medium or heavy units conducting manoeuvre warfare.

21 Thomas M. Huber, ed., *Compound Warfare That Fatal Knot,* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2002), 2-7.

22 Ibid., 3-7.

23 Huber does qualify this by stating, "Although the model of compound warfare offered here has been kept simple in hopes that it will serve as a convenient framework for analysis, readers should remember that enormous variety exists in the historical cases of compound warfare. As in most other realms of military thought, the theory is simple but the reality is complex. The Compound Warfare (CW) model assumes that one side in a CW conflict uses CW methods and the other does not. In reality, both sides may use CW methods. In most historical cases of compound warfare, one side uses CW methods predominantly; the other side deliberately uses them to the extent it is able. The model assumes two kinds of force, regular or conventional force, and irregular or guerrilla force. Several types of mobile regional militias may fall between these two poles and may contribute importantly to the leverage of the CW operator. In other words, various intermediate types of force are possible between the regular and irregular models promulgated here for simplicity." See Huber, *Compound Warfare That Fatal Knot,* 2-5.

24 See Gérard Chaliand. *Guerrilla Strategies. A Historical Anthology from the Long March to Afghanistan,* (Berkeley: University of California Press, 1982), 1-32.

25 Huber, *Compound Warfare That Fatal Knot,* 312. Huber makes it clear that "Accordingly, an important feature of the analytical framework of compound war is that although it informs and illuminates, this volume makes no claim that it is a quantitative or predictive model—at least not in terms of the scientific experimental method. Despite its utility in defining a historically significant pattern of warfare, it does not function well as a rigid template. Rather, it must be understood as a flexible framework that comfortably incorporates innumerable additional variables such as geography, social forces, culture, intensity of motivation, and the role of personalities which shape both the course and outcomes of events." Ibid., 308.

26 Colonel Bernd Horn, ed., *Forging a Nation: Perspectives on the Canadian Military Experience* (St. Catharines, Vanwall Publishing Limited, 2002), 46-47.

27 Michael D. Pearlman, "*The Wars of Colonial North America,1690-1763,*" in Huber, *Compound Warfare That Fatal Knot*, 39-40.

28 Huber, *Compound Warfare That Fatal Knot,* 92.

29 Cited in Ibid., 92. He does acknowledge that "Analysts calculate membership in Spanish guerrilla bands to have been about 50,000. Even if these are added to Wellington's conventional force, the French still enjoyed a favorable force ratio of almost 2.2 to 1." See also David G. Chandler, "Wellington in the Peninsula," 155-165, in David G. Chandler, *On the Napoleonic Wars* (London: Greenhill, 1994), 155-174.

30 From a historical perspective, compound war has often been used by weaker forces to provide them with an advantage over larger and stronger armies. This is a fact should be of interest to modern Western forces that are reducing their overall numbers to substitute technology for "boots on the ground."

31 Max Boot, senior fellow in national security studies with the Council of Foreign Relations "Statement to The House Armed Services Subcommittee on Terrorism, Unconventional Threats, and Capabilities," 29 June 2006. He goes on to state that "there is widespread concern within Army SF circles that their "softer," but no less vital, missions are being shortchanged by SOCOM in favor of sexier SWAT-style raids. One recently retired SF colonel wrote to me [Boot] a few weeks ago: "The current problem with SOCOM is that it is unbalanced. Most of the leadership and planning staff have come from the DA [Direct Action] side. They have no understanding of UW. To the degree that they are starting to develop an appreciation for it, it is only as an enabler for DA operations. In other words, they want to cherry pick techniques developed to wage unconventional war and use them to support conventional commando operations."

32 Ibid., 4-5.

33 Department of Defense (DoD), *Doctrine for Joint Special Operations Joint Publication 3-0517* (Washington D.C.: DoD, December 2003), 2-7.

34 Roy Maclaren. *Canadians Behind Enemy Lines: 1939-1945*, (Vancouver: University of British Columbia Press, 2004), 1-2. The SOE was established by the British War Cabinet

on 22 July 1940, and among other things, its purpose was to "to co-ordinate all action, by way of subversion and sabotage, against the enemy overseas." The mandate did not specifically state UW. See also Colonel (retired) Bernd Horn, *Now Set Europe Aflame* (Kingston: ERC Press, 2019).

35 Denis Rigden. *How To Be a Spy: The World War II SOE Training Manual* (Toronto: The Dundurn Group, 2004), 1-3.

36 Ibid., xv.

37 Ibid., 58.

38 Ian Southerland, "The OSS Operations Groups: Origin of Army Special Forces," *Special Warfare Magazine*, Vol. 15, No. 2 (June 2002): 10.

39 By the end of the war, the SOF's ability to carry out long-range independent operations had become one of their defining characteristics. This was due in large part to their move away from the short duration DA missions, which had been prevalent during the early stages of the war, to the more highly specialized tasks like UW that often required a long-term commitment in order to be successful. In the end, the excessive casualty producing DA missions were left to highly trained conventional forces, but remained a capability that all SOF units were expected to carry out when and if necessary.

40 Department of Defense, *History of the 10th Special Forces Group (Airborne)*, 1, http://www.soc.mil/SF/history.pdf, accessed 10 January 2003.

41 Sam Young, "A Short History of SF assessment and Selection," *Special Warfare Magazine* (May 1996): 23.

42 Southerland, "The OSS Operations Groups," 10-11. "A field radio repairman was added to the FA Team organization because of the problems the OSS operational teams had experienced with their communications equipment in the field. The next echelon in the OG organization functioned in a similar manner to that envisioned for the FB Team, Special Forces Operational Detachment District B."

43 Robert M. Cassidy, "The Long Small War: Indigenous Forces for Counterinsurgency," *Parameters* (Summer 2006): 55-56.

44 Ibid., 55-56.

45 Ibid., 56.

46 Ibid., 58-59.

47 Ibid., 58-59.

48 Ibid., 59-60.

49 John T. Carney and Benjamin F. Schemmer, *No Room for Error: The Covert Operations of America's Special Tactics Units from Iran to Afghanistan* (New York: Presidio Press Book, 2002), 13.

50 As a result, the Finnish army is divided into four operational military provinces (Southern, Western, Eastern and Northern) which bear the command responsibility for

all brigade-level units and military districts. Subordinated to the military provinces, there are 19 military districts, which are responsible for carrying out training and activating of reservists and planning and executing territorial defence of their areas. Logistical requirements are provided by the Army's Materiel Command, which has one Logistics Regiment for each military province. Today, the Finnish Army is divided into six branches: the infantry (which includes armoured units), field artillery, anti-aircraft artillery, engineers, signals, and materiel troops.

51 Pekka Visuri, *Evolution of the Finnish Military Doctrine 1945-1985* (Helsinki: Finnish Defence Studies, War College, 1990), 89, https://core.ac.uk/download/pdf/39979659.pdf, accessed 23 February 2023.

52 Ibid., 68-71 and 95.

53 Ibid., 70-77.

54 Ibid., 70-77 and 90.

55 Ibid., 95.

56 Ibid., 87.

57 The program was initially called *Force Design* 2030 but renamed *Force Design*, removing the "2030."

58 Mark F. Cancian, "The Marine Corps' Radical Shift toward China," *Center for Strategic and International Studies*, 25 March 2020, https://www.csis.org/analysis/marine-corps-radical-shift-toward-china, accessed 3 October 2024.

59 U.S. Marine Corps (USMC), *A Concept for Stand-in Forces* (Quantico, VA, USMC, 2021), 4-5, https://www.hqmc.marines.mil/Portals/142Users/183/35/4535/21120_A%20Concept%20for%20Stand-In%20Forces.pdf, accessed 3 October 2024.

60 Tyler Rogoway, "HSV-2 Swift Destroyed Off Yemeni Coast by Anti-Ship Missile A horrific reminder of how anti-ship missiles are falling into the hands of non-state," *The Warzone*, 2 October 2016, https://www.twz.com/5404/hsv-2-swift-destroyed-off-yemeni-coast-by-anti-ship-missile, accessed 2 December 2024.

61 USMC, *A Concept for Stand-in Forces*, 4-5.

62 Ibid., 4-5.

63 Cancian, "The Marine Corps' Radical Shift toward China."

64 TRADOC Pamphlet 525-5, 3-5.

65 USMC, *A Concept for Distributed Operations*, 1-2.

66 Ibid., 2-4.

67 USMC, *A Concept for Stand-in Forces*, 4-5.

68 Ibid., 17.

69 Cancian, "The Marine Corps' Radical Shift toward China."

70 General David H. Berger, "Notes on Designing the Marine Corps of the Future," *War On The Rocks,* 5 December 2019, https://warontherocks.com/2019/12/notes-on-designing-the-marine-corps-of-the-future/.

ABOUT THE AUTHOR

Tony Balasevicius is a retired infantry officer. During his career, he has served with the Canadian Airborne Regiment and with Joint Task Force Two (JTF 2). He has worked in the Department of Applied Military Science at the Royal Military College of Canada (RMC) and as an analyst with the Directorate Future Security Analysis (Chief force Development). He was Team Leader at the Canadian Forces Warfare Centre (CFWC) Concepts Group, and worked at Chief Defence Intelligence and the Canadian Forces Land Warfare Centre. Between 2015-2016, Tony was the Canadian representative on the Multinational Capability Development Campaign (MCDC) that produced the Analytical Framework for Countering Hybrid Warfare (CHW). Tony has a Master's degree in War Studies from RMC. He has completed the Land Force Technical Staff Programme and Canadian Forces Staff College. He is currently doing contract work. His current field of research is focused on Russian military modernization, Hybrid Warfare, the future of SOF, and non-state actors.

CANSOFCOM EDUCATION & RESEARCH CENTRE (ERC) PUBLICATIONS

Special Operations Forces: A National Capability
Dr. Emily Spencer, ed., 2011.

Special Operations Forces: Building Global Partnerships
Dr. Emily Spencer, ed., 2012.

"By, With, Through." A SOF Global Engagement Strategy
Dr. Emily Spencer, ed., 2014.

In Pursuit of Excellence. SOF Leadership in the Contemporary Operating Environment
Dr. Emily Spencer, ed., 2017.

The Birth of the Ranger Tradition. Irregular Warfare During the Lake Champlain Theatre of Operations, 1754-1760. A Battlefield Study Guide
Colonel (retired) Bernd Horn, PhD, 2017.

Thinking for Impact: A Practical Guide for Special Operations Forces
Dr. Emily Spencer, 2018.

"We Will Find A Way." The Canadian Special Operations Legacy
Colonel (retired) Horn, PhD, 2018.

Now Set Europe Aflame! The SOE and the Canadian Connection
Colonel (retired) Bernd Horn, PhD, 2019.

Risk & Decision-Making
Colonel (retired) Bernd Horn, PhD, ed., 2019.

Risk: SOF Case Studies
Colonel (retired) Bernd Horn, PhD, ed., 2020.

The (In)Visible Hand: Strategic Sabotage Case Studies
Colonel (retired) Bernd Horn, Dr. James Kiras and Dr. Emily Spencer, eds., 2021.

Strategic Competition: Implications for SOF
Colonel (retired) Bernd Horn, PhD, 2022.

A Perilous Future: High Intensity Conflict and the Implications for SOF
Lieutenant-Colonel Andrew L. Brown, PhD, ed., 2022.

Operating on the Margins: SOF in the Gray Zone
Dr. Howard G. Coombs with Dr. Christopher Marsh, eds., 2023.

Force Multiplier: Utilization of SOF from a Small State Perspective
Colonel (retired) Bernd Horn, PhD and Colonel (retired) Hans Ilis-Alm. eds., 2024.

Threat & SOF | Special Operations Response
Colonel (retired) Bernd Horn, PhD and Dr. Patricia J. Blocksome, eds., 2024.

The Northern Flank. The Arctic: Implications for SOF
Bernd Horn, Howard G. Coombs and Tony Balasevicius, eds., 2025.


VIAM INVENIEMUS