Strategic Competition: Implications for SOF

Colonel (Retired) Bernd Horn

Strategic Competition: Implications for SOF

STRATEGIC COMPETITION: IMPLICATIONS FOR SOF

Colonel (Retired) Bernd Horn, PhD

Canadian Special Operations Forces Command
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

Produced for CANSOFCOM Education & Research Centre
by 17 Wing Winnipeg Publishing Office.
WPO32201

Cover and interior artwork: Silvia Pecota
Interior Photos: CANSOFCOM

ISBN 978-0-660-45014-8 (print)
ISBN 978-0-660-45013-1 (PDF)

Government of Canada Catalogue Number D2-628/2022E (print)
Government of Canada Catalogue Number D2-628/2022E (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

ACKNOWLEDGEMENT

Initially, I wish to thank Dr. Emily Spencer for her assistance in research and editing in the completion of this publication.

I would also like to thank Silvia Pecota for her marvellous artwork on the cover and inside the book.

Last, but certainly not least, I must thank Evelyn Nymoen and Adrienne Popke of 17 Wing Publishing Office for their continuing outstanding support to CANSOFCOM ERC publications by creating the polished end products.


N
W
E
S

INTRODUCTION

Great Power Competition (GPC), also referred to as strategic competition, has seemingly taken centre stage. However, it is not new. Nations have always competed for influence and access to allies, partners, resources, colonies, etc., in their quest to attain political, military, economic and geographic advantage.[1] The Cold War (1948-1990) witnessed this competition in a very bipolar lens between the two superpowers, the United States and their allies against the Soviet Union and their alliance bloc. Throughout this period both sides were enmeshed in an ideological, political, as well military competition for ascendency.

With the fall of the Berlin Wall in November 1989, the subsequent disbandment of the Warsaw Pact and the collapse of the Soviet Union in 1991, the United States emerged as the single global Superpower.[2] As such, the U.S. and the North Atlantic Treaty Organization (NATO) were now in a position to more freely act unilaterally on the world stage. In the wake of the 11 September 2001 (9/11) terrorist attack on the twin towers of the World Trade Center in New York, the U.S. and its alliance partners became embroiled in, and focused on, the "War on Terror." Counter-terrorism (CT) and counter-insurgency (COIN), particularly in Afghanistan and Iraq, consumed political and military resources and focus.[3]

Although Russia was still in the throes of domestic reconstruction and China was still in its early-emergent phase, and even though neither could challenge the military or political strength of the U.S. and its allies in the same capacity as during the Cold War, they continued to "compete" in accordance with their capabilities during this period. They had never stopped attempting to ameliorate their position in the GPC. Espionage, support of proxy forces (particularly those engaged in conflict with the U.S. and their coalition partners), propaganda, disinformation, economic strategies, criminality, to name only a few lines of operation, were conducted to achieve national objectives. Although the U.S.-led international order may have lost sight of the GPC due to its dominant position at the time, it had never stopped. As former Chairman of the Joint Chiefs of Staff, General Joseph Dunford offered, "We think of being at peace or war.... Our adversaries don't think that way."[4] Dunford was right. For the Russians and the Chinese, they believe they were / are in a constant state of conflict with the West. As strategic advisor, author

and former military officer David Kilcullen observed, our adversary(ies) "may be acting in ways it considers warlike, while we with our narrower notion of warfare remain blithely unaware of the fact, so that by the time we realize we are at war, we have already lost."[5]

By 2014, Russian and Chinese actions (e.g., seizure of Crimea and the militarization of the Spratly Islands and coral reefs respectively) signaled a resurgent Russia and an emergent China had altered the geo-political landscape dramatically, requiring a reassessment of the U.S. strategic vision. This reevaluation led to a pivot in American focus (and subsequent NATO attention) and ushered in a "renewed" GPC.

The revision of Western strategic priorities and the renewed GPC, although in many ways similar to the Cold War, conducted in a much more ambiguous, complex and challenging security environment. The competition space is now far more exigent due to advances in computing and information technologies, as well as the proliferation of accessible advanced technology to all state and non-state actors. As such, the renewed GPC, although not a new phenomenon, is far more demanding than in previous eras. This reality means that there are also significant implications for Special Operations Forces (SOF).

CHAPTER 1

The Pivot

The renewal of Great Power Competition made widescale news in 2018, however, it was actually already acknowledged by President Barack Obama Administration's June 2015 National Military Strategy. Subsequently it became a centrepiece of the President Donald Trump Administration's December 2017 National Security Strategy (NSS) and in the January 2018 National Defense Strategy (NDS).[1]

Undoubtedly, the 2018 NDS was abundantly clear on the "pivot," or in other words, the transition from Department of Defense's (DoD) primary focus on counter-terrorism and the "global war on terror" to a shift of emphasis on Great Power Competition with its "peer and near-peer" rivals (i.e., China, Russia) and international rogue states / competitors (e.g., Iran, Republic of North Korea).[2] The 2018 NDS clearly states that DoD's "enduring mission is to provide combat-credible military forces needed to deter war and protect the security of our nation." As such, DoD "provides military options to ensure the President and our diplomats negotiate from a position of strength." Significantly, the strategy document also notes:

> Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.[3]

The document plainly labels Russia and China as revisionist powers who are set on remodeling the international system and, as such, pose "the central challenge to U.S. prosperity and security." The conclusion drawn is resoundingly clear, namely a return of the big power rivalry reminiscent of the Cold War, but now in an increasingly multipolar world. From the perspective of

the 2018 NDS this evolution has become the defining element of the international environment.

Another DoD strategy document echoed, "Our national focus on defeating Violent Extremist Organizations (VEO) over the last two decades allowed our strategic competitors to close the gap with our Nation's military capabilities. As rogue regimes and VEOs continue to destabilize regions and near-peer opponents increasingly undermine long-established international order, our national leaders have shifted their primary national security efforts back to interstate strategic competition, while balancing continued Counter-VEO requirements."[4]

The 2018 NDS clearly underscores that for the first time in a generation that the strategic focus of American defense policy is to compete with near power rivals in a multi-polar world. This shift would seem to indicate that the period of unrivaled American power that emerged following the collapse of the Soviet Union in 1991 has come to an end. As a result, the former American Defense Secretary, Mark Esper, revealed, "We are focused on great power competition, first with China, then Russia." Esper conceded, "My aim is to adjust our [military] footprint in many places."[5]

The change in American presidential administrations has not changed the American outlook. President Joe Biden Administration's *Interim National Security Strategic Guidance*, in consonance with Secretary of Defense (SecDef) Lloyd Austin's recent *Letter to the Force* (SecDef21), reinforces the focus on strategic competition with China as a top priority.[6] Moreover, on 28 March 2022, the Biden administration delivered the classified version of the 2022 NDS to Congress. The strategy, requiring a $773 billion budget, outlined four strategic priorities: pacing defense capabilities to the "growing multi-domain threat" posed by China, deterring "strategic attacks" against the U.S. and its allies, deterring aggression from China and Russia, and building a resilient "Joint Force" and defense ecosystem.[7] Additionally, SecDef Austin issued an internal directive to "laser focus" American military "efforts to address China as the nation's number one pacing challenge."[8]

Inevitably, the American pivot has led to a similar focus for its alliance partners. A NATO working group declared, "The main characteristic of the current security environment is the re-emergence of geopolitical competition."[9] Not surprisingly, Canada too, has pivoted to focusing on the renewed GPC.

Arguably, the 2018 NDS is exactly what the three traditional Services (i.e., Navy, Army, Air Force) have waited for since the demise of the Warsaw Pact and the fall of the Soviet Union, namely the peril of high-end state threats that allow the Conventional Services to focus their efforts on capability development, deployment and funding.[10] Predictably, this focus is more centred on traditional capabilities and threat scenarios than it is on the issue of "competition." Culture and deep-rooted perspectives based on Service affiliation, training and experience are difficult to change.

What Is The "Competition" Battlespace?

The "pivot" is unsurprising in its own right; however, the challenge comes in correctly identifying the battlespace and the threats within. As Dr. Daniel Nexon observed, "Competition isn't a strategic goal. It's a means to an end. The decision to compete with another great power should always be over something specific; it should center on the efficacy of competition, the value of the object at stake, and how the specific objective contributes to long-term goals."[11] As such, framing a national policy around great power competition obscures the reality that most, if not all countries (including the U.S. and China), share extensive interests (e.g., economic, global issues such as climate change, counter-terrorism, nuclear non-proliferation, pandemic prevention). Competition is not simply a military problem.

However, for too many conventional military commanders and some politicians the renewed GPC is seen as a return to "high-intensity" combat harkening back to the Cold War stand-off between super-powers.[12] Danish General Martin E. Dempsey acknowledged, "It's the first time in 41 years we've had a legitimate risk emanating from state actors, and we clearly have a persistent threat emanating from sub-state and non-state actors." He concluded, "That makes for a very volatile mix and makes it difficult for us to balance our resources to deal with these multiple threats simultaneously."[13]

The balancing of resources and identifying the "multiple threats" that exist is a formidable problem. Former Chairman of the Joint Chiefs of Staff (JCS), General Joseph Dunford, admitted, "We're already behind in adapting to the changed character of war today in so many ways." He argued that the U.S. national strategy with regards to GPC must recognize that the binary peace / war distinction is flawed. Rather, nations must understand conflict as a continuum, as a "range of different modes of conflict with increasing levels of violence, from measures short of armed conflict (Gray Zone) through

conventional warfare." He noted that by failing to fully understand the true breadth of our adversaries' stratagems and their strategic narratives, the Western alliance has ceded influence and access to China and the West's ability to compete with its adversaries' narratives. The result has been that both China and Russia have been able to commence dismantling, if not demolishing, the rules-based international order.[14]

This failure to understand the true nature of the strategic competition and the apparent willingness to return to a traditional warfare model mindset has clear dangers, as does ignoring the capability of current rivals and rogue states. "The biggest problem with DoD strategy development," Brigadier General Don Bolduc argued, "is that it is tied to an antiquated organizational structure." He insisted, "the department is in need of serious reorganization."[15] The Americans are not alone as most Western military institutions share the same experience.

It is this failure, if not unwillingness, to come to grips with the true nature of the GPC, or more accurately strategic competition, specifically, understanding the competition space and balancing resources correctly that disadvantages the West. Bolduc's concern is well-founded. Retired admiral and former NATO Supreme Allied Commander Admiral James Stavridis warned of an over-reliance on the military for the American approach to foreign policy. He reasoned, "diplomacy is preventive medicine that will help avoid costly surgical procedures (i.e., military operations) in the future."[16] This over-dependence on military solutions, or the use of force to achieve desired political outcomes, has left the U.S. and its alliance partners in a poor position to compete in the new "competition" battlespace. General Michael Mullen, a former chairman of the Joint Chiefs of Staff, lamented:

> My fear, quite frankly, is that we aren't moving fast enough in this regard. U.S. foreign policy is still too dominated by the military, too dependent upon the generals and admirals who lead our major overseas commands. It's one thing to be able and willing to serve as emergency responders; quite another to always have to be the fire chief.[17]

Mullen's concern was that political decision-makers were too quick and too dependent on the military to deal with an ever-increasing gamut of missions in a constantly evolving complex international forum. As a result, they are competing with a limited tool set, while their competitors utilize the entire array of national resources.

One area of concern is that DoD, much like its alliance partners, have employed an "artificial distinction between an environment of armed conflict and peace without significant military competition" since the end of the Cold War. Fortunately, some progress has been achieved. DoD has recently defined "the continuum of competition as cooperation, competition below the threshold of armed conflict."[18] Most recently, a report by the Joint Special Operations University (JSOU) defined the current level of competition as "the interaction among actors in pursuit of the influence, leverage, and advantage necessary to secure their respective interests."[19] To the U.S. Army, a competition period is described as:

> actions over time that exploit the operational environment conditions in order to gain a position of advantage below the threshold of armed conflict. At the crux of competition is the ability to create a strategic and operational standoff to gain freedom of action in any domain. This is done through the integration of political and economic actions, unconventional and information warfare, and the actual or threatened employment of conventional forces.[20]

DoD apparently has begun to establish a more robust framework for understanding and competing in the operational environment. Although the military is an essential component of the GPC, it is but a single actor in a nation's armoury. As the shadowy GPC competition has shown to date, it is not even the primary weapon.

Clearly, a sound understanding of what "great power competition" or "strategic competition" is, as well as what it looks like, is essential.[21] As a RAND report noted, "If the assertion that international politics is entering a new period of strategic competition has been widely accepted, there is no consensus about what this shift means." [22] For the previous two decades in the fight against terrorists and insurgents, the U.S. and its Western allies have been able to compensate for any lack of a strategic coherence in their approach to less capable opponents through technological and resource advantages. Against more formidable adversaries its technological and military capabilities may be equaled. What will be important is a change in strategic thinking that recognizes the exact nature of the current and future battlespace.[23]

In this light, the prognosis for a high-intensity, traditional war scenario is ominous, if not downright horrendous. Globalization, the proliferation of technology and its exponential, consistently increasing capability has made

a traditional war almost incomprehensible. An increasing number of nations with substantial nuclear arsenals, as well as the global propagation of stand-off precision missile systems and platforms, including highly manoeuvrable cruise missiles, as well as hypersonic weaponry (weapons that travel at five times the speed of sound) and glide vehicles, matched with networked sensors that are capable of delivering large payloads of munitions at increased ranges so that targets can be engaged and destroyed almost anywhere with accuracy within a short period of discovery and decision-making.[24] The use of Artificial Intelligence (AI), space based weapons, lasers, directed-energy munitions and high-powered microwaves will only increase lethality and reach.

In essence, the future battlefield will be characterized by increased lethality, enhanced speed and tempo of operations, amplified informatization empowered through AI, increased complexity, and the loss of traditional Western supremacy in all domains. Conflict between belligerents using modern weaponry will be disturbingly swift and horrifically destructive. In more than eight wargames set in the Indo-Pacific theatre, covering campaigns lasting from several days to several weeks, typical attrition exceeded the estimated combined U.S. and Japanese ship and aircraft losses from the Battle of the Coral Sea and the Battle of Midway, which were two of the costliest air and naval battles in World War II (WWII). The wargames also determined:

> The combat is also disorientingly chaotic, regardless of whether information and command systems worked (in which case, long-range precision fires resulted in catastrophic attrition and destruction) or not (in which case, both sides scrambled to understand what was happening, make decisions, and communicate these decisions across their forces). Second, the side that could rapidly impose chaos on its opponent while maintaining sufficient understanding and order to command its own forces gained an enormous advantage. This advantage accrued to the Chinese and Russian teams in nearly every scenario in which U.S. teams used current concepts. Most Chinese and Russian red teams had a relatively consistent "script" of attacks that they would use to systematically conduct ID/CD against U.S. forces. This script rapidly gave them an advantage in key aspects of the techno-cognitive confrontation, such as the ability to target ships at long range and coordinate attacks from multiple domains. Third, once gained (or lost), this advantage had cascading effects that put the weaker side—usually the U.S. team—into untenable dilemmas

> or, worse, seemingly unrecoverable positions. These games suggested that, without urgent changes to how the DoD is conceptualizing and engaging in techno-cognitive confrontation, U.S. forces face a real risk of losing their situational awareness, capacity to make decisions, ability to communicate reliably, and the initiative in plausible conflict scenarios. Once the fight for information and command is lost, U.S. forces may not be able to recover, and military defeat becomes likely.[25]

In another wargame that simulated an AI-enhanced ground fight where troops were outnumbered three to one by enemy forces, the addition "of autonomous air and ground sensors allowed troops to smartly detect, target, and engage adversaries (find, fix, finish), realizing an approximate 10–fold increase in combat power."[26] The Russian and Ukrainian experience in their 2022 conflict is yet another example of the lethality of modern arms and technology.

China's heavy investment in AI and "intelligent detection and identification" indicate that China intends to construct a connected network of persistent sensors, including meter-wave technology, for domain awareness and early warning.[27] Experts believe that a system of advanced sensors connected to air defense systems supported by advanced fighter aircraft would make penetrating Chinese-controlled airspace an incredibly difficult problem.[28]

Other wargames and simulations based on a Baltic scenario concluded that Russia could defeat and occupy the three Baltic states (i.e., Estonia, Latvia, Lithuania) in less than 60 hours and another wargame determined that Poland would fall in a conventional war with Russia in just five days. These assessments are now questionable considering the Russian difficulties and losses in its February 2022 invasion of the Ukraine. However, Russia's ability to learn and adjust from its Ukrainian experience should not be underestimated. Finally, simulations focused on conflict in the East China Sea region indicated analogous catastrophic results.[29]

The formidable capabilities of current and emerging technology and munitions makes the fielding of large conventional armies and their platforms laden with risk. Added to this daunting array of threats is a myriad of additional perils. Jamming of communications, electronic warfare and cyber-attacks that target networks and the vulnerable software programs that seemingly run the entirety of today's society and militaries will only increase risk and

consequence of a high-intensity war. The increasing development of autonomous systems only adds to this complexity.[30] In light of the lethality of the modern battlespace, as well as the substantive, imposing American and allied military capability, no nation would purposely attempt to compete with the U.S. and its allies in a traditional conventional war setting if at all avoidable. However, this situation is not to say American rivals and competitors will not wage a different form of conflict or competition.

Although competitors such as China and Russia maintain large military forces and continue to improve and expand their arsenals, arguably leading to a renewed arms race, they remain careful to avoid actions that would possibly activate the conventional war "trip wire."[31] Rather they maintain the military capability as a substantial, viable and overt threat, but compete on various levels under the threshold of a "hot" or "shooting war." They utilize "Hybrid Warfare," defined by NATO as "a wide range of overt and covert military, paramilitary, and civilian measures [...] employed in a highly integrated design."[32]

NATO political-military expert Chris Kremidas-Courtney described Hybrid Warfare as "the mix of conventional and unconventional, military and non-military, overt and covert actions employed in a coordinated manner to achieve specific objectives while remaining below the threshold of formally declared warfare."[33] A 2014, British Ministry of Defence report captured its essence more lucidly. It asserted:

> Our adversaries are unlikely to engage us on our terms and will not fight solely against our conventional strengths. They will seek an asymmetric advantage and some will employ a wide range of warfighting techniques, sometimes simultaneously in time, space and domain. Their logic will not necessarily be our logic and thus our ability to understand adversaries – and our ability to make them understand our intent – will be challenging…In some conflicts, we are likely to see concurrent inter-communal violence, terrorism, insurgency, pervasive criminality and widespread disorder. Tactics, techniques and technologies will continue to converge as adversaries rapidly adapt to seek advantage and influence, including through economic, financial, legal and diplomatic means. These forms of conflict are transcending our conventional understanding of what equates to irregular and regular military activity; the conflict paradigm has shifted and we must adapt our approaches if we are to succeed.[34]

The National Coordinator for Security and Counterterrorism (NCTV) of the Netherlands further refined the definition of Hybrid Warfare stating, "it is understood as conflict between states, largely below the legal threshold of an open armed conflict, with the integrated use of means and actors, aimed at achieving certain strategic goals." It characterizes this form of warfare by:

- The integrated deployment of multiple military and non-military means, such as diplomatic, economic and digital means, disinformation, influencing, military intimidation, etc., that belong to the toolbox of state instruments;
- Orchestration as part of a strategy/campaign;
- The intention of achieving certain strategic goals; and
- Important features, namely deception, ambiguity and deniability, which accompany the actions (or could do so), making it difficult to attribute them and respond to them effectively.[35]

Jānis Bērziņš, the director of the Center for Security and Strategic Research at the National Defense Academy of Latvia, explains the shift from "traditional" to "Hybrid Warfare" as the transition:

- from direct destruction to direct influence;
- from direct annihilation of the opponent to its inner decay;
- from a war with weapons and technology to a culture war;
- from a war with conventional forces to specially prepared forces and commercial irregular groupings;
- from the traditional battleground to information/psychological warfare and war of perceptions;
- from direct clash to contactless war;
- from a superficial and compartmented war to a total war, including the enemy's internal side and base;
- from war in the physical environment to a war in the human consciousness and in cyberspace;
- from symmetric to asymmetric warfare by a combination of political, economic, information, technological, and ecological campaigns; and
- from war in a defined period of time to a state of permanent war as the natural condition in national life.[36]

Importantly, the different interpretations of Hybrid Warfare, or how analysts see competition / conflict in the current security environment, puts the emphasis on non-military actions. It should be no surprise then that a recent study concluded that "in a future, large-scale conflict, Chinese forces will likely employ a modern and unique irregular warfare concept, focused on information and influence, tightly integrated with conventional capabilities. A return to great power competition does not portend a shift away from irregular warfare to conventional warfare, but rather an amalgamation of the two."[37] Quite simply, adversaries have discovered, and more importantly, will continue to refine and evolve, methods to achieve their political, economic and military objectives while remaining in "Phase 0", the American doctrinal period describing pre-conflict. The fact that the U.S. and its allies are extremely hesitant to go to war, further emboldens and provides adversaries with a competitive edge.[38]

In essence, the new competitive landscape, blends conventional, irregular, asymmetric, criminal and terrorist means and methods to achieve a political objective. This actuality makes the opponent largely irrelevant. Whether a state or non-state actor, adversaries will make use of the proliferation of technology and information that has accompanied globalization. Instruments such as cyber warfare, economic coercion or even blackmail, exploitation of social / societal conflict in a target country and the waging of disinformation campaigns and psychological warfare are all in the inventory. Criminal behaviour and terrorism are also in the repertoire of opponents.

General Valery Gerasimov, Chief of the General Staff of the Russian Federation, markedly identified the weakness of modern states. He insisted that history has shown that "a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war."[39] This state of affairs is due, in his estimation to the fact that "the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[40]

Similar to Gerasimov, General-Lieutenant, Adrei V. Kartapolov, in 2015, then chief of the Russian General Staff's Main Operational Directorate, published an article in the *Journal of the Academy of Military Science* that described the "new-type war." It clearly highlights the fact that the military was not seen

as the only actor in the renewed GPC. Kartapolov argued that the framework of conflict included:

- political, economic, informational, and psychological pressure;
- disorientation of the political and military leadership;
- spreading dissatisfaction among the population;
- support of internal opposition in other countries;
- preparing and deploying armed opposition;
- deployment of special forces;
- conduct of subversive acts; and
- employment of new weapon systems.[41]

Rather than a kinetic solution to conflict, Gerasimov and Kartapolov argue that the focused application of political, economic, informational, humanitarian, and other non-military measures, when applied in a coordinated manner with internal discontent and protest can wield significant results. In addition, all of these actions are also combined, at the right moment, normally to achieve final success, with concealed military action, often "under the guise of peacekeeping and crisis regulation." Gerasimov insisted, "Asymmetrical actions have come into widespread use, enabling the nullification of an enemy's advantages in armed conflict. Among such actions are the use of special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected."[42]

From a strategic perspective, the methodology of rivalry in the great power competition entails the mobilization of a wide range of a state's resources, primarily non-violent to achieve a desired political end-state. The use of violence is not remotely desired. A "Hybrid Warfare" approach is seen as a methodology of achieving the political end state without tripping the threshold of war, which would allow an opponent the recourse to legally use force and / or attract international intervention.[43] Hybrid Warfare creates a perfect ambiguity that paralyzes opponents since they are not even aware that they are under attack.

The case of the Russian annexation of the Crimea and the conflict in Ukraine in 2014 is a perfect example. Russia was able to skillfully manipulate the U.S. and its NATO allies to remain largely passive while Russia dismembered the

Ukraine.[44] It was so successful that the Supreme Allied Commander Europe (SACEUR) at the time, General Phillip Breedlove, proclaimed that Russia's use of Hybrid Warfare in Eastern Ukraine represented, "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[45]

Consequently, the challenge is recognizing that strategic competition / GPC, as well as dealing with rivals and rogue states, is on a completely different playing field. Although conventional military capability will always be required, as both a deterrent and back-stop to military aggression, the majority of the never-ending competition / conflict will be waged on economic, informational, political, societal and technological planes. Experts have argued that "China and Russia compete across five primary domains of competition: population / political warfare, economic statecraft, cyber operations, armed conflict and international institutions."[46]

General Stephen J. Townsend touched on the issue. He noted, "Competition is forever. It's endless. It's like mowing the grass. You don't just do it once." He explained "You want to achieve your strategic objectives. You want to thwart your adversaries' strategic objectives, and you want to avoid major war. So, you always want to be in a state of competition to avoid major war." He rhetorically queried, "What do we want? We want access and influence, right? And how do you get access and influence? Well, you can get that by helping your partner with a problem that they have."[47]

Underlying his point was the fact that to continually compete, you must compete on the same playing field as your opponents. That means, you must wage competition / conflict on the same domains / planes as your adversaries.

CHAPTER 2

China in the Competition Space

China is almost universally identified as the major competitor in the GPC. The Biden Administration explained that China "is the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system.[1] Experts believe that China "presents the greatest challenge to the United States and to Western-based international norms in large part because it does so on many fronts."[2] Director of National Intelligence Avril Haines called China an "unparalleled competitor" because of the wide range of ways it spreads its influence and undermines Western-based norms.[3]

China has clearly studied the Americans and their Western allies and shaped a strategy that has allowed it to increase its influence and prosperity. It has achieved this success through a deliberate focus on irregular activities that have allowed it to arguably surpass "the United States as the dominant global technological, military, and economic power."[4] It has created an incredibly sophisticated cyber capability (e.g., Unit 61398 of the People's Liberation Army (PLA)), extended its global reach and influence through its economic program and utilized its military and para-military capabilities to secure contested territory, utilized its political and economic clout to muzzle criticism of the regime and stolen sensitive technologies.[5]

To many analysts, China has mastered the GPC and as a result has made great strides in advancing their interests and confounding Western influence, access and dominance. They have achieved this by methodologies short of triggering a "hot war." Analysts from the PLA have argued that future wars will be the "three non-warfares: non-conflict, non-linear and non-symmetric" to attack its opponents' weaknesses.[6] In short, they have utilized multiple levers of national power and other means. Specifically:

Political Means

Many experts have asserted that China has adopted a "Wolf Warrior" diplomacy rather than one based on cooperation and friendship. The slightest criticism of China is met with aggressive condemnation. One report notes that "a combative attitude has seeped into every part of China's foreign policy, and it is confronting many countries with their gravest threat in generations. Beijing is churning out warships faster than any country has since WWII, and it has flooded Asian sea-lanes with Chinese coast guard and fishing vessels. It has strung military outposts across the South China Sea and dramatically increased its use of ship ramming and aerial interceptions to shove neighbors out of disputed areas. In the Taiwan Strait, Chinese military patrols, some involving a dozen warships and more than 50 combat aircraft, prowl the sea almost daily and simulate attacks on Taiwanese and U.S. targets."[7]

What is seen as a shift, however, is somewhat misguided. What the West tends to miss is that as far as China is concerned it is, and always has been, at "war" with the U.S. and its alliance. "The PRC [People's Republic of China]," one expert observed, "considers itself engaged in a political war with the United States and its partner nations and allies. Beijing perceives U.S. and Western diplomatic, economic, and military measures targeting China as a concerted Western effort to prevent China's rise, as well as to undermine the Chinese Communist Party's (CCP) rule.[8] Failure to understand their perception and the nature of this 'war' severely undermines the ability to conceptualize the threat and to implement appropriate countermeasures.[9] This failure ensures ultimate defeat."[10]

For China, political warfare includes using international and national laws, bodies and courts to influence and shape decision-making to obtain favourable outcomes, economic warfare, biological and chemical warfare, cyber-attacks, terrorism, public opinion / media warfare, psychological warfare, espionage, bribery, censorship, deception, subversion, blackmail, "enforced disappearances," street violence, assassination, use of proxy forces, public diplomacy, and Hybrid Warfare.[11] Quite simply, China views Gray Zone activities as a natural extension of how countries exercise power. These activities are methods to achieve China's political objectives, specifically to advance its domestic, economic, foreign policy, and security objectives—without triggering backlash or conflict. A RAND report concluded that over the past decade, "China employed nearly 80 different Gray Zone tactics across all instruments of national power against Taiwan, Japan, Vietnam, India, and the Philippines."[12]

China places great emphasis on what Western experts have termed the three forms of warfare, which include Psychological Warfare, Public Opinion / Media Warfare and Legal Warfare (Lawfare) at the strategic level. Specifically, Psychological warfare (PSYOPS) is utilized to influence domestic and international opinion, adversary will, and third-party support. The intent is to undermine an opponent's will to resist. PSYOPS "seeks to influence and/or disrupt an opponent's decision-making capacity, to create doubts, foment anti-leadership sentiments, to deceive opponents, and to attempt to diminish the will to fight among opponents. It employs diplomatic pressure, rumor, false narratives, and harassment to express displeasure, assert hegemony, and convey threats."[13]

Their multi-faceted approach is not unexpected. Hans Morgenthau a correspondent and expert on international relations observed that utilizing indirect power (i.e., cultural imperialism over the minds of individuals) is a more subtle and effective means to alter relations between nations than the use of force.[14] It is not surprising that China is continually expanding its intelligence capabilities.[15] As one expert explained, "Beijing has been intensifying efforts to shape the political environment in the United States to promote its policy preferences, mold public discourse, pressure political figures whom Beijing believes oppose its interests, and muffle criticism of China." [16] It is for this reason, China "invests substantial resources in translating and exploring the contours of U.S. culture and politics."[17] It pays for inserts in newspapers such as the *Washington Post* and *New Your Times,* as well as other venues.

As a result, Chinese influence extends deep into the U.S. and European countries. Chinese political and intelligence agencies have conducted operations on American university campuses to purloin sensitive technologies, collect information, monitor Chinese students, and pressure publishers and researchers not to print negative images of the PRC. A recent RAND study noted the same practices in UK universities. It reported that "almost three-quarters of joint research centres established between UK universities and Chinese partners focus on sensitive areas with potential national security risks. These include synthetic biology, advanced materials, artificial intelligence, and satellite and space technologies."[18]

China's influence even extends to Hollywood, where approval by the CCP determines whether a film release can be distributed in China. Often the CCP pressures American movie studios to adjust their content. Interestingly, there

are very few "Chinese villains in Hollywood movies, a far cry from the Cold War, when movies like The Hunt for Red October pitted the United States against the Soviet Union." As one study concluded, there is an epidemic of "self-censorship" in Hollywood to ensure access to the Chinese market.[19] No-one wishes to lose out on a potential market that numbers over a billion people.

Similarly, for the same reason, The PRC forced numerous concessions from American corporations including Apple, Disney, Facebook, Google, and Microsoft. For example, Apple portrayed disputed islands on its maps as larger than they actually are, and Facebook ran Chinese government advertisements denying persecution of Uyghur Muslims.[20]

Its impact on Europe is no different. China has invested heavily in its efforts at influencing European Union (EU) political elites. These efforts have resulted in dramatic results. For instance, the EU has become less able to cohesively hold China accountable on upholding the rule of law and protecting human rights. In July 2016, Hungary and Greece resisted EU attempts to make a direct reference to Beijing in an EU statement about a binding international tribunal ruling that struck down China's legal claims over the South China Sea. The following year, in March 2017, Hungary derailed the EU's consensus to sign a joint letter denouncing the reported torture of detained lawyers in China. Several months later in June, Greece blocked an EU statement at the United Nations (UN) Human Rights Council criticizing China's human rights record. This action represented the first time that the EU failed to make a joint statement at the UN's top human rights body.[21]

Moreover, in the spring of 2017, the Czechoslovakian Ambassador to Beijing was severely criticized publicly by Czech President Milõs Zeman after he had signed a non-public human rights observance appeal addressed to the Chinese Public Security Minister along with ambassadors from other EU member states and like-minded countries. Moreover, Zeman appointed Ye Jianming, a Chinese citizen, former Chairman and Executive Director of Global Fortune 500 energy and finance conglomerate CEFC China Energy, who was also a major investor in the Czechoslovakian Republic as well as an individual with strong ties with the PLA, as a senior economic policy advisor. Significantly, Ye undoubtedly had access to a vast array of confidential EU documents related to trade and investment, as well as other issues of interest to China.

RAND researchers have concluded one of the most effective means of influence was "China's targeted, often clandestine outreach—sometimes with financial incentives—to specific leaders, elites, and opinion shapers in targeted countries." They noted that China "has demonstrated significant capability to build sympathetic reservoirs of support among other countries' elites and public officials."[22] Alarmingly, China has a growing number of former top-level politicians from Western Europe on its payroll.[23] These individuals are tasked with popularizing Beijing's policies. For example, former British Prime Minister David Cameron took on a leadership role in a one billion U.S. dollar Bridge and Road Initiative (BRI) infrastructure investment fund in December 2017. Similar types of roles have also been accepted by former prime ministers and ministers from France and Germany.[24] Predictably, security experts fear that the CCP's increasingly close connection to some European leaders may also lead to the passage of sensitive EU and national information to Chinese agents.

China's influence campaign also extends to executives and high-level decision-makers in major European firms in an attempt to get their support for China's global infrastructure foreign policy initiatives such as the BRI program. China trades access and partnership for vocal support. For Western firms, this support is a prerequisite for becoming a partner with Chinese investors and contractors in BRI projects in Third World markets. The strategy has been effective. Senior executives in firms such as the logistics company DHL and Siemens Automation company have publicly repeated Chinese BRI marketing language and praised the CCP for its vision. Both DHL and Siemens are key contractors on various BRI projects. Furthermore, individual businesses and business associations have also lobbied their respective national governments to adopt a positive stance towards BRI, playing down any of the known adverse geopolitical and macroeconomic effects of the Chinese initiative.[25]

For those who are uncooperative to Chinese overtures, or those that remain critical or take actions that anger China, they face aggressive action. The PRC has repeatedly engaged in freezing political and economic dialogues with individual EU member states, including Belgium, Denmark, Estonia, Germany, Lithuania, Slovakia and the United Kingdom (UK).[26] These measures are deliberate and part of a long-term strategy that aims to cultivate "self-restraint among European governments when it comes to criticizing China."[27] For example, after a prolonged period of frozen relations between

Norway and China between 2010 and 2016, as a result of the Norwegian Nobel Committee awarding the 2010 Nobel Peace Prize to Liu Xiaobo, Norway's political elites have been very cautious when making public pronouncements on China and Chinese policies. In 2017, Norway's Prime Minister Erna Solberg refused to comment on demands for Liu Xiaobo's release because she did not want to jeopardize negotiations over a free-trade agreement with China.[28]

The aggressive punitive action to signal displeasure with criticism of the regime is wielded without prejudice against any interlocuter. After Australia called for an investigation into the origins of COVID-19, China imposed restrictions on imports of Australian coal, wine, barley, cotton and other goods.[29] Their unhappiness with Canadian criticism of their human rights record, as well as the detainment of the Huawei Chief Executive Officer (CEO) Meng Wanzhou also resulted in diplomatic and economic retaliatory actions.

Although researchers have identified that it is "very difficult to distinguish between targeted and unintended or passive political influencing, and between accepted activities (such as public diplomacy) and those that harm national security," the point is that targeted political influence has become a progressively recognized feature of China's engagement in Europe.[30] Despite the specific targeting of primarily political and business elites, media and think tanks, the ultimate objective is to have impact on the overall public opinion. Researchers have observed that the "potential security risks are likely to be of a long-term rather than a short-term nature and relate to the weakening of European and the EU's global influence (through the erosion of economic competitiveness) and to the EU's ability to act as a unified actor and a close partner of the United States.[31]

Chinese political actions to further their national interests also extend to foreign universities. For instance, the high numbers of Chinese students at Australian universities have created an environment of self-censorship. According to Human Rights Watch, lecturers avoid criticizing Beijing policies and actions and Chinese students remain silent to avoid harassment. There are cases of parents in China being questioned by Chinese police about the activities of students in Australia. Moreover, due to the COVID-19 pandemic and the move by universities to on-line courses, Chinese students who join classes from behind China's highly controlled system of internet, self-censorship has only increased. Academic freedom has been greatly

compromised. For example, one on-line course removed references to the bloody 1989 Tiananmen Square crackdown.[32]

China has also worked at extending its influence in academia and scholarship. By 2009, there were a total of 440 Confucius Institutes worldwide, with 90 in the U.S. alone.[33] This investment furthers Beijing's tentacles in spreading its narrative and countering criticism.

Further to the political competition landscape, China uses public opinion and media warfare from both an internal and external lens. It strives to shape domestic and foreign opinion, as well as support, through mass information platforms such as television, radio, newspapers, the internet and social media to generate support at home and abroad, as well as opposition to its adversaries / competitors.[34] This approach is a "constant, on-going activity aimed at long-term influence of perceptions and attitudes."[35] Researchers have concluded:

> It leverages all instruments that inform and influence public opinion including films, television programs, books, the Internet, and the global media network (particularly Xinhua and CCTV) and is undertaken nationally by the PLA, locally by the People's Armed Police, and is directed against domestic populations in target countries. Media warfare aims to preserve friendly morale, generate public support at home and abroad, and weaken an enemy's will to fight and alter an enemy's situational assessment. It is used to gain 'dominance over the venue for implementing psychological and legal warfare.' Media warfare ties into Chinese diplomacy. At the UN and in other venues, China promotes the use of phrases that align with its diplomatic vision, such as "win-win cooperation," "people to people connectivity," and "creating a community of shared future for mankind."[36]

China's persistent, ubiquitous influence over external audiences is insidious. Often, its impact is not always fully realized. An example of China's willingness to exert its muscle was evident when the National Basketball Association general manager of the Houston Rockets criticized China's approach to Hong Kong on Twitter. China responded by blocking the broadcast of NBA games in China and then conducting a devastating on-line attack on the general manger in question.[37]

The attempts at controlling negative discourse extend even further. In March 2022, the U.S. Justice Department charged five people with assisting the CCP to "stalk, harass or spy on political dissidents in the US, including a congressional candidate and a Los Angeles sculpture artist."[38] In another case, a retired Chinese intelligence agent, Qiming Lin was charged with conspiracy for his efforts to smear a 2022 congressional candidate in New York.[39]

Another political means of waging strategic competition is China's use of Legal Warfare (or "Lawfare"). This approach focuses on exploiting the legal system to achieve political or commercial objectives. China practices legal warfare to validate actions in law and create support both domestically and externally. It utilizes domestic law, as well as the laws of armed conflict and international law to argue that China is within its rights to take whatever respective action is underway. By invoking the chimaera of legality, China attempts to cloak its actions in legitimacy.[40]

As part of its "lawfare" approach to competition, China has embedded itself within international organizations and uses these platforms to further its objectives. Significantly, Beijing has assumed powerful leadership positions within international institutions. Out of 15 UN agencies, China controls the head of the UN Food and Agriculture Organization, the UN Industrial Development Organization, as well the International Telecommunication Union and the International Civil Aviation Organization.[41] As Melanie Hart, a senior fellow and the director of China policy at the Center for American Progress, observed, "No other nation leads more than one." She added, "Making contributions is one thing, but [the Chinese delegates] show up big, and they push."[42]

Researchers have affirmed that "China has demonstrated an increasingly assertive and proactive stance within these organizations, which has combined in some cases with greater institutional power." They explained, "Across the board, China has become more effective in utilizing international organizations to advance national interests, and to extract what it needs from these institutions." They concluded, "Importantly, from a tactical point of view, China's constructive engagement in these organizations is shrewd because it heightens Chinese credibility, which further strengthens China's influence, and its ability to achieve its objectives.[43]

Its increasingly oblique penetration of international organizations, as well as its own initiatives, to garner access, influence and leverage in regions such as

the Middle East and Africa are extremely worrisome. A RAND report noted, "Chinese success in establishing itself as a principal arbiter in Middle Eastern affairs, as the main sponsor of Africa's economic development, and as a major partner in Latin America could result in a severe weakening in the strategic position of the United States as a global leader and undercut its position in the Indo-Pacific theater as well."[44] China is also establishing international organizations that compete with the functions of the Western-dominated UN. For instance, it has created the Asian Infrastructure Investment Bank and the China Development Bank. As of 2018, the China Development Bank had funded 500 projects in 43 different African countries worth a total of $50 billion.[45]

Additionally, in 2018, China invited 50 African countries and the African Union to participate in the inaugural China-Africa Defense and Security Forum, which represented a more formal and far-reaching level of dialogue. Such venues allow Chinese and African representatives to establish deeper ties and to conduct sustained discussion that identify opportunities to enhance collaboration in the defence and security domain.[46]

Similarly, in May 2022, China was in the process of signing a security agreement with the Solomon Islands, which would allow the Solomon Islands to request the Chinese government to provide military and law enforcement personnel to maintain "social order" in exchange for China's ability to use the Solomons for "logistical replenishment," "stopover" and "transition." The agreement met great consternation from New Zealand, the U.S. and other Western partners. Such an agreement would allow China a growing presence in the South Pacific, giving it a strategic foothold and potentially a military presence in the Pacific that could destabilize Western influence.[47]

Beijing did not stop there. China has pressured ten small Pacific nations to endorse a sweeping agreement covering everything from security to fisheries. Experts warn this is a "game-changing" bid by Beijing to seize control of the region. The pact would see a jointly developed marine plan for fisheries, increased cooperation on running the region's internet networks, the establishment of even more cultural Confucius Institutes and classrooms and possibly the creation of a free zone with the Pacific nations. The concern from experts emanates from the fact that China "has a pattern of offering shadowy, vague deals with little transparency or regional consultation in areas related to fishing, related to resource management, development, development assistance and more recently even security practices."[48] The agreement

would, in essence, pave the way for China to own and control the region's fisheries and communications infrastructure.

China's geopolitical aim, according to Thomas Mahnken, a Senior Research Professor and the Director of External Programs at the Philip Merrill Center for Strategic Studies, "is to exercise predominant influence over the defining ideas, rules, and institutions of world politics, competing with the US to shape the foundational global system through political warfare." He explains that the CCP "seeks to use overt and covert means to influence, coerce, intimidate, divide and subvert rival countries in order to force their compliance or collapse" and has a "deep attachment to revisionist strategies that overturn domestic and international norms."[49] In essence, "China focuses on long-term positional advantages, sustaining a campaign with exceptional patience and persistence, resulting in competing countries to acquiesce and accept the 'new facts' as normal, such as in the South China Sea."[50]

Over the last decade, China (as well as Russia) have also slowly chiseled away at US influence in the Middle East. They have achieved this by entering into lucrative arms deals and investing commercially, as well as backing America's adversaries in diplomatic forums. Most recently, some analysts argue that China (and Russia) intend to use vaccines as another strategy to position themselves as "benign scientific leaders" and extend their influence and status in a post-COVID-19 world.[51] Some analysts argue that Beijing and Moscow are using vaccines as the most recent vehicle "to pull the Middle East deeper into their sphere of influence."[52]

China has also used "lawfare" and its coercive tactics to further its position itself in its geographic pursuits. China has claimed almost all of the 1.3 million square mile South China Sea. Since 2014, it has transformed indistinct reefs and sandbars into man-made artificial islands, fortified with missiles, runways and weapons systems. In the process they have antagonized governments with overlapping claims, including the Philippines, Vietnam, Malaysia, Indonesia, Brunei and Taiwan.[53] Part of its approach has been to threaten the use of force against foreign naval vessels navigating the surrounding waters citing sovereignty over the contiguous maritime zone, as well as plundering the natural resources within the exclusive internationally recognized economic zones of other countries. Cleverly, the Chinese government utilizes a combination of civilian fishing vessels, coast guard ships, and maritime law enforcement forces to protect its island-building efforts and

enforce its claims. Since these vessels are unarmed, American or regional naval forces cannot respond with military force without significantly escalating the confrontation.

And, that is exactly the intent of the Chinese government. To enforce its will and achieve its political objectives without provoking a military response from the West. Their efforts continually erode U.S. influence and credibility in the region and push the U.S. that much closer to being shut-out from the Indo-Pacific region.

Economic Means

Another important component of China's strategy in the GPC is its economic power. General Stanley McCrystal, a former commander of the Joint Special Operations Command (JSOC) affirmed, "For China competition is 80 per cent economic and 20 per cent diplomatic and military."[54] A RAND report concluded, "the most effective source of influence in the various cases and data sources that we investigated was the weight of attraction of China's economy. Countries' desire for trade, direct investment, technology transfer, and other economic benefits far outweighed other potential sources of influence, such as direct military threats or any form of the China model (e.g., development, sociopolitical).[55]

Quite simply, the PRC uses its economic capacity to great effect. China uses its economic might to threaten the sale of state debt, to pressure foreign businesses to invest in China's market, to employ boycotts, to restrict critical exports (rare earth minerals), to inhibit imports, and to employ predatory practices (e.g., steel production) to expand market share.[56] Its latest five-year plan calls for dominating "chokepoints," namely goods and services that are indispensable to other countries. China then uses its dominating position, as well as the lure of its large domestic market, to force concessions from other states. As such, it sees itself becoming "the dominant dispenser of overseas loans, loading up more than 150 countries with over $1 trillion of debt."[57]

Moreover, it has massively subsidized strategic industries to gain a monopoly on hundreds of vital products, and it has installed the hardware for digital networks in dozens of countries.[58] The PRC uses its monopoly in materials and resources (e.g., rare earth elements (REE)) as a political weapon to achieve its objectives. For example, in 2010, China halted shipments of REE to Japan following the Japanese detention of a Chinese fishing crew during a maritime border dispute.[59]

One of its most widely known economic strategies has been the BRI, which utilizes state-owned enterprises that have strong links to the PLA to:

- boost PRC domestic growth;
- solve internal demographic problems; and
- realize the PRC's strategy for dominating global economic-security diplomacy.

The BRI is the PRC's international, transcontinental, multi-domain strategic infrastructure construction project. Its announced investments are as high as $8 trillion across Europe, Africa and Asia. While originally envisioned in 2013 to be limited to 60 countries, the PRC has expanded BRI, as of 2020, to 130 countries representing over two-thirds of the world's population.[60] As such, the BRI has become an infrastructure financing initiative for a large part of the global economy that will also serve key economic, foreign policy and security objectives for the Chinese government.

Far from being simply an infrastructure project, the BRI has become a strategic foreign policy initiative. It allows China to position itself as an alternative global and political order to the Western rules based international order. Additionally, it situates China to make important economic and strategic inroads throughout the world.

The BRI allows the PRC to leverage its economic power to forge ties with other nations, expand its influence and strategic geographic positioning.[61] Although seemingly benevolent, the BRI is used to force recipient nations into onerous debtor relationships. China's "generosity" has a steep price. The BRI is used to persuade partner nations to accumulate high levels of debt. For instance, in 2016, Sri Lanka defaulted on loans and as a result, China forced Sri Lanka to cede control of the Hambantota Port to the China Merchant's Port for 99 years.[62] Beijing's "debt trap" diplomacy has allowed China to gain access to a number of other strategic assets as well such as the Piraeus Port in Greece, Zambia's Kenneth Kaunda International Airport and Djibouti's Doraleh Naval Port. [63]

Additionally, although the PRC furnishes "loans" for projects, the actual construction jobs go to Chinese, not local, workers, as well as Chinese or affiliated partner firms.[64] For example, in 2008, in the Democratic Republic of the Congo, China agreed to build 3,800 kilometres (km) of road, 3,200 km of railway, 32 hospitals and 145 health clinics and two universities. However,

China stipulated that at least 70 per cent of the labour would be supplied by China. Moreover, the Chinese-owned firms used for construction imported cheap goods that pushed the local entrepreneurs out of the market. Additionally, the PRC did not transfer technology, it flouted local labour laws, created environmental damage, and neither offered competitive wages, nor adhered to work hour limitations.[65]

The key, however, is that China is willing to provide massive loans for mega-industrial and infrastructure projects that can seemingly unlock Africa's potential. Importantly, unlike their Western competitors, the PRC doesn't dwell on issues such as good governance or fiscal management. One African ambassador explained, "The Chinese just come and do it. They don't hold meetings about environmental impact assessments or human rights, bad governance and good governance…Chinese investment is succeeding because they don't set very high benchmarks."[66] As a result, as of 2019, according to the London School of Economics, China had a total $165 billion in direct investments in Africa. From 2014 to 2019, China invested almost double what the U.S. and France did in Africa. As one analyst observed, "You're going to have to write the cheques to be taken seriously." In the new "Great Game" in Africa, the most powerful weapon is money.[67]

The importance of money has not been lost on China in its competition for influence and access to achieve its objectives. In North Africa, the PRC has spent $11 billion since 2015 on the Trans-Maghreb highway alone. This road network that spans from the Western Sahara to Libya will connect 60 million of the region's 100 million people. In East Africa, China built a network of roads and a rail lines linking Ethiopia and Djibouti, as well as financing a large port in Djibouti (a location that just so happens to be a chokepoint for global shipping and the port is large enough to host Chinese nuclear submarines and aircraft carriers).[68] In West Africa, in Gabon, the PRC built a railway from mining territory 800 km inland to the country's main port. In addition, it is also building a deep-water export terminal and a hydropower dam. In southern Africa, China, in conjunction with the African Development Bank, supported a Namibian port expansion at the cost of $300 billion and Angola was loaned $4.5 billion for a hydroelectric plant.[69] In Uganda, the PRC financed the building of a $350 million road from Entebbe to Kampala.[70]

China's focus on Africa is easy to understand. Africa is home to 11 of the world's 25 fastest growing economies, as measured by gross domestic product data for 2020.[71] Moreover, Africa's population is young, growing fast, and

expected to top two billion by 2050, at which point more than a quarter of the world's population will reside on the continent. By 2100, Africa's population could nearly double again. Not only is the continent's growth rate the highest in the world, but the population is the youngest, with 41 percent under the age of 15.

Quite simply, the growth and demographic of the African population, fuels its rising global importance.[72] In 2002, trade between the U.S. and Africa was $21 billion, nearly double China's $12 billion in trade. Six years later, in 2008, U.S. / Africa trade swelled to $100 billion, although by 2019 it plummeted to $56 billion. However, in the same eleven-year period, Chinese / African trade rose from $102 billion to $192 billion. Currently there is no other country that comes close to the PRC's investment in Africa.[73]

China's success is easily discerned. Its practice of bundling infrastructure projects with concessional, resource-backed loans has proven particularly appealing to impoverished African nations. These nations receive large loans at below world market rates for major infrastructure projects. In return, the resource rich countries pay back the Chinese with resources such as oil, copper, cobalt and other minerals over a long-term period. For the African countries, they do not have to deal with pesky Western requirements for good governance and transparency. Moreover, the projects are delivered quickly with no lectures.[74]

China's economic strategy as part of strategic competition is not solely limited to Africa. The PRC became the largest trading partner of Arab countries in the first half of 2020 with two-way trade of more than $115 billion. In fact, it has launched partnerships, specifically a "Comprehensive Strategic Partnership" with 12 Arab nations. Alarmingly, a recent survey conducted in the region found China is viewed more favourably than the U.S.. "Arab Barometer," a research network based at Princeton University, polled citizens in six countries in the Middle East (i.e., Algeria, Jordan, Lebanon, Libya, Morocco and Tunisia) to gauge their attitudes toward China and the U.S. "The survey results make clear that Arab publics prefer China," the organization reported.[75] In fact, Israel, America's closest ally in the region, also joined the Chinese BRI initiative.[76]

Beijing economic and political leverage has also pushed the Americans out of Cambodia. For the past two decades China has carefully cultivated closer ties with that state by backing Prime Minister Hun Sen's 33-year authoritarian

hold on power. In 2017, Sen trashed the long-running American military aid program called Angkor Sentinel. Instead, he increased training with the PLA. In September 2020, the Cambodian government demolished the American facility at Ream Naval Base. Prime Minister Sen also ceded 20 per cent of the Cambodian coastline to Chinese-owned companies. In addition, the influx of thousands of Chinese nationals moving into Cambodian provinces puts them in a position to sway provincial elections due to a 2016 legal change that allows foreigners with Cambodian identification cards to vote.[77]

China's strategy of using its economic clout also bled into its campaign to become invested in UN operations. In November 2020, Beijing announced it would work with the international community to achieve long-term peace in the Sahel. As such, the PRC pledged $45.7 million for security and counter-terrorism during a UN Security Council meeting to support the G5 (i.e., Burkina Faso, Chad, Mali, Mauritania and Niger). China is the second largest contributor to the UN peacekeeping budget, currently contributing approximately $6 billion a year.[78]

Their ability to maximize impact is noteworthy. For instance, during the spring of 2020, when President Donald Trump declared, during the midst of the COVID-19 pandemic, that he would stop funding for the World Health Organization (WHO), a sum of more than $400 million annually, Chinese President Xi Jinping a week later pledged another $30 million to the organization. The fact that the PRC still owed the WHO $60 million in membership dues was lost in the noise. The move was a stroke of genius. The message conveyed was clear to most. Once again, China's cheque book diplomacy scored another important victory. Their desired message was abundantly clear, "*You can't count on the U.S., but you can count on us.*" Rear Admiral Kenneth Bernard, a former political adviser to the director-general of the WHO explained, "The Chinese give as little money as they can get away with. They give as little money as will buy influence. This isn't about being fair. This is about winning."[79]

China's "cheque book diplomacy" is not only at play in third world countries. The U.S. is also a key proponent of the PRC's success in this field. American corporations, universities and colleges, as well as Hollywood film studios and sports leagues are all seduced by Chinese money and markets. As a result, they willingly gorge themselves on CCP money they pour in the trough. "It's akin to fattening chickens and cattle until they have served their purpose and are ready to be devoured," explained Peter Thiel, a billionaire

entrepreneur and venture capitalist who criticized "Big Tech" for chasing Chinese funding and deliberately turning a blind eye to China's forced labour camps and human rights violations. Senator Marco Rubio reinforced Thiel's criticism stating, that the PRC has "deputized major American corporations and their leaders to ... push for and pressure for policies that favor the Chinese position."[80] Amazingly, already in 2015, the Chinese budget for influence operations alone was estimated at $10 billion. As an example, in the past six years Stanford University "received $32,244,826.00 in monetary gifts from China" and Harvard "received $55,065,261.00 through a combination of contracts and monetary gifts."[81] Not surprisingly then, more than 500 U.S. scientists are under investigation for being compromised by China and other foreign countries, according to a recent hearing before the Senate Health, Education, Labor and Pensions Committee.[82]

A final application of its economic muscle is to advance its intelligence and military capabilities. "Innocent" economic investment opportunities seemingly for diversification also are used as a front to gain access for strategic purposes. In 2013, Huang Nubo, a former official in the CCP, who was now a property developer in Beijing, attempted to buy land in Grímsstaðir, Iceland, to build a luxury hotel and eco-golf course. A luxury resort in such a remote area quickly gleaned suspicion. A few years later, in 2016, the Chinese mining firm General Nice Group attempted to buy a defunct U.S. naval base in Greenland and tried to build at least two airports in the country. These attempts at procuring infrastructure are a clear attempt at the Chinese to gain a physical foothold in the Arctic and position themselves astride NATO lines-of-communication.[83]

In 2015, China's Shandong Landbridge Group, which has ties to the PLA, spent $506 million (Australian) to acquire a controlling stake in the Port of Darwin. Darwin Naval Base, which is home to Australia's fleet of patrol vessels and it hosts American and other allied warships, is co-located with the port. That same year, China Ocean Shipping Company gained control of the port of Piraeus, which is the location of Greece's largest naval base and a hub for NATO operations in the Mediterranean as well as for the U.S. Navy's Sixth Fleet.[84]

More obvious yet, was the Chinese effort to purchase the Hotel del Coronado, which overlooks the San Diego Naval Base, where there exists volumes of military traffic (e.g., radio, cellphone, microwave and satellite signals, Wi-Fi, sensor feeds, radar waves, GPS, navigation signals). The hotel is an

ideal "listening post." It was eventually purchased for $1 billion USD in 2016 by the Anbang Group, a Beijing-based company taken over by the Chinese Government.[85]

Similarly, in 2018, a group of Chinese nationals bought Rosslea Hall, which sits at the base of a spit of land projecting into Gare Loch, which connects the Firth of Clyde network of waterways west of Glasgow and its port. Approximately, six kilometres away is Faslane, formerly Her Majesty's Naval Base Clyde, home to Britain's entire fleet of four Vanguard-class missile submarines, which represents the country's only nuclear deterrent. Almost from the moment they cast off, submarines are in direct visual and electronic line of sight from Rosslea Hall.[86]

Finally, China Radio International (CRI), a state run firm, holds the controlling interest of at least 33 radio stations in 14 countries, including an English language news station in Washington D.C.. This control allows China to deliver native language news biased towards the CCP and its preferred narrative of events. A Center for Strategic and International Studies 2020 report, revealed, "Nearly every Chinese language news outlet in the U.S. is either owned by, or works closely with the Party - and it is making inroads into English language media as well. There are more than a dozen radio stations in cities across the country where Americans hear subtle pro-Beijing propaganda on their FM radio."[87]

As with most Gray Zone activities the true motives are often hard to distinguish. Is it simply foreign economic investment? Are they simply diversifying? Or, is it a more diabolical intent to gain strategic advantage and leverage in the GPC? The simple truth, however, is that Beijing uses subsidies, loans and espionage to help its firms dominate global markets and access infrastructure, territory and resources to further its political, economic and military objectives.

Military / Para-Military

An important component of China's approach to strategic competition is its military and para-military capability. First, its military modernization in all domains, including nuclear, naval, and missile capabilities, introduces new risks and potential threats to the West, as well as to global security and stability. It also acts as a nuanced hammer either as a deterrent or as a means to bully and intimidate others. "In the coming years," cautioned

General Richard Clarke, commander of U.S. Special Operations Command (USSOCOM), "China will become the most capable adversary, and they are rapidly modernizing."[88]

Notably, Beijing's approach to deterrence is guided by its Active Defense Strategy in accordance with its National Security Law of 2015, as well as China's 2019 White Paper, *National Defense in the New Era*. Accordingly, China approach is depicted as "strategically defensive but operationally offensive." In essence, if China perceives that its interests have been damaged, or are about to be injured, at the strategic level by another state, it will take offensive action to defend its interests. It "seeks to control events on its terms, initiating actions to escalate or deescalate tensions to achieve its objectives."[89] As part of this strategy, Beijing "is prepared to undertake risky actions that threaten to escalate a crisis unless the other side accommodates Beijing's demands."[90] Menacingly, China has demonstrated a propensity to use limited force to show both its "capability and willingness to escalate a crisis and employ larger scale military forces to deter adversaries."[91]

To support its use of military means to achieve its objectives in the GPC, China has focused on building up its military capability. Of particular concern is their advanced anti-access / area denial (A2/AD) network, which is a series of sensors, antiship, antiaircraft, and ground defenses; and long-range fires designed to prevent China's rival and competitors from entering into a close fight. China has installed a vast array of A2 / AD zones conceived to deny U.S. and allies access to Taiwan and the South China Sea.[92]

The PLA has built-up a massive number of missiles that for the most part have a greater range than those of the U.S. and its regional allies. General John Hyten, vice chairman of the Joint Chiefs of Staff, revealed that the Chinese launched a hypersonic weapons test that sent a missile around the world at more than five times the speed of sound. "They launched a long-range missile," Hyten described, "It went around the world, dropped off a hypersonic glide vehicle that glided all the way back to China, that impacted a target in China."[93]

The PRC has also reportedly developed a 30-kilowatt road-mobile Direct-Energy (DE) system, the LW-30, designed to engage unmanned aerial vehicles and precision-guided weapons. These systems can be used to interfere with adversary aircraft and to disrupt freedom of navigation operations in the Indo-Pacific. According to the Defense Intelligence Agency (DIA), China is

also "pursuing DE weapons to disrupt, degrade, or damage satellites and their sensors and possibly already has a limited capability to employ laser systems against satellite sensors."[94] Experts predict China likely will field a ground-based laser weapon that can counter low-orbit space-based sensors by 2020, and by the mid-to-late 2020s, it may field higher power systems that extend the threat to the structures of non-optical satellites.[95]

As a result of the Chinese advancements, American commanders have warned that "China holds a clear advantage in these weapons" and that the "United States, long the dominant military power in Asia, can no longer be confident of victory in a military clash in waters off the Chinese coast."[96] Quite simply, the Americans are no longer the indisputable military power in Asia.

China is also modernizing its nuclear forces as part of its overall military modernization effort. Most analyst agree that China will increase the size of its nuclear force in the near future.[97] Experts predict that China could have as many as 1,000 nuclear warheads by 2030.[98] The Director of National Intelligence (DNI) annual threat assessment asserted:

> Beijing will continue the largest ever nuclear force expansion and arsenal diversification in its history. Beijing is not interested in agreements that restrict its plans and will not agree to negotiations that lock in U.S. or Russian advantages. China is building a larger and increasingly capable nuclear missile and bomber force that is more survivable, more diverse, and on higher alert than in the past, including nuclear missile systems designed to manage regional escalation and ensure an intercontinental strike capability in any scenario. China is building hundreds of new intercontinental ballistic missile (ICBM) silos. As of 2020, the People's Liberation Army Air Force (PLAAF) had operationally fielded the nuclear capable H-6N bomber, providing a platform for the air component of the PRC's nascent nuclear triad. China conducted a hypersonic glide vehicle (HGV) flight test that flew completely around the world and impacted inside China.[99]

Central to China's build-up and modernization of its military capability is its increasing reliance on space to provide it with a beneficial edge in any future conflict with the U.S. and its allies. The PRC has aggressively launched, acquired, and obtained through espionage the counter-space capabilities necessary to prevail according to a DIA report. It revealed that China has

made great strides in its space program, doubling the number of intelligence, surveillance, reconnaissance (ISR) satellites it has in space (i.e., 250) since 2018. The DIA report also noted that the PRC probably is developing jammers dedicated to targeting SAR [synthetic aperture radar]. Importantly, those jammers would be key to preventing American and U.S.-affiliated commercial satellite firms from maintaining a clear picture over Taiwan, as they have in Ukraine.[100] Similarly, the DNI annual threat assessment noted, "Counterspace operations will be integral to potential military campaigns by the PLA, and China has counterspace weapons capabilities intended to target U.S. and allied satellites. The PLA is fielding new destructive and nondestructive ground- and space-based antisatellite (ASAT) weapons."[101]

Another critical component of its use of military forces in strategic competition is China's focus on irregular warfare. These activities are fully integrated with their conventional doctrine and tactics. The Chinese do not even identify any of their actions as irregular. The PLA is planning to fight concurrently across multiple domains. Significantly, the PLA emphasizes "informationized wars." It considers "information superiority as the driver of operational planning." The components "of irregular warfare, such as psychological warfare, legal warfare, and cyberwarfare, are central to the PLA's concept of information warfare and its theory of victory in a conventional conflict."[102]

Within Chinese military writing and operations there are three principal elements of irregular warfare, namely the "three warfares" (i.e., Psychological Warfare, Public Opinion / Media Warfare and Legal Warfare (Lawfare)) as discussed earlier. These methodologies are used to stifle domestic criticism and more importantly attempt to influence foreign governments "in ways favorable to China." The "three warfares" shape the battlespace by creating a favourable strategic and operational environment prior to hostilities. One analyst noted that the application of the "three warfares" is exceptionally interactive in nature. For example, legal warfare provides the basis for launching an attack; public opinion warfare delegitimizes the adversary; and psychological warfare demoralizes the opponent.[103]

Another component of China irregular warfare capability is the use of SOF. Although Chinese SOF have a smaller band of missions than those of their U.S. adversary, they do emphasize Direct Action (DA) and Special Reconnaissance (SR). They do not specialize in unconventional warfare (UW), which would represent a shortfall in their ability to support insurgencies or organize indigenous resistance groups.[104]

Yet, another irregular warfare capability is the use of paramilitary forces. These are composed of the People's Armed Police (PAP), the maritime militia, and private security companies. The PAP is responsible for reacting to internal unrest, maintaining social stability, fighting terrorism, and protecting national sovereignty. Notably, the PAP also functions internationally. In 2018, the CCP transferred control of the Chinese Coast Guard to the PAP, which was now responsible for the maritime security role as well. In addition, the PAP also operates a base in Tajikistan, which is believed to be responsible for supporting counterterrorism operations along the Tajikistan-Afghanistan border, as well as inside Afghanistan. Moreover, PAP units have also deployed on UN peacekeeping missions. However, its primary role remains its national-level focus on maintaining internal stability and policing restive Tibet and Xinjiang, which connotes an emphasis on counter-terrorism and counter-insurgency missions. This focus, residing in the PAP instead of the PLA, led analysts to believe that there is a possibility of PAP ground units being deployed beyond China's borders during a conventional war to carry out counter-terrorism and counter-insurgency operations.[105]

Key to the Chinese military component in its strategic competition posture is the integration of its military and civilian capabilities, as well as its investment in artificial intelligence. The American National Security Commission on Artificial Intelligence warned of a "'new warfighting paradigm' pitting 'algorithms against algorithms,' and urges massive investments 'to continuously out-innovate potential adversaries.'"[106] China has heeded this call and its latest five-year plan places AI at the centre of its research to assist the PLA in its focus on "intelligentized warfare." As Russian President Vladimir Putin stated in 2017, "whoever becomes the leader in this sphere [AI] will become the ruler of the world."[107]

Further to China's integrated military / civilian complex is its industrial policy and military-civil fusion (MCF) strategy. At the core of its strategy is the Chinese belief that "all international states are in perpetual competition across all domains. It is important for a state to adapt and apply the will and strength of the entirety of society to support security and development goals."[108] MCF allows for improved efficiency and resource-sharing to maximize the strategic effects of China's economic growth and defense spending. As one analyst concluded:

> It is also important to note that the focus of the strategy is internal and is on improving interactive ecosystems such as manufacturing,

> science and technology, education, social services, and public safety within China, not simply ensuring efficient cooperation between civilian organizations and the Chinese armed forces. By blurring the line between military and commercial endeavors, military-civil fusion (MCF) has heightened the risk that U.S. companies or universities may be unwittingly eroding U.S. military advantage through cooperation with Chinese companies, institutions, or individual researchers. The primary threats linked to MCF involve IP theft and tech transfer tactics, which are often linked to, but hardly synonymous with, MCF.[109]

The MCF strategy has caused enormous Western concerns about the PRC. President Xi Jinping has taken a long-standing policy and pressed MCF as a priority. He has expanded, intensified, and accelerated the effort across multiple domains, particularly placing an emphasis on a more integrated development of emerging technologies. He elevated MCF to national grand strategy "in response to complex security threats and as a means of gaining strategic advantages."[110]

Another means the PRC is utilizing its military in strategic competition to gain influence and access is through its participation on UN peace keeping operations. The year 2020 marked the 30th anniversary of China's participation in UN peacekeeping operations. During this period, the PLA deployed over 40,000 personnel on twenty-five UN missions, the majority in Africa. China is currently the second-largest contributor to both peacekeeping missions, as well as UN membership fees.[111]

Although PRC contributions to Africa have initially, for the most part, been involved with support tasks such as medical and engineering personnel, they have expanded into more active roles such as mediation, enforcing UN mandates to protect civilians, policing and infantry-centric operations. As of February 2020, China has more than 2,000 soldiers and support staff deployed in Africa in locations such as the Central African Republic (CAR), the Democratic Republic of Congo, Mali, South Sudan and Sudan.[112]

The Chinese support of UN operations is not benevolent. Clausewitzian "realpolitique" is at play. At the 2015 Forum on China-Africa Cooperation, the PRC pledged $100 million in military assistance to create an African Standby Force. Additionally, the People's Liberation Army Navy (PLAN) also conducts goodwill ship visits and deployed a hospital ship known as the "Peace Ark"

to provide medical assistance and healthcare to Djibouti, Kenya, Tanzania and the Seychelles. These initiatives are designed to further PRC economic interests, access and influence.

The military has also been used outside of UN operations to extend Chinese influence. For example, four Chinese-made Wing Loong II combat drones were deployed to Nigeria to take part in ongoing counter-insurgency and anti-banditry operations. The Chinese initiatives also include the sale of armaments. From 2015-2019, the PRC was the second largest supplier of weapons to Saharan Africa representing nineteen per cent of sales. Russia accounted for thirty-six per cent.[113]

China's military engagement is a key component of its strategy to penetrate Africa. The PRC provides a panoply of benefits in its arms sales as it blends the sale of weapons with military assistance, economic overtures including investment and trade deals, as well as other programs. Notably, China does not focus on human rights records or corruption. As such, the PRC holds significant advantages over its Western competitors in Africa.[114] These Chinese inroads have not been missed. Africa Command (AFRICOM) Commander General Townsend acknowledged, "We cannot compete economically with China."[115]

General Townsend further elaborated that China was apparently seeking to extend its influence beyond the Pacific with the potential construction of a large Atlantic naval base on the western coast of Africa. He observed that the PRC has been dealing with countries as far north as Mauritania and as far south as Namibia with regard to creating a naval base that is capable of hosting submarines or aircraft carriers.[116]

General Townsend's concerns were not alone. Senate Armed Services Committee member Senator Mark Kelly reinforced the warning, asserting that China was expanding its influence on the continent with military infrastructure. "They've got a strategy to expand there," he cautioned, "and to be able to project power in regions of the world that they haven't previously."[117]

Another of its key military components in undertaking strategic competition is its maritime militia, which is a critical element of its Gray Zone operations to assert control over disputed territory. The maritime militia is based on civilian fishers and their vessels, which also represent a component of the

Chinese national fishing fleet.[118] Although the majority of the members are civilians with little military training, there is also a core in the militia that is full-time, do not partake in fishing activities and are better trained. The Maritime Militia have proven to be an influential force. They were involved with the 2009 provocation of the *USNS Impeccable*, the stand-off at the Scarborough Reef in 2012 and at the Haiyang Shiyou 981 oil rig in 2014, the surge of ships near Senkakus in 2016, as well as more recently the confrontation at the Whitsun Reef.[119]

The maritime militia's versatility is unquestionable. It acts to "enforce" territorial claims, provides an intelligence capability and an economic tool for plundering foreign resources. In 2021, approximately 350 Chinese-flagged vessels deployed just beyond Argentina's territorial waters for over six months. The fleet was suspected of plundering squid stocks. China has been consistently ranked as the world's worst fishing offender due to its massive distant-water fishing fleet, which is estimated to number in the thousands. Their vessels fish illegally employing bright lamps to draw fish to the surface at night and they turn off their GPS-based automatic identification systems so they cannot be identified.[120]

Although employed in Gray Zone operations, the Maritime Militia would also feature in a conflict. The Chinese have demonstrated historically that they would utilize irregular and conventional forces in a war with its adversaries. Chinese writing has identified a number of wartime missions for the Maritime Militia including ISR, counter-ISR, sabotage, anti-aircraft missions, raiding, and electronic warfare.[121]

A final use of the PRC's military in strategic competition is to bully its neighbours and adversaries. For instance, Taiwan expelled nearly 4,000 Chinese vessels that were illegally dredging sand from its waters in 2020, a more than six-fold increase on the previous year.[122] Additionally, Taiwan's coastguard expelled more than 500 vessels up to November 2020, compared to 91 in 2019 and none in 2018.[123] Furthermore, in 2020, Chinese jets made a record 380 incursions into Taiwan's air defence identification zone (ADIZ). June 2022 provides a single example of the magnitude of intrusions. On just one given day, Taiwan scrambled jets to intercept 29 Chinese aircraft, which included 17 fighters, six H-6 bombers, as well as a number of electronic warfare, early warning, antisubmarine and aerial refuelling aircraft. The airplanes penetrated the Taiwanese ADIZ. This Chinese practice is designed

to both wear out Taiwanese forces by making them repeatedly scramble, as well as to test Taiwanese responses.[124]

In another example, in three separate incidents over a period of two months in the spring of 2022, Chinese law enforcement vessels challenged marine research and hydrocarbon exploration activities within the Philippines' exclusive economic zone in the South China Sea.[125] The intimidation tactics were designed to press Chinese claims to disputed waters.

Additionally, Chinese jets repeatedly buzzed Canadian aircraft as they were taking part in a multilateral UN mission over the Pacific Ocean to enforce sanctions against North Korea.[126] They actually sprayed metallic chaff in the path of an Australian surveillance plane that approached the Paracel Islands, which are a Chinese-held archipelago in the South China Sea that is also claimed by Vietnam and Taiwan.[127] In all cases, the Chinese actions were extremely aggressive and dangerous.

Although not military per se, China is expanding its use of private security companies (PSC) as a method of growing its reach globally as well. China has in excess of 5,000 PSCs, some of which operate internationally. Although not used in the same manner as the American PSCs in Afghanistan and Iraq, their presence in support of Chinese corporations participating in the Road and Belt initiative give the PRC additional access and influence.[128]

Espionage

Espionage is yet another key tool in the PRC's pursuit of global competition. Director Christopher Wray of the Federal Bureau of Investigation (FBI) disclosed that the current scale of espionage and cybersecurity threats from China were "unprecedented in history." He divulged, "The biggest threat we face as a country from a counterintelligence perspective is from the People's Republic of China and especially the Chinese Communist Party." He explained, "They are targeting our innovation, our trade secrets, our intellectual property, on a scale that's unprecedented in history." He revealed that China's hacking program is larger "than that of every other major nation combined." Wray noted, "They have stolen more of Americans' personal and corporate data than every nation combined." He exposed, "We are now moving at a pace where we're opening a new China counterintelligence investigation about every 12 hours."[129]

The PRC espionage efforts extend to cultivating agents within adversary intelligence organizations. In 2019-2020, four former DIA and Central Intelligence Agency (CIA) case officers were convicted for spying for Beijing. Similarly, in 2020 two former French General Directorate for External Security (DGSE) officers were also convicted of spying for China for over ten years.[130]

China, however, does not have to rely on foreign recruited agents. Its National Intelligence Law requires "Any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public."[131] Paul Moore, a China analyst for the FBI, explained the Chinese approach. He described:

> If a beach was an espionage target, the Russians would send in a sub, frogmen would steal ashore in the dark of night and with great secrecy collect several buckets of sand and take them back to Moscow. The Americans would target the beach with satellites and produce reams of data. The Chinese would send in a thousand tourists, each assigned to collect a single grain of sand. When they returned, they would be asked to shake out their towels. And they would end up knowing more about the sand than anyone else.[132]

As an expert witness explained to the U.S. Senate Intelligence Committee, "Counterintelligence is the new counterterrorism."[133]

Cyber

Another important arrow in the quiver for China in strategic competition is the use of cyber operations. Cyber operations are defined as "the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks."[134] Cyber operations, however, can also be undertaken by non-state actors (e.g., terrorists, hacker groups) independently or in concert with a sponsor state.[135]

China has invested heavily in its ability to mount cyber operations. It has established a PLA cyber force that numbers approximately 300,000 personnel as well as "a netizen '50 Cent Army' of perhaps 2 million individuals who 'are paid a nominal fee to make comments on social media sites in favor of [PRC] propaganda."[136]

The DNI annual threat assessment stated:

> We assess that China presents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks. China's cyber pursuits and export of related technologies increase the threats of attacks against the U.S. homeland, suppression of U.S. web content that Beijing views as threatening to its control, and the expansion of technology-driven authoritarianism globally. China almost certainly is capable of launching cyber attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems. China leads the world in applying surveillance and censorship to monitor its population and repress dissent, particularly among minorities. Beijing conducts cyber intrusions that affect U.S. and non-U.S. citizens beyond its borders—such as hacking journalists—to counter perceived threats to the CCP and tailor influence efforts. China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.[137]

Significantly, the U.S. Government has recently determined that China was behind a series of hacks against key targets in its U.S. government, private companies and the country's critical infrastructure. The penetration enabled China to gain access to numerous federal agencies and major U.S. companies for months.[138] One hack attacked the Office of Personnel Management from which they stole "detailed, often highly sensitive personnel data from 21.5 million current and former U.S. officials, their spouses, and job applicants, including health, residency, employment, fingerprint, and financial data. In some cases, details from background investigations tied to the granting of security clearances—investigations that can delve deeply into individuals' mental health records, their sexual histories and proclivities, and whether a person's relatives abroad may be subject to government blackmail."[139] William Evanina, the U.S. top counterintelligence official, confided that China is "one of the leading collectors of bulk personal data around the globe, using both illegal and legal means." He explained, "Just through its cyberattacks alone, the PRC has vacuumed up the personal data of much of the American population, including data on our health, finances, travel and other sensitive information."[140]

The hacking software that was used, Aria-body, was also targeted against Australia and Southeast Asia.[141] A cybersecurity company in Israel identified Aria-body as a tool utilized by a group of hackers, known as Naikon, that has previously been traced to the PLA. Specifically, the hacking group is believed to be part of the PLA's Second Technical Reconnaissance Bureau, Unit 78020, based mainly in the southern city of Kunming and is believed to be responsible for China's cyberoperations and technological espionage in Southeast Asia and the South China Sea.[142]

The Chinese cyber capability fuels Western concerns about the Chinese company Huawei and its 5G (fifth generation of wireless internet access) aspirations. 5G will allow for much faster speeds and stable connections critical for the future of the internet. It will also be critical for the interrelation with applications of AI. However, it will require substantial investment in infrastructure such as an expansive network of antennas. Huawei is the dominant player in a shrinking pool of telecom equipment suppliers. For security, as well as the desire not to be dependent on a single, particularly potentially hostile foreign, commercial entity, the West must carefully examine long-term solutions.[143]

The summary of known PRC cyber-attacks is concerning, if not impressive. In addition to the examples already given, the PLA also hacked into Equifax's computer system allowing it to obtain full names, birth dates, Social Security numbers of 145 million Americans, as well as driver license numbers for at least 10 million Americans. PLA hackers also collected credit card numbers and other information belonging to 200,000 Americans.[144]

China has also stolen information on such sensitive technologies as the W62 Minuteman III intercontinental ballistic missile, W76 Trident C4 submarine-launched ballistic missile and the W88 Trident D5 submarine launched Ballistic missile. Additionally, the PRC stole information on cruise missile systems, stealth technology, F-16 jet engine design, trade secrets from US corporations (e.g., Ford Motor Company, General Motors), computer chip design and the development design of the F-35 fighter jet.[145]

In 2020, the U.S. Attorney General indicted four Chinese military hackers, linking large-scale data thefts from the U.S. Office of Personnel Management, Marriott hotels, Anthem Insurance, and Equifax to the Chinese government.[146] Chinese agents are also accused of hacking into Microsoft's Exchange email service allowing them to steal Western defence and commercial secrets,

as well as harassing Chinese dissidents overseas and bugging the headquarters of the African Union.[147]

Early cyber-attacks, many which were deemed "sloppy," were conducted by PLA agents. However, China's Ministry of State Security has now contracted out the work to an elite satellite network of contractors at front companies and universities that work at the direction of the ministry.[148] This approach has allowed for a degree of deniability as well as increased expertise.

Disinformation

China's view of strategic competition to gain access and influence and advance its national interest is not constrained by any boundaries. According to Major-General He Fuchu, Vice President of PLA Academy of Military Science, "The sphere of operations will be expanded from the physical domain and the information domain to the domain of consciousness; the human brain will become a new combat space. Consequently, success on the future battlefield will require achieving not only 'biological dominance' but also 'mental /cognitive dominance' and intelligence dominance." In fact, He Fuchu anticipates the development of a "new brain-control weaponry that interferes with and controls people's consciousness, thereby subverting combat styles."[149]

The PLA contends that warfare is a constant struggle that involves both the enemy and its population. It noted:

> The target of modern psychological warfare is not limited to the enemy forces as it also includes all people of the hostile country… in order to cause wrong understandings, assessments, and decisions, and shake its thinking and conviction and will of resistance to achieve the objective of defeating the enemy without fighting. It is implemented not only in wartime but also in a massive and continued scale in peacetime.[150]

A component of this approach is disinformation[151] and "hostile social manipulation," namely "the purposeful, systematic generation and dissemination of information to produce harmful social, political, and economic outcomes in a target country by affecting beliefs, attitudes, and behavior."[152] A RAND report concluded, "China is treating Taiwan as a test bed for developing attack vectors using disinformation on social media." The report notes that the PRC's use of disinformation to date has achieved mixed results primarily in the

political domain. It has also carried out disinformation operations with regard to the COVID-19 crisis. The significant take-away is that the PRC will undoubtedly launch disinformation campaigns against its adversaries in the event of a crisis or conflict. Inevitably, China will deeply embed disinformation and social media further into its military operations and utilize this capability to "shape" the environment prior to conflict or during "heated" competition.[153]

A disinformation network with ties to China used hundreds of fake social media accounts, including one belonging to a fictitious Swiss biologist, to spread an unfounded claim that the U.S. pressured scientists to blame China for the coronavirus. Within hours of the initial posting, hundreds of other accounts, some of which were created only that day, began liking, posting or linking to the post. Many of the accounts were later found to be fake, with some of the users posing as westerners and others using likely fabricated profile photos. A Facebook investigation discovered links between the accounts and a tech firm based in Chengdu, China, as well as to overseas employees of Chinese infrastructure companies. Within a week of the initial post, large media outlets in China were reporting on the claims of U.S. intimidation as if they had been made by a real scientist.[154]

This methodology has also been used by the PRC to discredit criticism of the regime. Researchers discovered an expansive network of more than 350 fake social media profiles that pushed pro-China narratives and attempted to discredit critics of the PRC. The accounts were spread across Twitter, Facebook, Instagram and YouTube. All used fake AI-generated profile pictures, while others seem to be stolen from postings in other languages.[155] China is also using part of its internal internet surveillance network to mine data from Western social media and provide its government agents with information on foreign targets.[156]

In summary, China is a highly capable and effective actor in the GPC. It utilizes all of its capabilities (i.e., economic, political, military, cyber, informational) to achieve access and influence in its pursuit of its political objectives. Although preferring to compete below the threshold of armed violence, the PRC does not hesitate to use aggressive action, including the use of its military, to deter perceived adversary assaults on its interests or to push its claims.

CHAPTER 3

Russia in the Competition Space

The Russian play book for strategic competition is little different from the Chinese approach. Historically, they have been masters of deception, using ambiguity to mask intent and operations, and operating on the cusp of detectability. They have cleverly shaped operational theatres by methods such as escalating to de-escalate, creating political leverage through limited-objective coup de main operations, using political means to achieve military objectives and vice versa. They emphasize ingenious ambiguity to cover their activities.[1] Additionally, they utilize their conventional military threat, as well as offensive cyber warfare, state-sanctioned assassinations and poisonings, political coercion, and other methods to violate the sovereignty of other nations.[2] "He [Putin] has played the great game better than anyone on the world stage," Admiral William McRaven, a former commander of USSOCOM conceded.[3]

As President Joe Biden stated, Russia remains determined to enhance its global influence and play a disruptive role on the world stage.[4] Much like the China, they have utilized multiple levers of national power and other means. Specifically:

Political

Unlike China, Russia actively seeks to undermine democracy and sway voters, to a very destructive end, while the PRC is more focused on seeking to "shape" perceptions to advance its policy objectives.[5] Once Russia stabilized its own domestic issues after the disintegration of the Soviet Union, it quickly returned to the competition space seeking to weaken the U.S. and its allies, as well as the international norms in place.[6] There is ample, strong circumstantial evidence that Russia interfered with, or at a minimum attempted to influence, Britain's Brexit referendum and the U.S. presidential election in 2016, the Catalonian vote for independence from Spain in 2017, the German federal elections and U.S. midterm elections in 2018, as well as Montenegro's entry into NATO in 2018, the rise of Far Right and Far Left

parties from Greece and Hungary to Austria, Sweden and France.[7] Quite simply, as the 2022 DNI annual threat assessment expounded;

> Russia presents one of the most serious foreign influence threats to the United States, using its intelligence services, proxies, and wide-ranging influence tools to try to divide Western alliances, and increase its sway around the world, while attempting to undermine U.S. global standing, amplify discord inside the United States, and influence U.S. voters and decision-making.[8]

In essence, as a U.S. DoD publication concluded, "Russia exploits the conditions of the operational environment to achieve its objectives by fracturing alliances, partnerships, and resolve, particularly through the effective use of information in undermining friendly will."[9] Russia's approach embraces low levels of violence and attempts to avoid direct confrontation between adversaries. Russia often threatens escalation to achieve its political objectives and deter retaliation. Consistently, Russia attempts to engage and defeat an adversary by:

- undermining territorial integrity,
- subverting internal political cohesion, and
- disrupting a target's economy.[10]

To achieve these outcomes Russia uses its own, as well as third-party media outlets, cyber hackers, business interests, non-governmental organizations (NGOs) and government-organized NGOs, Russian-speaking communities abroad and sponsorship of political parties to undermine democratic processes and decision-making in individual countries, the EU and NATO.[11]

Nowhere is this more apparent than in Russia's international relations, particularly its challenging of the status quo in Africa by using insecurity, instability and diplomatic disputes with Western powers as a springboard to expand its presence on that continent. Russia has been building key military alliances and improving its public image in states such as Libya, Chad, Mali, Burkina Faso, Nigeria, Mauritania, Ethiopia, Sudan, CAR, Mozambique and Angola. Key to these inroads was the African discontent with Western diplomatic partnerships, which place emphasis on human rights and fiscal responsibilities. Conversely, Russia pays scant attention to human rights offences or corruption. Additionally, it has provided food and medical assistance, as well as its growing commercial, economic and military support across the continent.[12]

As analysts have observed, "Developing countries now have a Russian option to provide them with foreign internal defense, security force assistance, or counter-terrorism capabilities against irregular threats." They noted, "such a choice is especially appealing to authoritarian or corrupt regimes who want a military answer to an irregular threat but have limited interest in the oversight and pressure to reform that comes from Western support.[13] The net result is that Russia has made significant inroads in displacing Western influence and access in a myriad of African states.

Economic

Although not capable of wielding as much economic clout as China, Russia also uses economic leverage to influence, bully and press other states to bend to its will. The export of energy to Europe is often used to pressure, as well as divide, European nations. For example, Russia cut gas supplies and raised prices to European customers such as Bulgaria, Germany, Italy, the Netherlands, Denmark, Finland and Poland as a result of their support to Ukraine since Moscow's 2022 invasion.[14] It has also blockaded Ukrainian ports, thus restricting grain exports to developing nations creating an artificial food shortage in some of the most destitute countries in the world. Additionally, Russia threatened to boycott Czechoslovakian beer and prior to its invasion was already putting unremitting economic pressure on Ukraine by raising gas prices and interfering with cross-border trade.[15]

Similar to China, Russia appoints influential Western businessmen and politicians on the boards of key Russian companies, as well as paying extravagant consulting fees. This approach creates advocates for Russian policies, as well as creating reluctance to forcefully push back at Russian breaches of international norms and regulations. As one researcher observed, "the Western preference is to view Russia's elites as a collection of entrepreneurs who want to participate in the free market alongside their Western peers." However, he also explained:

> In actuality, what has emerged in Russia in the last decade is anything but a free market—something more akin to a statewide organized crime syndicate. The central government controls the conditions for international trade and is in turn backed by those who profit from this arrangement. Low-level crime and corruption are allowed to flourish as long as the government is not targeted and as long as whatever services are required (criminal, cyber, paramilitary) are at the government's disposal when needed. The West maintains

a significant economic advantage over Russia, so Putin has chosen to forego direct competition in this arena, opting instead for local bilateral arrangements that provide Moscow with economic leverage over certain neighbors.[16]

Military / para-military

As was witnessed in the Ukraine in 2014, as well as in 2022, Russia wields its military cudgel with impressive finesse. Whether deploying "little green men," "peace stabilization forces," intimidating military build-up on the borders of neighbouring states, escalating forces to de-escalate a situation, or outright military invasion such as in Georgia in 2008 or Ukraine in 2022, the military is an important tool for Russia in the competition space. For this reason, whether as a deterrent, threat or enhanced capability, Russia has pushed advancements in hypersonic missiles, electromagnetic pulse weapons, thermobaric (heat and blast) munitions, and other specialized systems.[17]

Russia is also upgrading its bombers, intercontinental ballistic missiles, submarine launched ballistic missiles and warning systems. Admiral Charles Richard, head of the U.S. Strategic Command, opined Russia is restructuring its "entire strategic force structure." He explained that Moscow was building hypersonic weapons, as well as nuclear-powered torpedoes.[18]

The array of weaponry, if described capability can be believed, is impressive. For example, the Kh-47M2 Kinzhal is a Russian nuclear-capable hypersonic aero-ballistic air-to-surface missile that can hit a target up to 2,000 km away and can fly faster than 6,000 km/h.[19] The Russians have also tested a missile that struck a defunct space satellite, which indicates Moscow's proclivity to further militarize space. The satellite explosion created approximately 1,500 pieces of trackable space debris and hundreds of thousands of smaller pieces.[20]

In addition, Russia also announced the deployment of a new generation of powerful laser weapons in Ukraine that allow them "to burn up drones." President Vladimir Putin specifically mentioned the Peresvet laser and its ability to blind satellites up to 1,500 km above the Earth. In one test, the Persvet allegedly burned up a drone five km away in five seconds.[21]

Finally, Russia is also investigating the possibility of arming its fleet with loitering munitions, specifically kamikaze drones that can quickly deploy from ships.[22]

To complement the deployment of new weapons, Russia's military also formed twenty new units in the country's west in 2021 to counter what it claims is

a growing threat from NATO. The Russian Defence Minister explained that these new units commissioned about 2,000 new pieces of weaponry as well.[23] Russia has also conducted a series of annual strategic exercises such as Vostok 2018, Tsentr 2019 and Grom 2019. All were designed to message various audiences (internal and external). For instance, Vostok 2018 aimed to demonstrate the enhanced "operational art," performance and capabilities of the Russian military as one of the segments of power that supports Russia's geopolitical, military and political objectives. The theme of international partnerships with such associates as China and Belarus was reinforced during Tsentr 2019. Finally, Grom 2019 was a demonstration of Russia's sovereign nuclear might, intended to remind all of Russia's status as a nuclear superpower. Significantly, analysts assess that Russia is planning to blend its conventional forces with nuclear forces in future conflicts. They believe that Russia may be able to deploy a mix of high-yield, medium-yield and low-yield warheads integrated with cyber, space and non-nuclear forces.[24]

The 2022 military invasion of Ukraine is yet the latest example of how Russia leverages its military to achieve its political objectives. In 2014, Russia expertly carved out both the Crimea and the Eastern Donbas region. In a matter of weeks, without a shot being fired, relying on "little green men," as well as cyber, disinformation and psychological warfare, the Ukrainian military was broken and all of their 190 bases had surrendered. Russia had less than 10,000 assault troops stationed in Crimea, supported by a few battalions of airborne troops and Spetsnaz commandos, arrayed against 16,000 Ukrainian military personnel. Yet, armed groups, believed to be Russian SOF blocked Ukrainian troops in their bases and seized the Crimean Parliament.[25] One analyst observed, "this well-armed and highly professional unit turned out to be the first deployment of operators from KSO [Russia's new Special Operations Command: Komanda spetsialnogo naznacheniya], supported by the elements of the VDV's [Airborne] 45th opSn [Independent Spetsnaz Regiment]."[26] The KSO operators subsequently fortified the building while well-organized but unarmed pro-Russian protesters assembled outside to prevent local law enforcement forces from seizing the building.

Since then, in the Spring of 2021, Russian-conducted field training exercises in Crimea involved more than 60 ships, over 10,000 troops, around 200 aircraft and approximately 1,200 military vehicles.[27] More recently, Russia increased its pressure on Ukraine amassing what American intelligence sources estimated to be 169,000-190,000 troops along the border, in Belarus, as well as in the Crimea.[28] Although denying any intention of invading the Ukraine, the continuing build-up fixated the U.S. and NATO on the

issue. Putin clearly attempted to use the build-up as a pressure tactic to force the West to cede to his will.

Prior to February 2022, unsure whether President Putin was playing a high-stakes poker match, Western diplomats both threatened Russia and scurried to Moscow to negotiate with Putin to avoid war. Consistent with the Russian "playbook" disinformation campaigns and "false flag" events to shape possible invasion have also been played out. The United States acquired intelligence about a Russian plan to fabricate a pretext for an invasion of Ukraine using a faked video that would build on recent disinformation campaigns that stated the U.S. had assembled chemical warfare factories in Ukraine. The plan, which the U.S. spoilt by making it public, involved the staging and filming of a fabricated attack by the Ukrainian military either on Russian territory or against Russian-speaking people in eastern Ukraine. The Russians then intended to use the video to accuse Ukraine of genocide against Russian-speaking people. This outrage would then justify an attack by the Russians, or equally, provide the separatist leaders in the Donbas region to invite a Russian intervention.[29]

The failed chemical weapon false flag plan was not the only effort. Separatist leaders in the Donbas also accused the Ukraine of planning an invasion of the rebel held territory. Additionally, Russia accused the Ukraine of breaking the ceasefire agreement by shelling rebel held territory, as well as Russia itself. It also conducted "provocative firing" along the 250 km frontline, as well as carrying out suspected sabotage attacks in the Ukraine itself.[30] On 21 February 2022, President Putin recognized the break-away territories in the Donbas region (i.e., the Donetsk and Luhansk People's Republics) and deployed Russian forces as "peacekeepers" citing Ukrainian provocations and ceasefire violations.[31] Subsequently, on 24 February, Russian forces invaded Ukraine, supported by massive cyberattacks on Ukrainian government agencies and banks, false flag operations, disinformation, mercenaries and irregular forces.[32]

Notably, and as to be expected, as Western and international reaction including crippling economic sanctions and the supply of armaments and munitions to Ukraine took hold, President Putin once again dipped into the well of military leverage and on 25 February implied any interference would trigger "such consequences that you have never encountered in your history," interpreted by most to mean the potential use of nuclear weapons. He went one

step further two days later when he ordered his military commanders to put his nuclear forces on high alert based on "aggressive statements" made by NATO.[33] A classic case of escalate to de-escalate. Once again, he has achieved a desired political objective by wielding, as well as threatening to escalate the use of, military force in the competition space.

Russia has also deployed its military and proxies internationally (e.g., Syria, Libya, CAR, Sudan) to expand its influence and access. For instance, the CAR solicited the assistance of Russia in 2017 to reclaim its control of its diamond trade from the rebels, as well as to end its insurgency. Russian trainers, or more accurately mercenaries, were deployed, as well as Russian bodyguards to protect the President and a former spy to act as the presidential security advisor.[34]

Moreover, Russia's return to Africa in 2017 was only the beginning. Utilizing the Wagner Group, a public-private paramilitary army run by Yevgeny Prigozhin, a secretive oligarch who is part of Putin's inner circle, Russia has been able to spread its influence and gain access while maintaining a degree of deniability. The Russian mercenaries of the Wagner Group have deployed in Sudan, the CAR, Madagascar, Libya, and Mozambique. Moscow's inroads are based on paramilitary security forces, natural resource extraction, and Russian manipulation of local media. In the CAR, as well as in Mali, for example, Russia's Wagner Group was able to displace French influence. In addition, in Burkina Faso, in the aftermath of the successful military coup in January 2022, supporters of the new regime thronged the streets of the country's capital waving Russian flags. In May 2022, the new junta that took control of Mali by coup in May 2021, struck a deal with the Wagner Group that required the Russians to deploy 1,000 armed mercenaries in exchange for providing access to Mali's state-owned gold mines to a Russian company said to be controlled by Prigozhin.[35]

The concept of irregular warfare is not lost on Russia. Similar to the Cold War, Russia undertakes aggressive irregular campaigns against the United States and its allies to "weaken the United States" and to "drive wedges in the Western community alliance of all sorts."[36] In June 2020, U.S. intelligence officials concluded that Russian military intelligence agents, specifically from Russian Unit 29155, had offered payments to Taliban-linked militants to attack U.S. and other international forces in Afghanistan.[37]

Moscow has also leveraged special operations forces, intelligence units, PSCs, and other government agencies and NGOs to expand its influence,

build the capacity of partners and allies, and secure economic gains. Some Russian PSCs have direct or indirect links with the Russian Ministry of Defense (particularly the *Glavnoye Razvedyvatelnoye Upravlenie* (Military Intelligence Directorate (GRU)), *Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii* (Federal Security Service (FSB), *Sluzhba vneshney razvedki Rossiyskoy Federatsii* (Foreign Intelligence Service (SVR)), and the Kremlin.

In fact, between 2015 and 2021, Russia has increased its use of PSCs sevenfold (e.g., from four countries to 27). Russian PSCs are active in Africa, the Middle East, Europe, Asia, and Latin America.[38] Particularly, Russia utilizes the Wagner Group, as well as proxies as another "military" vehicle to gain access and influence in the competition space.[39] Importantly, the term "private" does not mean "independent of the state" in the Russian context. Rather, mercenaries are deployed to serve both oligarchical and state interests, which are often difficult to untangle. The Wagner Group, which maintains a close connection to the GRU, as well as to private commercial interests, is a perfect example. Although mercenaries are not necessarily given state direction, they never act counter to Moscow's interests.[40]

Russian PSCs are used as a force multiplier to achieve objectives for both government and Russia-aligned private interests while minimizing both political and military costs. Russian decision-makers utilize PSCs as a tool to support, if not prop up, friendly regimes. In many ways, Moscow uses PSC to deal with complex foreign-policy initiatives which allows for a low-risk, flexible means of interfering internationally, while maintaining plausible deniability. For example, 2,500 Wagner mercenaries served in Syria in 2015 alone.[41] Russian PSCs operate alongside and embedded with client state militaries as well as non-state armed groups in offensive combat operations. Tellingly, the command and control of Russian PSCs sometimes falls under the command and control of the Russian Ministry of Defense (MoD) or Russian intelligence agencies, or under client state governments (or aligned private interests).[42] Moreover, often there appears to be a close working relationship between Russian special operations teams and private contract groups. Interestingly, Wagner and an elite GRU Spetsnaz unit reportedly share a military base in the Russian town of Molkino.[43] Amazingly, the Wagner Group has assets deployed throughout Africa in Sudan, Libya, Zimbabwe, Angola, Madagascar, Guinea, Guinea Bissau, Mozambique, Democratic Republic of Congo and the CAR. It trains local armies, protects important persons, combats rebel and terror groups, as well as providing security over gold, diamond and uranium mines.[44]

Cyber

Cyber warfare is an important instrument for Russia in strategic competition. General Paul K. Nakasone, head of U.S. Cyber Command and the National Security Agency, asserted in 2018, "as the most technically advanced potential adversary in cyberspace, Russia is a full-scope cyber actor, employing sophisticated cyber operations tactics, techniques, and procedures against U.S. and foreign military, diplomatic, and commercial targets, as well as science and technology sectors."[45] He was not wrong. Russia has a long record of conducting devastating cyber-attacks in conjunction with other methodologies to achieve its political objectives. A U.S. Homeland Security report warned, "Russia maintains a range of offensive cyber tools that it could employ against US networks—from low-level denials-of-service to destructive attacks targeting critical infrastructure." It explained, "Russia continues to target and gain access to critical infrastructure in the United States… Russian Government cyber actors compromised US energy networks, conducting network reconnaissance and lateral movement, and collected information pertaining to industrial control systems." It added, "Russian state-sponsored cyber actors have successfully compromised routers, globally, and US state and local government networks."[46] Moreover, Russia has clearly demonstrated its capability to launch disruptive, if not destructive, cyber operations against its adversaries.

Examples abound. Russia used cyber warfare:

- in Estonia in 2007 as part of its political disagreement;[47]
- in Georgia prior to the short-term invasion in 2008;
- in 2008 to hack into the Pentagon's Secret Internet Protocol Router Network (SIPRNet);
- from 2012-2018, targeted the global energy sector in hacking campaigns that targeted thousands of computers, at hundreds of companies and organizations, in approximately 135 countries;[48]
- as part of its Ukrainian operations in 2014;
- to attack on Ukraine's electrical grid in 2015, which cut its power in the middle of winter;[49]
- to interfere in the U.S. elections in 2016;[50]
- as part of an attempt to change regimes in Montenegro in 2016;
- to conduct attacks against the World Anti-Doping Agency in 2016;

- to attack the Organization for the Prohibition of Chemical Weapons in 2018;
- to target a Saudi Arabian refinery in 2017;[51]
- to seize a U.S. State Department e-mail system to infiltrate into the computer networks of human rights groups and other organizations that had been known to be critical of President Putin;
- to attack the U.S. software company Kaseya, with a crippling ransomware attack demanding $50 million;
- to hack the Republican National Committee in 2021; and
- in Ukraine prior to its invasion in February 2022.[52]

The Russian cyber-attacks are particularly concerning. Between 2012 and 2017, the U.S. Justice Department reported that three Russian intelligence agents and accomplices targeted the energy sector, hacking hundreds of companies and organizations around the world. Russian hackers also managed to get inside the computer network at a nuclear power company in Kansas.[53]

Additionally, the 2016 interference in the U.S. presidential election is particularly telling as well. Dan Coats, then-Director of National Intelligence, explained, "Russia conducted an unprecedented influence campaign to interfere in the U.S. electoral and political process."[54] Special Counsel Robert Mueller as well as investigations by the Senate Select Committee on Intelligence concluded that Units 26165 and 74455 were directly responsible for Russia's "hack-and-leak" operation.

These investigations discovered that Unit 74455 was responsible for releasing tens of thousands of the stolen documents through various fictitious online personas and in coordination with WikiLeaks. Beginning in March 2016, the GRU conducted an extensive spearphishing and malware campaign to hack the networks and email accounts of the Democratic National Committee, the Democratic Congressional Campaign Committee, and the Clinton campaign, including the email account of campaign chairperson John Podesta. The GRU stole tens of thousands of documents and emails from these accounts until at least September 2016. They then coordinated the release of the stolen information to interfere in the 2016 election. According to the Senate Investigation, the GRU used aliases to communicate with WikiLeaks to transmit stolen documents, which WikiLeaks then released for "maximum political impact" starting on the eve of the 2016 Democratic National Convention.[55]

Additionally, both American and British security agencies have disclosed the invasive methods that Russian intelligence has utilized to attempt to penetrate the cloud services of hundreds of government agencies, energy companies and other organizations. An advisory released by the U.S. National Security Agency acknowledged that the attacks were linked to the Russian GRU. Experts contend that the campaign is likely ongoing.[56]

Disinformation

Integral to Russia's approach to competing in the international arena is its utilization of disinformation.[57] Jānis Bērziņš cautioned that "The new Russian view of modern warfare is based on the idea the main battlespace is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare, in order to achieve superiority in troops and weapons control, morally and psychologically depressing the enemy's armed forces personnel and civil population."[58] Key to this approach is the concept of reflexive control, which entails disseminating information that motivates the target to make a predetermined decision. In essence, "the goal is to manipulate information to compel an enemy to take desired actions. The conditions for using reflexive control require strong target audience analysis, which enables anticipating enemy action and using harsh forms of pressure that take social elements as well as intellectual, psychological, theological, and ideological factors into account."[59]

The Russians utilized disinformation throughout the Cold War to sow division and distrust of democracy in Western societies. However, with the advent of social media, Russia has been able to weaponize disinformation to undreamt levels. Its disinformation campaigns have infiltrated the mainstream political discourse, news, media and especially social media. A report from the Global Engagement Center at the U.S. Department of State revealed Russia's disinformation program consists of five pillars, namely, official government communications, state-funded global messaging, cultivation of proxy sources, weaponization of social media, and cyber-enabled disinformation.[60]

A Facebook report revealed that Russia "remains the largest peddler of disinformation around the world" and that it "had run disinformation campaigns in more than 50 countries since 2017."[61] One researcher asserted, "The internet, however, has allowed these adversaries to weaponize and tailor their disinformation campaigns against specific audiences and obfuscate their roles like never before."[62] As a result, analysts have explained:

> The effectiveness of information, misinformation, and disinformation is the cornerstone of their [Russian] influence strategy. It has proven effective and low-cost, both politically and economically. The key aspect of Russia's nonlinear warfare is centered around various methods of subversion to demoralize and cast doubt in a political and social system. Utilizing the preexisting divisions in a society creates opportunities for Moscow to stoke internal flames, seizing the strategic advantage and erode a targeted nation's legitimacy and influence.[63]

In essence, the focus of Russia's disinformation campaign in the West is designed to diminish the trust, credibility and legitimacy of target governments and politicians, democratic institutions, as well as the free media. These efforts are meant destabilize and create internal turmoil in Western nations, as well as demonstrating that the Western liberal democracies are dysfunctional and in no way represent a superior system to the Kremlin.[64] The disinformation campaigns are also devised to weaken, if not undermine and spoil U.S. relations with its allies and other friendly states.[65]

Once again, examples abound. Russian leaders launched Operation Infektion 1983 as an attempt to place blame on the origins of HIV/AIDS on a U.S. bioweapon laboratory in Fort Detrick, Maryland. World media and Western newspapers widely reported this AIDS disinformation. By late 1987, the story had circulated in media of 80 countries appearing in over 200 periodicals in 25 languages.[66]

In 2014, well before the COVID pandemic, a Kremlin campaign urged parents not to vaccinate their children. The impact was such that in 2019, the WHO proclaimed that "vaccine hesitancy," which the Moscow disinformation campaign contributed to, had become a leading global health risk.

As the COVID crisis began to emerge in early 2020, Russian state propagandists quickly exploited the divisive potential of the pandemic. Russian government-controlled and aligned media have promulgated narratives that contain disinformation and conspiracy theories about COVID, vaccines, dangerous treatments and government health protocols that contributed to the anti-vaccination movements and spurred vaccine hesitancy among the public. Researchers have noted that Canadian anti-vaccination and anti-mask groups have shared Russian state media narratives and conspiracies about the pandemic, which served to legitimize and fuel pandemic-related protests.[67]

Subsequently, in March 2020, the EU's External Action Service issued a caution with regard to the threat of Russian COVID disinformation. The warning stated that Russia was engaging in a "significant disinformation campaign" and that "the overarching aim of Kremlin disinformation is to aggravate the public health crisis in Western countries…in line with the Kremlin's broader strategy to subvert European society."[68]

In 2021, researchers at the Digital Forensic Lab, run by the U.S.-based thinktank the Atlantic Council, exposed how pro-Russian Facebook pages in Mali coordinated support for anti-democracy protests, as well as the Wagner Group, which was subsequently invited into the country after the military coup. Similarly, the same investigators revealed that pro-Russian content spread on Facebook in West Africa in the months preceding the military takeover in Burkina Faso in January 2022. Mere hours after the coup, demonstrators in the country's capital, Ouagadougou, chanted pro-Russian and anti-French slogans.[69]

The 2022 war in Ukraine is but the latest example of how Russia uses disinformation to attempt to achieve its objectives in strategic competition. Concerned with international, but particularly domestic public opinion, President Putin directed that a massive disinformation campaign be launched to justify is invasion of Ukraine. Claims that Ukraine was led by neo-Nazis, that the U.S. had bioweapon laboratories in Ukraine, and that the Ukraine was developing chemical weapons to use against Russia quickly spread on-line and in the media. Putin also blocked all access to Western social media in Russia.[70]

As the war progressed, Russian disinformation narratives proliferating online attempted to spread false claims that Western volunteers (labelled mercenaries) captured by Russian forces were evidence of NATO's direct involvement in the war. This Russian disinformation was intended to prove that the West was supporting "Ukrainian Nazis" and that NATO was now "directly" involved in the conflict. This narrative was important to convince Russia's domestic population of the rationale for the war. Importantly, these false claims also gained traction overseas, including throughout the Middle East and Africa.[71]

Additionally, Moscow also circulated several deep fakes on Facebook and Reddit, the most prominent was that of Ukrainian President Volodymyr Zelensky calling on Ukrainians to surrender. Another was of a supposed Ukrainian teacher hailing Putin as a saviour.[72]

The Russian disinformation also targeted other countries in an attempt to sow support for the Russian invasion. On March 3, the day following India's, as well as 34 other countries, refusal to condemn Russia's invasion of Ukraine in a United Nations vote, the hashtags "IStandWithPutin" and "IStandWith Russia" began trending on Twitter in India. The hashtags, were propelled by tweets lauding President Putin for opposing the U.S. and "standing against the West's hypocrisy." The tweetstorm was not a spontaneous show of support. Researchers uncovered evidence that the hashtags were boosted by networks of fake or hacked accounts. Most were created very recently and were coordinated with each other to artificially amplify the pro-Russian hashtags.[73]

The methodology was similar to what transpired in the days before the Russian invasion of Ukraine. At that time a series of hashtags also began to emerge on social media that stated #IstandwithPutin and #IstandwithRussia. As the invasion commenced, these hashtags began to trend on Twitter.[74]

Russian Playbook

Russia has demonstrated that it is very effective at utilizing sub-threshold methodologies to achieve its strategic objectives. Jānis Bērziņš identified the Russian playbook as following eight distinct phases that allow the Kremlin to achieve political objectives without triggering too adverse a reaction from the West and international community. These are:

Phase One: 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).

Phase Two: special operations to mislead political and military leaders by coordinated measures carried out by diplomatic channels, media, and top government and military agencies by leaking false data, orders, directives, and instructions.

Phase Three: intimidation, deceiving, and bribing government and military officers, with the objective of making them abandon their service duties.

Phase Four: destabilizing propaganda to increase discontent among the population, boosted by the arrival of Russian bands of militants, escalating subversion.

Phase Five: 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.

Phase Six: commencement of military action, immediately preceded by large-scale reconnaissance and subversive missions. All types, forms, methods, and forces including special operations forces, space, radio, radio engineering, electronic, diplomatic and secret service intelligence, and industrial espionage.

Phase Seven: combination of targeted information operation, electronic warfare operation, aerospace operation, and continuous air force harassment combined with the use of high precision weapons launched from various platforms (long-range artillery and weapons based on new physical principles including microwaves, radiation, and non-lethal biological weapons).

Phase Eight: 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 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.[75]

Professor Alexander Lanoszka boils down the Russia pattern of attack in a similar, but more succinct manner. He noted that the Russia approach to strategic competition includes:

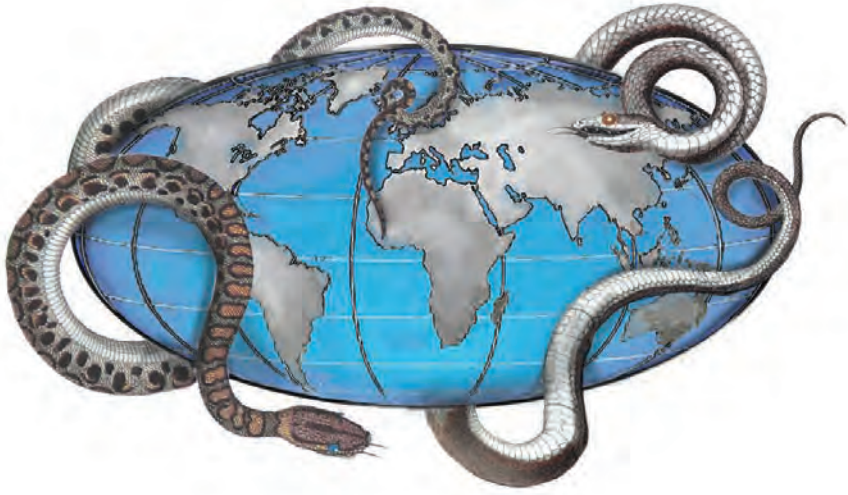
- Propaganda to dampen the target's popular support and increase discontent;
- Espionage to gain intelligence that confers a bargaining advantage or spreads false information about belligerent activities and intent;
- Agitation to create dissension and discord;
- Criminal discord for hit-and-run attacks, cyberattacks, sabotage, and kidnapping;
- Fifth columns: covert groups embedded in the population to agitate or wait for hostilities to break out;
- Insert unmarked soldiers to establish and operate checkpoints, occupy buildings, seize military assets, and clear an area ahead of an overt military operation; and

- Border skirmishes: short of military confrontation used to probe target's weaknesses and sap its resources.[76]

And, finally, intelligence analyst Guido Torres, explained that the Russian "non-linear" warfare, or in other words, preferred method of strategic competition can be described by the following indicators:

- Sudden spike in political unrest (organized online protest using trolls and bots;
- Increased violent acts to destabilize the security situation and degrade political legitimacy (e.g., terrorism, crime, mass migration);
- Cyberattacks (e.g., DDoS on government infrastructure, defacing public websites);
- An abrupt surge of intelligence and subversive operations;
- Fake news, propaganda, and disinformation substantially increase:
    - An exponential rise in social media posts against the current political party;
    - Increase in articles related to lack of security, political turmoil, corruption, and socioeconomic inequality; and
    - Russian state-run media (*RT Español* and *Sputnik Mundo*) amplify disinformation;
- Deployment of Russian special forces or mercenaries in the region; and
- Direct or indirect support for an opposition candidate that would be critical of the U.S.[77]

Similar to the Chinese, Russia has demonstrated itself to be a savvy, if not wily, player in the strategic competition space. One major difference, however, is the Russian proclivity to use military force, as it lacks the economic muscle of China. Although, the 2022 invasion of Ukraine has shown the Russian military modernization to have been highly over-rated, the fact that Russia's strength is rooted to a foundation of nuclear capability means that Russia can never be discounted or dismissed.



CHAPTER 4

Rogue Actors in the Competition Space

The current strategic competition is not played out solely by great powers. Other international actors such as rogue states (e.g., North Korea, Iran), as well as non-state actors (e.g., Islamic State or Daesh, al-Qaeda) also aggressively compete to achieve their strategic political objectives. All use a battery of asymmetric methodologies to achieve their aims from low level military operations, to cyber warfare, disinformation, criminality and terrorism.

North Korea is a graphic example. It has an extended if not colourful history of conducting wide-ranging and ever-changing provocative acts to garner attention, as well as exert political influence abroad, while avoiding a major military confrontation. Central to its objectives is the destabilization of South Korea and particularly its military alliance with the U.S. Its asymmetric, hybrid operations include terrorist attacks, involvement in transnational organized crime, localized military incidents, as well as missile or nuclear weapons tests.[1]

The use of its military is dominant in its approach to strategic competition. It has utilized both outrageous military assaults such as the shelling of Yeonpyeong Island and the torpedo sinking of the Pohang-class corvette, Republic of Korea Ship *Cheonan*, in 2010, to less overt actions such as the planting of landmines along the border patrol routes along the South Korean border in 2015. Alarmingly, it consistently holds the city of Seoul, with its millions of inhabitants only sixty kilometres from the border, hostage to its massive artillery and missile capability.

In addition, it utilizes its long-range missile and nuclear tests as a constant reminder and threat to its adversaries. Even long before its nuclear weapons were operational, the regime used them as a tool of provocation, persistently threatening to use nuclear weapons even though they were not yet usable.

Rather, its missile and nuclear weapon program were meant to frighten and deter its adversaries.[2]

North Korea has also used bullying as a tactic. It has dammed rivers close to the border allowing it to create sudden floods that killed people in South Korea and it has regularly, through its increased and improved electronic warfare capability, jammed Global Positioning System (GPS) signals that negatively affected air and naval traffic in South Korea.

North Korea has also developed its cyber capabilities to the point it has become one of the world's pre-eminent cyber players. Since the start of the new millennium, North Korea has been responsible for a myriad of cyber-attacks aimed at South Korean banks and media. Apparently, the intent was nothing more than attempting to destabilize South Korean society. It has also used cyber warfare to target both South Korea, the U.S. as well as other states, to conduct espionage and theft of sensitive and security-related data, as well as money. It conducted the digital bank robbery of $81 million USD from the Central Bank of Bangladesh in 2017, as well as the WannaCry ransomware attack that crippled hospitals in Western Europe by exploiting a vulnerability in Microsoft Windows the same year.[3]

A second prominent example of a non-great power that is actively competing in the strategic landscape is the Islamic Republic of Iran. Similar to the others, it utilizes a host of hybrid methodologies to achieve its political objectives. Beginning in 2005, Iran developed its Mosaic Doctrine, which is a forward-defence approach aimed at offsetting the power imbalance between Iran and its regional and extra-regional adversaries. The new doctrine substitutes asymmetric forms of interactions with its opponents rather than direct kinetic engagement.

Among its favourite methodologies is direct action through its own military elements or proxy forces. Many of Iran's direct action activities are conducted through its Ministry of Intelligence and Security (MOIS) or the Islamic Revolutionary Guard Corps-Quds Force. Notably, as part of their efforts to achieve domestic and external political objectives, Iranian agents and their proxies have targeted dissidents, Western opponents, as well as other perceived enemies for assassination, surveillance, and abduction in plots around the world since 1979 up until the present.[4]

Researcher Matthew Levitt has built a dataset of 98 Iranian plots carried out since the Iranian Revolution in 1979.[5] Contemporary examples abound.

In January 2018, German authorities raided several homes after weeks of surveillance confirmed they were tied to Iranian agents. These operatives were reportedly scoping out potential Israeli and Jewish targets in Germany, including the Israeli embassy and a Jewish kindergarten. In March of the same year, Albanian authorities charged two Iranian operatives with terrorism after they surveilled a venue where Iranian Nowruz (New Year) celebrations were set to begin. In June 2018, the Netherlands expelled two Iranian diplomats based at the Iranian embassy in Amsterdam following an investigation by Dutch intelligence. This action followed shortly after an Iranian Arab activist was assassinated by gunfire in Amsterdam. [6]

Additionally In February 2021, a Belgian court convicted Assadollah Assadi, an Iranian diplomat, who was actually an intelligent agent based in Vienna, of organizing the July 2018 plot to bomb the annual convention of the National Council of Resistance of Iran near Paris. Three accomplices, all Iranian-Belgian dual citizens living in Brussels, were also sentenced for their participation in the failed plot. The foiled plot, however, was just one of a number of Iranian operations conducted by Iranian operatives or their proxies. Levitt documented twenty-six such plots from 2018-2021 in such countries as Colombia, Cyprus, Denmark, Dubai, Ethiopia, France, Germany, Iraq, Israel, Kenya, the Netherlands, Scotland, Sweden, Turkey, the United Kingdom, and the United States. This campaign includes an attempted plot in July 2021 to kidnap New York-based journalist and human rights activist Masih Alinejad, a U.S.-Iranian dual citizen, and forcibly take her to Iran. Moreover, authorities have identified Iranian plots in Colombia (September 2021), Cyprus (October 2021), Kenya (November 2021), Tanzania (November 2021), and Turkey (September 2021, February 2022).[7]

Iran has outsourced some operational activities to criminal organizations to conduct surveillance and / or execute plots (e.g., assassination, abduction, bombings). In Baku, Azerbaijan, members of a crime gang were reportedly paid $150,000 each to target a Jewish school. Furthermore, Iranian students were sent abroad to study to collect intelligence and dual citizens living abroad were paid to carry out surveillance missions. For example, an Iranian was paid $300,000 to abduct an Iranian dissident and a Shi'a imam in Africa was paid around $24,000 to carry out surveillance in Nigeria.[8]

Iran has also used its conventional military capability to prosecute its political agenda, particularly maritime provocations. It has used swarms of fast small coastal vessels to swarm, charge and attempt to intimidate Western warships

in the Persian Gulf and it shot down a U.S. drone over the Strait of Hormuz.[9] Iran also conducted a series of limpet mine attacks that damaged oil tankers in 2019 and a drone attack on an Israeli-linked tanker in 2021 that resulted in the deaths of two crew members. Additionally, it has seized oil tankers in the Gulf. In 2021, Iranian operators hijacked a Panamanian-flagged asphalt tanker off the United Arab Emirates (UAE), seized a Vietnamese tanker and snatched a South Korean flagged tanker for months. More recently, on 27 May 2022, Iran's paramilitary Revolutionary Guard seized two Greek oil tankers in international waters in helicopter-launched raids. The attack was apparently in retaliation for Athens assistance in the U.S. seizure of crude oil from an Iranian-flagged tanker in the Mediterranean as a result of violating American sanctions on Iran.[10]

Another effective tactic utilized by Iran is the supplying of rockets and munitions to its proxies (i.e., Iranian affiliated militias). Not surprisingly, Iran maintains the largest ballistic and cruise missile force in the region, which it shares with its proxies. Many of these munitions have been used to carry-out a long string of rocket attacks aimed at the Green Zone in Baghdad, as well as U.S. bases in Iraq. Pentagon spokesman John Kirby described one series of rocket attacks as "a complex, coordinated, and deliberate attack." He conceded that similar attacks have been carried out by Iranian-allied Shiite militias against U.S. troops elsewhere.[11]

Iranian munitions supplied to proxies have also been used for multiple attacks against Israel, Saudi Arabia, the UAE and American forces in Syria. In fact, Israeli intelligence assessed that Iran or its proxies conducted 15 drone attacks alone in the region between February 2018 and September 2021.[12] The transfer of munitions to proxies is quite transparent. In a recent interview, the spokesman for the al-Nasser Salah al-Din Brigade, Abu Atayya, thanked the IRGC Quds Force and the Hezbollah for supplying the militant group and the "Palestinian Resistance" in its war against Israel. "Every missile, shell, or any tool of the Resistance," he proclaimed, "the hands of the Revolutionary Guards and the Quds Force have been credited with delivering, developing and supplying them to us and to all military arms facing the Zionist enemy."[13]

Terrorism is another key strategic tool Iran uses to achieve its foreign policy objectives. Indeed, Iran has been identified as the world's foremost state sponsor of terrorism, which it uses as a strategic tool to achieve its foreign policy objectives. Not surprisingly, the Quds Force and MOIS spearhead

the "Iran Threat Network," which comprises an alliance of surrogates, proxies, and partners such as Hezbollah, Hamas, and Iraqi Shi'a militants, among others. Researchers have revealed that "Iran funds, trains, and equips these terrorist organizations, in whole or in part, to use in attacks around the world" to destabilize countries throughout the Middle East and disrupt regional security.[14]

As already mentioned, proxies play a substantive role in Iran's "playbook" of strategic competition. Iran has increasingly resorted to irregular warfare as a primary means of expanding its influence. Rather than conducting attacks directly against its adversaries, Iran operates indirectly through partners and proxies.[15]

As part of this strategy, Iran deploys the IRGC and other Iranian actors (e.g., advisors, soldiers, trainers) as well as weapons to militias. These forces provide direct support, as well as other forms of assistance such as funding, logistics, recruitment, and social service provisions. For example, during the Syrian civil war, the most common forms of support were training, funding, provision of weapons, as well as participation in attacks. Overall, training was the most often provided, followed by joint attacks and funding.[16]

Analysts have noted that the U.S. "is grappling with a rapidly evolving threat from Iranian proxies in Iraq after militia forces specialized in operating more sophisticated weaponry, including armed drones, have hit some of the most sensitive American targets in attacks that evaded U.S. defenses." For instance, in the Spring of 2021, Iranian proxy militias conducted strikes using "small, explosive-laden drones that divebomb and crash into their targets in late-night attacks on Iraqi bases — including those used by the C.I.A. and U.S. Special Operations units."[17] Similarly, on 17 January 2022, Iranian-supported Houthi rebels in Yemen launched a group of armed drones on a journey of nearly 1,600 km to strike at its enemies. Houthi forces have also used Chinese-made C-801 anti-ship missiles, with a range of 42 km, for attacks on tankers in the Red Sea.[18]

RAND researchers explained that Iran's "network of nonstate actors is an essential component of the Iranian defense doctrine and one of the main tools that the regime possesses to deter adversaries, bolster its homeland defenses, increase its strategic depth, grow its regional reach and influence, and project power outside its borders."[19] The use of proxies complements other Iranian

asymmetric capabilities such as its nuclear ballistic missile program and Quds force. Taken together, Iran has been able to use these "tools" to fill the gap of its shortfalls in its conventional capabilities.

Much like China, Russia and North Korea, Iran also uses disinformation to achieve its ends. In October 2020, the Department of Justice announced the dismantling of approximately a hundred websites linked to Iran's powerful Revolutionary Guard. According to the Americans, "the sites, operating under the guise of genuine news outlets, were waging a global disinformation campaign to influence U.S. policy and push Iranian propaganda around the world."[20]

Its targets ranged beyond the United States. Iran also interfered with the UK, specifically targeting Scottish independence. British researchers have identified seven distinct areas where Iran possesses, or seeks to influence, targeted audiences to achieve its political objectives. These are:

- political networks;
- religion;
- the media;
- cultural networks;
- the Iranian diaspora;
- education and academia; and
- the fields of business and finance.[21]

As part of its attempts to influence targeted audiences, Iran also established its Al Mustafa International University, which is a religious seminar based in Qom. It opened in 2007 with the specific mission of converting non-Shiite and non-Muslim people. The university is one of Iran's main vehicles to export its revolutionary brand of Shiite Islam. Its principle is to indoctrinate and radicalize its pupils, as well as actively train Shi'a militias that Iran deployed in Syria. Despite Iranian economic hardships due to Western sanctions, it still spends $80 million per year. As such, it has trained tens of thousands of students, including numerous Latin Americans, who Iran hopes will turn the Western Hemisphere into a hotbed of anti-Americanism and a forward operating base for Iran.[22]

Finally, cyber warfare is also another recurring theme that Iran embraces to achieve its ends. According to researchers, in the space of a decade, Iran's

"cyberspace propaganda machine has become one of the spearheads of Tehran's short-of-war strategy, achieving a degree of sophistication equivalent to that of similar approaches developed by Moscow and Beijing."[23] In 2013, IRGC leaders gloated that Iran possessed "the 4th biggest cyber power among the world's cyber armies," a boast that was substantiated by the Tel-Aviv-based Institute for National Security Studies. By the end of 2018, cyber experts suspected Iran was using thousands of fake private accounts on social media platforms such as Facebook and Twitter to run a worldwide disinformation campaign. Moreover, Iran was impersonating real news organizations by using such techniques as mimicking the name, logo and visual branding of various outlets. In 2019, an EDP audit, control and security (EDPACS) report concluded that "China, Russia and Iran stand out as three of the most capable and active cyber actors." In 2022, Iran was unanimously viewed as "one of the most sophisticated and feared online actors in the world."[24]

Indeed, Iran has used its much-improved offensive cyber capabilities to target U.S. casinos, dams, the power grid, and financial institutions such as the Bank of America, JPMorgan Chase, and the New York Stock Exchange.[25] In 2018, Iran hacked into hundreds of universities and companies to steal sensitive research, proprietary data and intellectual property.[26] In June 2021, Iran attempted to hack the Boston Children's Hospital.[27] In fact, the U.S. Treasury Department targeted an Iran-based cyber company that worked with the Iranian Republican Guard Corps and MOIS to gain access to the computer systems of current and former U.S. counterintelligence agents and implant malware on their computer systems.[28]

The four brief case studies (i.e., China, Russia, North Korea and Iran) were intended to provide an overview of how just a selection of adversaries are conducting operations as part of the ageless strategic competition in the international arena. Problematic for the West is its mind frame that conflict / war is a military event. It has never been able to reconcile, unlike its opponents, that it exists in a world where, for many, conflict / competition is an ongoing process. Nonetheless, within this competitive arena, the American 2018 NDS clearly stated that the U.S. strategy was to "compete, deter, and win in this environment. The re-emergence of long-term strategic competition, rapid dispersion of technologies, and new concepts of warfare and competition that span the entire spectrum of conflict require a Joint Force structured to match this reality." Therefore, the strategy called for:

> A more lethal, resilient, and rapidly innovating Joint Force, combined with a robust constellation of allies and partners, will sustain American influence and ensure favorable balances of power that safeguard the free and open international order. Collectively, our force posture, alliance and partnership architecture, and Department modernization will provide the capabilities and agility required to prevail in conflict and preserve peace through strength.[29]

But again, the conventional military component is a small fraction of what is required. To compete on an equal footing, competition must be seen beyond the traditional warfare scenario. As Katherine Zimmerman, an analyst with the American Enterprise Institute in Washington assessed, "It's [U.S.] not losing militarily, but in the soft-power space."[30] RAND researchers have worked towards developing a better understanding of the competition space. They have defined hostile measures as "State activities other than high-order conventional or nuclear attack applied against other states at any time, and in any context, with the hostile intent of gaining advantage and reducing that state's capabilities, stability, or advantages.[31]

In the end, the prize of strategic competition is access, influence and the attainment of one's political objectives and the denial of the same to adversaries. For too long, the West has missed the nuance of strategic competition. Not so with Lieutenant General Tovo, a former Commander of U.S. Army Special Operations Command. He acknowledged:

> [Our adversaries] did what any good adversary would do. They searched for our weaknesses, and invested heavily in asymmetric techniques, Hybrid Warfare. It's an ability to get right to the heart of a nation's power, its people. And arguably, our adversaries are doing this better than we are.[32]

CHAPTER 5

Too Small to Bother - What About Canada?

When the topic of Great Power Competition, or strategic competition arises, it is easy to discount Canada or other smaller nations to be directly impacted. However, nothing could be farther from the truth. Canada, as well as other small to mid-size powers, due to their own actions, their membership to certain alliances (e.g., NATO, five-eyes, regional coalitions, etc.) and their economic and geo-political interests, willingly or unwillingly, are actors in, and influenced by, the GPC and strategic competition.

This reality has not been lost on Canadians. In a 2021 survey by Maru Public Opinion, 52 per cent of respondents viewed China as the highest security threat facing Canada, followed by Russia (42 per cent) North Korea (39 per cent) and Iran (33 per cent). Related, 55 per cent of respondents agreed that "a global war is already happening in the form of 'death by a thousand cuts,' in which some countries use 'ongoing activities to destabilize, disrupt and undermine' the sovereignty and political institutions of their adversaries." Respondents also identified that "there are different levels of attack, that can be constant, that can be ongoing, can be penetrating, and can be devastating to national security."[1]

Of note, 78 per cent of respondents believed that "the potential exists over the next five years for Canada's national security to be destabilized by a foreign threat."[2] Their concern is warranted. A report by the Task Force on National Security of the Graduate School of Public and International Affairs (GSPIA) at the University of Ottawa asserted that "China and Russia will continue to pose a significant threat to Canada through their foreign interference, disinformation, espionage, hostage diplomacy, and cyber-attacks." They note that "These activities directly threaten government institutions, but also individuals, businesses, universities, and research institutions. They

reach into our homes through the intimidation of citizens who have come to Canada to escape tyranny."[3]

The Minister of National Defence (MND), Anita Anand, simply disclosed, the world is "growing darker." The Canadian Global Affairs Institute agreed. "In this new world, Canada's geographic position no longer provides the same protection that it once did," it stated, "And in this new world, the security environment facing Canada is less secure, less predictable and more chaotic."[4]

The apprehension is real. In the case of Canada, there are currently six activities conducted by foreign actors within the realm of strategic competition that impact directly on the nation and Canadians. These are: foreign interference in national life, hostile economic measures, cyber-attacks, disinformation, espionage and Organized Crime.

Foreign Interference in National Life

Foreign interference is a substantive threat to the security of Canada. The Canadian Security Intelligence Service (CSIS) has identified that foreign entities "use direct and indirect contact to influence democratic and electoral institutions and processes by manipulating ethnocultural communities, persons in positions of authority or influence, and the media." CSIS Director David Vigneault identified "foreign interference and espionage as the greatest threats to Canada's national prosperity and national interests."[5]

The National Security Committee revealed, "states target Canada and seek to exploit the openness of our society and penetrate our fundamental institutions to meet their objectives." Not surprisingly, foreign entities target ethno-cultural communities, attempt to corrupt the political process, and try to manipulate the media and as well as academic institutions.[6] Moreover, a report for Public Safety Canada by Clairvoyance Cyber Corp in 2019, concluded, "hostile military and intelligence forces are targeting Canada in a new 'sophisticated, multifaceted' type of warfare using a range of tools from criminal gangs to cyber-hackers to high-tech companies such as Huawei and China Telecom." The report assessed that state-sponsored cybercrime could be costing Canada an estimated $100 billion per year.[7]

The CSIS director conceded that China in particular, "presents a direct threat to our national security and sovereignty."[8] This admission was not startling. After all, China has established a sophisticated network in this country

to access and if required harass people of Chinese ethnicity and Uyghur- and Tibetan-Canadians, as well as to disseminate disinformation, distort information in the media, influence politicians, as well as form partnerships with universities to secure intellectual property. As noted in Chapter 2, China utilizes influence operations to entice politicians and business leaders through all-expense-paid trips and lucrative investment projects to become sympathetic, if not supportive of China's interests.[9]

CSIS is dully concerned with Chinese efforts, as well as those of its agents of influence to covertly cultivate relations with elected officials to gain sway over parliamentary debates and government decision-making. For instance, in June 2021, 33 Canadian senators voted to defeat a motion decrying China's treatment of Uyghur Muslims as a genocide. All faced criticism, but Senator Yuen Pau Woo, leader of the Independent Senators Group, was specifically blasted as a "stooge of China's communist regime." In fact, some charged that "By claiming Meng [Wanzhou] was 'taken hostage' @yuenpauwoo has violated his oath as a Canadian senator and should resign." Canadian politicians have argued that "Mouthpieces for foreign propaganda … should have no place in Canada's Parliament. They also accused Woo "being unabashedly 'Beijing friendly,' a mouthpiece and lobbyist for the Communist Party of China, even though he points out he's 'three generations removed from the mainland (China).'"[10]

CSIS has also reported that China is also known to harass and intimidate critics of Beijing, particularly in the Canadian-Chinese community. In fact, Canadian officials have alleged that the Overseas Chinese Affairs Office (OCAO) was tasked with "influencing or manipulating" community members, and using "coercive tactics" against dissidents and minorities. "This involves intimidation of OC (Overseas Chinese) at every level of society."[11]

In addition, China attempts to control Chinese-language media, "thereby undermining the free and independent media in Canada." McGill University researchers Sze-Fung Lee and Benjamin Fung published an article stating a disinformation campaign against a Conservative Party candidate during the 2021 election demonstrates how hostile foreign actors could use propaganda tactics to interfere with Canada's political system. Former B.C. MP Kenny Chiu proposed a similar mechanism during the campaign. Mr. Chiu's proposal was condemned on Chinese-language social media, with claims it would "suppress the Chinese community" in Canada. The comments were disseminated

on apps and websites widely used by Canadians of Chinese origin, who make up about half of his riding's population. The Conservatives believe the MP lost his seat because of disinformation attacks.[12]

Their concerns are not mere paranoia. The Atlantic Council's Forensic Research Lab and the Canadian NGO Disinfo Watch analyzed the September 2021 election. Their deductions match The Conservative Party's allegations. Atlantic Council's researchers concluded, "China-linked actors took an active role in seeking to influence the September 20, 2021 parliamentary election in Canada, displaying signs of a coordinated campaign to influence behaviour among the Chinese diaspora voting in the election." What concerned the PRC was the Conservatives' proposal for a foreign agents registration law along the lines of the Australian model. As a result, Chinese-language media, as well as numerous China-based social media platforms, warned that the proposed law was a means of forcing Chinese-Canadians to register en masse as foreign agents for merely maintaining relations with businesses or family members back in China. As a result, the Conservatives took a beating at polls in many ridings where Chinese diaspora communities are concentrated. Their loss was not due to actual Conservative policy but rather how their policies "were distorted, misrepresented, and mischaracterized as racist and far right."[13]

Another example of Chinese infiltration to covertly shape and influence public opinion is the use of two Canadian community organizations, the Xinjiang Association of Canada and the Ontario-based Council of Newcomer Organizations, which was co-founded by a former Liberal member of parliament. In both cases, the organizations, who actually received Federal subsidies, consistently promote Beijing's narratives and their leadership invitations to visit China with all expenses covered by the PRC.[14]

The case of the "two Michaels" is yet another case of Chinese interference. Detained illegally by China on false charges of espionage, Michael Kovrig and Michael Spavor in December 2018 were held in grim detention conditions for 1,020 days. China was using them as hostage diplomacy because of the apprehension of Huawei CEO Meng Wanzhou, who was arrested by the Royal Canadian Mounted Police (RCMP) at the Vancouver Airport in response to an American extradition request for sanction-breaking violations. On 24 September 2021, Meng struck a deal with U.S. prosecutors. The same day, the U.S. extradition request was dropped and Meng flew to Shenzhen, China. Simultaneously, Kovrig and Spavor boarded a plane to return to Canada.[15]

Hostile Economic Measures

The economic cudgel is another means foreign states have used to attack Canada. China once again comes to the fore. Beijing, angry at the detention of Meng Wanzhou, aside from arresting the "two Michaels," slapped a ban on Canadian canola imports. It banned shipments from two Canadian companies, Viterra and Richardson International, in March 2019, and China introduced a more aggressive regime of inspections, as well as slowing trade with other Canadian shippers. Moreover, when Canada attempted to take the issue to the World Trade Organization for dispute resolution, China blocked the move. Beijing's economic action in this case alone is estimated to have cost Canada's canola industry approximately $2 billion due to lost sales and lowered prices.[16]

China also retaliated by effectively quashing a deal for Canada to test and produce a Chinese-made COVID-19 vaccine. The decision cost the Canadian government more than a quarter-million dollars. The National Research Council (NRC) paid Dalhousie University $253,997 to conduct a clinical trial of the CanSino Biologics vaccine, however, the trial was cancelled before any patients were actually treated. The partnership was terminated when Chinese Customs officials refused to allow any of the vaccine to be shipped to Canada. This action was also tied to the diplomatic feud over Canada's arrest of Meng Wanzhou.[17]

Cyber-attacks

The use of cyber warfare has become a mainstay of strategic competition (as well as criminality). The National Cyber Threat Assessment 2022 revealed that "While cybercrime is the most likely threat, the state sponsored programs of China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada. State-sponsored cyber activity is generally the most sophisticated threat to Canadians and Canadian organizations."[18]

CSIS has confirmed that "Canadian organizations are the victims of thousands of cyberattacks every single day, and that number is only going up." CSIS Assistant Director, Cherie Henderson, revealed that "Canada suffers of thousands of cyber threat attacks on a daily basis all across the country and numerous organizations are under that attack." The Communications Security Establishment (CSE) disclosed that there had been 235 known ransomware attacks against Canadians in 2021, with more than half against critical infrastructure.[19]

One researcher noted that there are between two to seven billion cyber-attacks of varying degrees of maliciousness every day. [20] In 2011, China hacked into the Finance Department, Treasury Board, and Defence Research and Development Canada. The attacks effectively forced the temporary shut-down of government servers.[21] These intrusions were not isolated incidents. A CSIS report revealed that there is a higher frequency of cyber-attacks being directed toward Canada than ever before. The report asserted that "espionage and foreign interference activity at levels not seen since the Cold War" and that those attacks were conducted mostly by Chinese and Russian-backed actors.[22]

The CSE reached similar conclusions. CSE assessed that the number and sophistication of cyber threat actors are increasing. In its annual report, CSE revealed it provided assistance to the Government of Canada or its critical infrastructure partners 2,206 times, including 84 incidents "affecting Canada's health sector."[23] CSE concluded that "state-sponsored programs from China, Russia, Iran and North Korea pose the greatest strategic threat to Canada, and that state-sponsored actors are likely attempting to develop cyber capabilities to disrupt Canadian critical infrastructure." It emphasized that those countries have all demonstrated an intent to develop cyber-attack capabilities against industrial control systems linked to critical infrastructure. It also warned that state-sponsored actors will continue to conduct commercial espionage against businesses, academic and government to steal intellectual property and information. Additionally, CSE asserted that online foreign influence campaigns continue and that they are not limited to major political events such as elections. Finally, it warned that cyber criminals will continue to target Canadian institutions and businesses in ransom-ware attacks.[24]

Both CSIS and CSE reporting affirm that China and Russia, as well as other entities, are conducting cyber and human espionage that targets individuals, institutions and corporations in Canada. The intent appears to be the ability to shape and / or control Canada's political discourse, as well as to steal economic and trade secrets from corporations and personal data from individuals. Experts note that the threat will only increase with the advent of 5G networks and densely populated "smart cities." Clairvoyance Cyber Corporation CEO Dave McMahon, stresses that "Hostile intelligence services and militaries will continue to exploit, interfere with and influence Canadian interests domestically and abroad, using cyber as part of a broader Hybrid

Warfare campaign," He insists "5G-connected smart cities intertwined with emerging technologies such as artificial intelligence and quantum computing will become battlefields in a new type of military conflict." He added, "city-dwellers interconnected through mobile technologies will provide the most target-rich environment for spying ever." Concernedly, McMahon stated that "China Telecom, a state-owned telecommunications entity, has systematically diverted Canadian Internet traffic … through its own network to facilitate espionage and targeting."[25]

Due to concerns of foreign cyber penetration, the Canadian Government finally announced on 19 May 2022, that it would prohibit "Canadian telecommunications service providers from deploying Huawei and ZTE products and services in their 5G networks" because of its concerns that those corporations "could be compelled to comply with extrajudicial directions from foreign governments in ways that would conflict with Canadian laws or would be detrimental to Canadian interests."[26]

Disinformation

Not surprisingly, Canada is not immune from foreign actors targeting the country with disinformation. A Public Safety Canada report warned that China will attempt to control Canadians through disinformation, media manipulation, psychological warfare and legal warfare.[27] CSIS has cautioned that "In particular, PRC media influence activities in Canada have become normalized." Quite simply, "Chinese-language media outlets operating in Canada and members of the Chinese-Canadian community are primary targets of PRC-directed foreign influenced activities." CSIS spokesperson John Townsend explained that "foreign states target both mainstream media outlets [e.g., print publications, radio and television programs] as well as non-traditional online outlets and social media channels in order to shape public opinion, debate, and covertly influence participation in the democratic process."[28]

For instance, one PRC cartoon campaign depicted Prime Minister Justin Trudeau "sitting on what appears to be the skulls of Indigenous people, grave stones in the background. 'We stole your land, we killed your men, we buried your child (sic),' says the smirking Trudeau character as vultures circle behind him. 'Let's reconcile.'" The message was subsequently retweeted by both a Chinese diplomat and Hu Xijin, editor in chief of *Global Times*, a Chinese Communist Party newspaper with an active online presence.[29] The

attack was similar to a doctored photo posted by a Chinese Foreign Ministry official that appeared to show an Australian soldier slitting the throat of an Afghan child, which sparked outrage in Australia.

Russia and other adversaries are no different. In 2017, during the Canadian military's deployment in Latvia, troops were subject to a variety of disinformation campaigns ranging from stories about Canadians being accommodated in luxury apartments at taxpayers' expense, to images that purported to show them littering, all in an effort to sow distrust in NATO's presence. More recently, over the course of the pandemic, Russian state media, and platforms aligned with it, published and amplified narratives that questioned the existence of COVID-19, along with the legitimacy of Canadian public health protocols. "A lot of it targets our own democracies," one researcher explained, "to erode our trust in our democratic institutions, our elected officials," he said.[30]

With the 2022 Russian invasion of Ukraine, the disinformation campaigns continued. Researchers identified clusters and main influencers in Canada and abroad who were promoting pro-Russian narratives. They discovered that in "the Canadian Twitter ecosystem" discussions on the war, approximately 25 per cent of the accounts were spreading pro-Russian talking points. Some accounts were "Trojan horses," with some Canadians unaware the pro-Putin narratives trace their origins back to Russia, China or right-wing influencers in the U.S. Additionally, many of the tweets in pro-Russian social media conversations also expressed mistrust of institutions and "a specific mistrust of Canada's Liberal government, and particularly of Prime Minister Trudeau." Researchers concluded that "foreign interference in the Canadian information space is now so pervasive it is sowing distrust in Canada's democratic institutions, including the federal government and mainstream media." Furthermore, they noted that "social media has more and more been able to shape people's view. It weakens our democratic resiliency and it creates dissent and erodes trust in institutions."[31]

Espionage

The Public Safety Canada report affirmed that foreign entities, particularly China and Russia are "conducting cyber and human espionage that targets individuals, institutions and corporations in Canada."[32] State-sponsored espionage in Canada is conducted both in the cyber and traditional human

domains. Foreign entities seek to exploit social and economic conditions, which have been especially exacerbated during the Covid-19 pandemic.

The challenge to counter the espionage is daunting. Foreign threat actors, such as the Chinese, use liberal Western democratic freedoms to embed themselves into the target society. For example, the Chinese government's OCAO has been identified as being involved in espionage that harms Canada's interests. Beijing and the OCAO insist there is nothing nefarious about its presence or mandate. They contend "the united front led by the Communist Party of China is to unite people's hearts and minds, gather strength, actively promote harmony in relations among political parties, ethnic groups, religions, classes and compatriots at home and abroad … to achieve national prosperity, national rejuvenation and people's happiness." In foreign relations, it defended, the party has "always advocated tolerance and mutual appreciation among different civilizations in the world." As for the OCAO specifically, Beijing maintains that it is designed to provide support to members of the Chinese diaspora.[33]

The RCMP and CSIS disagree. They argue the OCAO is designed to influence and monitor Chinese Canadians. Although both agencies continually advise the government about such interference a multitude of hurdles are placed in their path. First, politicians tend to suppress the information for fear of undermining trade between the two countries and second, the actual targets are often too frightened, for themselves as well as for their relatives in China, to make a complaint. In the final analysis the real goal of OCAO as seen by Canada's security agencies is to "legitimize and protect the party's hold on power, burnish China's international image and exert its influence."[34]

Some examples of high-profile espionage include the infiltration of a Canadian lab working with the Wuhan Institute of Virology. A Chinese couple working in the Canadian lab passed information and virus samples to the Chinese facility representing a breach in both biosecurity and bio-defence.[35] CSIS also sent multiple warnings to the Canadian Space Agency (CSA) about Wanping Zheng, a former engineer accused of negotiating on behalf of a Chinese aerospace company. While Zheng was working at the agency, CSA technicians noted the presence of unauthorized software by a foreign company. They also reported at least one secure file transfer service and a messaging application that was discovered on the computer, violating internal policy. Zheng eventually resigned after 26 years with the CSA.[36]

Organized Crime

Organized crime is another tool foreign entities use in strategic competition that has had a direct impact on Canada. Researchers have found that "Chinese agents have used criminal syndicates to corrupt Canadian officials, flood Canada's streets with dangerous drugs, intimidate local Chinese communities, and buy up vast swaths of Canadian real estate."[37] Chinese agents have turned a Canadian politician and used him to launder Asian drug money; facilitated a crime boss who ran Chinese gang wars from his Vancouver home; and organized a local fentanyl super-factory capable of killing scores of Canadians.[38] Moreover, an RCMP operation code named Project Sidewinder in the late-1990s uncovered the partnership between the Chinese government and Asian criminal gangs that had worked together in drug smuggling, nuclear espionage and other criminal activities that constituted a threat to Canadian security.[39] More recently, a Public Safety Report concluded that China and Russia have no hesitation in utilizing organized crime supported by high-tech networks to target citizens and institutions in Canada.[40]

CHAPTER 6

What, If Anything, Will Change With Regard to the Security Environment?

Strategic competition started neither with the Cold War, nor with the current iteration of international skirmish between the great powers and other actors. Throughout history, empires, alliances and nation states have always competed for influence, access and advantage. The great Prussian strategist Carl von Clausewitz wrote, "Is war not just another expression of their thoughts [competing governments], another form of speech or writing. Its grammar [conduct of war], indeed, may be its own, but not its logic [policy]."[1]

So, although competition between global competitors is ageless, the context, circumstances and "grammar" of the competition has evolved into a much more complex and challenging affair. The prominent Soviet military scholar Aleksandr Svechin wrote:

> It is extraordinarily hard to predict the conditions of war. For each war it is necessary to work out a particular line for its strategic conduct. Each war is a unique case, demanding the establishment of a particular logic and not the application of some template.[2]

And, so it is with the current iteration of strategic competition. The shift ushered in by the 2018 NDS galvanized conventional military commanders. For many, if not most, it hearkened back to the "good old days" of the Cold War, which focused on large mechanized armies. In fact, former U.S. Secretary of Defense Mark Esper speaking to the U.S. Naval War College remarked that "times have changed" and he asserted that the U.S. "needed to focus on conventional war."[3]

Esper did not have difficulty in convincing his military commanders. The pivot created renewed interest in large exercises and increased funding for conventional military capability, as well as new modernized armaments. However, the key is to fully understand the competition space and balancing resources correctly. A return to a traditional warfare model mindset has clear dangers, as does ignoring the capability of current rivals and rogue states. The bias to refocusing primarily on "old school" conventional warfare could hold serious consequences.

Admiral Stavridis argued the over-dependence on military solutions, or the use of force to achieve desired political outcomes, has left the U.S. in a poor position to compete in the new "competition" battlespace.[4] This recognition is not necessarily widespread. The conventional warfare bias is in play. From May until the end of September 2019, "93 separate military exercises were held, with forces operating continuously in, above and around 29 countries." The exercises were manifestly designed to send a message to Moscow and they represented "the most intense uninterrupted set of drills since the end of the Cold War."[5]

For example, NATO Exercise Steadfast Defender 2021, rekindled Cold War memories. It had been almost four decades, not since 1986, that NATO had exercised as an alliance the complex organizational and logistical challenge of rapidly deploying personnel and equipment from North America to reinforce Europe. For over two weeks NATO warships, submarines and aircraft war-gamed methods to maintain open the sea lines of communication in the event of war in Europe.[6] In addition, NATO also conducted Defender-Europe 21, which witnessed approximately 28,000 forces participating from 26 different countries.[7]

The return to conventional-centric high-intensity conflict is simple enough to understand. It is the "bread and butter" of conventional forces. NATO is good at it. And, importantly, the consequences of losing are catastrophic. Although all countries must maintain a conventional military capability of fighting and winning its nation's war, attention must be paid to what the actual looming threat(s) is. General Joseph Votel, a former commander of both USSOCOM and Central Command (CENTCOM) lamented, "We are way too focused on conventional war and deterrence…Conventional war dominated our approach."[8] Similarly, General Charles Cleveland, a former Commander of U.S. Army Special Operations Command warned, "The United States is facing

death by a thousand cuts. We are not prepared for competition the way the Russians, Chinese, and Iranians see it."[9]

This misunderstanding, or willful blindness, to the exact nature of strategic competition is filled with risk. American diplomat George Kennan continually counselled that political warfare / strategic competition is "the perpetual rhythm of struggle, in and out of war."[10] General Sir Nick Carter, the British Chief of the Defence Staff asserted, "They [Russian and China] regard the global context as being a continuous struggle where non-military and military means are used unconstrained."[11] It is critical that the West begin to act with an analogous approach to strategic competition. As Michael Vickers, former Undersecretary of Defense for Intelligence, cautioned, "Today we face perhaps the greatest threat environment since the end of the Cold War. The further you go out, the more dangerous it gets, especially when you combine advances in technology with the rise of really capable adversaries."[12]

Kimberley Kagan the founder and president of the Institute for the Study of War agrees. She explained:

> The U.S. is falling behind in this intellectual race perhaps even more than in the technological race. Military thinkers envisioning future conflict typically imagine returning to the large-scale wars of the past with new technologies. They struggle to imagine new modes of warfare and the systems, organizations, and doctrine to use them well – particularly before the full revolutionary capabilities of new technology have come to fruition in ways that permit large-scale experimentation. They remain excessively focused on the challenges of high-end conventional conflict without taking adequate account of the transformation particularly in Russian military thinking around the concept of hybrid war, in which military operations are subordinated to informational objectives. Our adversaries, and particularly Russia (and Iran), are now aggressively experimenting with new concepts and techniques in small wars, overseas engagements, and domestic crises. The Russians are conducting extensive lessons-learned activities based on their experiences fighting in Syria and Ukraine, and are constantly updating their theory, doctrine, organization, and practice based on those lessons. The Chinese are learning lessons from their historical and current pandemic and disaster relief operations, their special operations, wargaming, and observing other actors such as Russia overseas.[13]

This concern is shared by former U.S. Secretary of Defense Robert Gates, who cautioned, "the black-and-white distinction between conventional war and irregular war is becoming less relevant in the real world … Possessing the ability to annihilate other militaries is no guarantee we can achieve our strategic goals - a point driven home especially in Iraq."[14]

The point is that our adversaries are competing on the entire spectrum from peace / competition to conflict. As shown, they are attempting to dismember the West without fighting directly in a hot war. Rather they are attacking Western democracy, stealing critical technologies, promulgating disinformation, launching cyber-attacks and undermining alliances and coercing partners. They are practicing hybrid, or in more current parlance, Gray Zone operations.

General Gerasimov distinctly articulated the application of the Russian methodology of competing (or more accurately great power competition / conflict). He explained:

> Moscow is increasingly focusing on new forms of politically-focused operations in the future. In many ways this is an extension of what elsewhere I've called Russia's 'guerrilla geopolitics,' an appreciation of the fact that in a world shaped by an international order the Kremlin finds increasingly irksome and facing powers and alliances with greater raw military, political and economic power, new tactics are needed which focus on the enemy's weaknesses and avoid direct and overt confrontations. To be blunt, these are tactics that NATO–still, in the final analysis, an alliance designed to deter and resist a mass, tank-led Soviet invasion–finds hard to know how to handle.[15]

Although competitors such as China and Russia maintain large military forces and continue to improve and expand their arsenals, arguably leading to a renewed arms race, they remain careful to avoid actions that would possibly activate the conventional war "trip wire." Rather they maintain the military capability as a substantial, viable and overt threat, but compete on various levels under the threshold of a "hot" or "shooting war." They utilize "Hybrid Warfare," defined by NATO as "a wide range of overt and covert military, paramilitary, and civilian measures [...] employed in a highly integrated design."[16]

Similar to strategic competition, Hybrid (or Gray Zone) Warfare is not new. In its simplest form it represents a state or non-state entity using every "tool" at its disposal to achieve its political objectives. The big difference is globalization and the explosion and proliferation of cheap and available technologies and information networks have made the ability to impact adversaries far easier. The inherent strategic ambiguity that is created with asymmetric methodologies implicit in Hybrid Warfare impacts the ability of adversaries to recognize real threats (or attacks), make the necessary decisions and react accordingly.

So, the issue becomes what if anything has substantively changed in the security landscape? Is the current strategic competition a throwback to the Cold War? Does the CT / COIN focus of the last two decades need to be discarded? For Sir Michael Howard, the renowned military historian, the issue is straightforward. "No matter how clearly one thinks," he explained, "it is impossible to anticipate precisely the character of future conflict." In finding a solution to this quandary, his philosophy was simple. He asserted, "The key is to not be so far off the mark that it becomes impossible to adjust once that character is revealed."[17]

As such, in the current turbulent, if not continually disintegrating security environment, recognizing the "mark" and adjusting accordingly is a daunting challenge. The proliferation of Chemical, Biological, Radiological, Nuclear (CBRN) weapons, advanced conventional weapons, new and emerging military technologies, as well as invasive influence activities and cyber warfare has, and will continue to, increase complexity and risk in strategic competition. As a result, Seth Jones, a RAND Corporation researcher and political scientist at the Center for Strategic and International Studies, argues, "The future of conflict means that the United States needs to prepare to compete with these states not primarily with divisions, aircraft carriers and strategic bombers—but by, with, and through state and non-state proxies, cyber tools, and overt and covert information campaigns."[18]

Additionally, climate change has created turbulent weather events that have skewed traditional predictability of seasons and weather patterns, as well as increasing the severity of storms. Flooding, drought, increased temperatures have caused dramatic changes to the environment (e.g., forest fires, expanding deserts, increased sea states, melting ice packs, etc.) that impacts operations in affected regions, as well as causing humanitarian crises that also fuel global instability.

The COVID-19 pandemic has highlighted the potential disruptive, if not destructive, impact of future epidemics in a globally connected world. As researchers concluded:

> An invisible virus borne on the air and reaching across continents and oceans, moving freely among people, disrespecting borders and ideas of state sovereignty, will mark the most profound shake-up of thinking about national security since the beginning of the atomic age in 1945. We have entered an era in which national security is not just about protecting the state against adversaries, but also against dangers that have a direct impact on the daily lives of people. The vectors of these threats are new and different — they don't present the menacing face of armies and war, the shadowy artifice of the traditional spy, or the low-tech threat of terrorism. The new threats come at us straight out of our digital environment and are unleashed out of the natural world. Digitally enabled threats take aim at precious resources — our data, our economy, our research — and the fundamentals of our democracy. They rob us and bend the truth, and as more of our economy is digitally enabled it is capable of being digitally disabled. Natural hazards from climate change and the globalized spread of serious infectious diseases threaten livelihoods and lives across the country.[19]

Consequently, the challenge is recognizing that great power competition, as well as dealing with rivals and rogue states, is on a completely different playing field. Although conventional military capability will always be required, as both a deterrent and back-stop to military aggression, the majority of the never-ending competition / conflict will be waged on economic, informational, political, societal and technological planes.

However, what if we fail to identify, accept or understand the character of conflict once it is revealed? The U.S. as well as most NATO countries are transitioning from a focus on primarily low-tech, low-resourced adversaries (e.g., the Islamic State, al-Qaeda and other jihadist terrorist groups) to a focus on GPC, especially with China and Russia, who have both an advanced military capability (conventional and nuclear) and also a well-developed asymmetric / special warfare capability.[20]

Therefore, it is important to frame the changes that will impact operations in the future security operating environment, which will be characterized

by increased lethality, enhanced speed and tempo of operations, amplified informatization empowered through AI, increased complexity, and the loss of traditional Western supremacy in all domains. Quite simply, an outright shooting war itself between belligerents using modern weaponry will be disturbingly swift and horrifically destructive. The competition space, fought below the threshold of actual kinetic engagement, will become frustratingly ambiguous and complex as adversaries struggle to make sense of events to determine if they are real? Constitute an attack? And / or, require a decisive response?

In summary, some of the major changes that will require actors to absorb and determine methodologies to deal with include:

Disintegrating Rules-Based International Order

The relative adherence and stability of the post-WWII rules-based international order is, and will continue to, fray. A resurgent Russia, an emergent China, and a host of rogue state and non-state actors will continually challenge the status quo of international relations and norms. The *Global Trends 2040* report concluded, "the international system is directionless, chaotic, and volatile as international rules and institutions are largely ignored by major powers like China, regional players, and nonstate actors."[21] The transformation in the international system will create structural challenges that increase risk to global stability and security. The Report noted, "In the international system, no single state is likely to be positioned to dominate across all regions or domains, and a broader range of actors will compete to shape the international system and achieve narrower goals. Accelerating shifts in military power, demographics, economic growth, environmental conditions, and technology, as well as hardening divisions over governance models, are likely to further ratchet up competition between China and a Western coalition led by the United States."[22]

The manifestation of this deterioration of the rules based international order and the inherent risks are clearly evident by contemporary events. China's build-up and militarization of the Spratly Islands and associated reefs, as well as its intimidation of Taiwan and other neighbours demonstrates a clear rejection of international norms. So too, Iran's aggressive regional expansion through the use of proxies and its own military provides another example, as does North Korea's rejection of international rules and agreements. Finally, the Russian annexation of the Crimea and support to the break-away Donbas

separatists in 2014, and its outrageous invasion of Ukraine in February 2022 represent the most lurid examples of the disintegrating rules-based international order.

This reality bodes ill for stability and security. Against a backdrop of toothless international rules and agreements, as well as impotent international bodies to enforce compliance, and the precedence of rule-breaking actors who are able to achieve their political objectives without substantive harm to their regimes, strategic competition will take on considerable risk. At what point does an actor or actors miscalculate, thereby tripping the threshold of violence? And, how will autocratic regimes reshape the geopolitical landscape / international order?

Proliferation of Technology

Another key major change that will impact strategic competition is the proliferation of cheap, accessible, advanced technology. This expansion of available technology, whether weapons, sensors, delivery vehicles, informational technology and robotics will make adversaries, particularly those that are not great or middle powers, as well as non-state actors, more capable and dangerous. A report to the U.S. Senate cautioned, "U.S. national security will likely be affected by rapid technological advancements and the changing character of war.… New technologies include advanced computing, 'big data' analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future."[23]

Significantly, the proliferation of technology also means the West will lose its monopoly of advanced technology and the advantages in ISR and fighting to which the West has become accustomed. The sheer scope of technological developments makes the current era of strategic competition so much more complex and daunting than the past. Hypersonic missiles, directed-energy weapons, AI, cyber warfare / hacking technologies, for instance, have increased the capabilities of state and non-state actors to impact adversary governments, militaries and societies.

A British report on strategic competition concluded that science & technology (S&T) has become an arena of systemic competition. It noted, "over the coming decade, the ability to advance and exploit S&T will be an increasingly

important metric of global power, conferring economic, political and military advantages."[24] However, the wild card becomes the ability to repurpose off-the-shelf consumer / civilian systems in warfighting that will further enhance the abilities of adversaries to do harm. In addition, many state powers have little hesitancy in sharing technology with their proxies who can then target adversaries allowing their sponsor(s) plausible deniability in culpability.

The key impact will be the heightened effectiveness, reach and lethality of all actors. Unmanned aerial vehicles (UAVs), commonly known as drones, are a simple example of how technology has been exploited to enhance warfighting capability in modern warfare. Although military UAVs have been in use for two decades, the Nagorno-Karabakh conflict demonstrated how pivotal drones have become in combat. Globally, state and non-state actors are increasingly relying on drone technology. UAVs no longer simply provide an ISR or kinetic-strike function. They are also used for command and control, particularly to coordinate the fires and manoeuvre of combat arms units. Currently, it is estimated that there are 30,000 military UAVs in use.[25]

For example, during the Nagorno-Karabakh conflict between Armenia and Azerbaijan from 27 September to 10 November 2020, the use of Israeli and Turkish manufactured military UAVs by Azerbaijan to target Armenian personnel and equipment proved extremely effective during the forty-four-day conflict. Analysts observed that Azerbaijan used its UAV fleet "to stalk and destroy Armenia's weapons systems in Nagorno-Karabakh, shattering its defenses and enabling a swift advance." Azerbaijan used surveillance drones to spot targets and subsequently sent armed drones or kamikaze drones to destroy them. Confirmed Armenian losses numbered: 185 T-72 tanks; 90 armored fighting vehicles; 182 artillery pieces; 73 multiple rocket launchers; 26 surface-to-air missile systems and five S-300s; 14 radars or jammers; one SU-25 war plane; four drones and 451 military vehicles.[26]

The significance lies in the fact that the expanding array of relatively low-cost UAVs can offer state and non-state actors aerospace power at a fraction of the cost of maintaining a traditional air force. Michael Kofman, military analyst and director of Russia studies at the Center for Naval Analyses (CNA) asserted, "Drones offer small countries very cheap access to tactical aviation and precision guided weapons, enabling them to destroy an opponent's much-costlier equipment such as tanks and air defense systems."[27]

As noted, it is not just state actors that are deploying UAVs. A large number of non-state actors have utilized drones in combat, including Islamic State in Syria (ISIS), Hezbollah, Houthi rebels, Hamas, Boko Haram, Shiite Militias and the Afghan Taliban, among others.[28] For example, in Yemen, Houthi rebels have used UAVs to attack Saudi oil facilities, effectively penetrating Saudi Arabian air space and striking their target with impressive precision. In the first three months of 2021, Houthi rebels launched 45 drone attacks against Saudi Arabia.[29] Three of the UAVs struck oil facilities and airports. UAVs also attacked the capital Riyadh, which is approximately 1,000 km from the Yemeni border.[30] Moreover, on 17 January 2022, Houthi rebels deployed a group of armed drones on another extended almost 1,600 km mission as part of a drone / ballistic missile coordinated attack against the Saudi coalition partner UAE hitting the Abu Dhabi airport and starting a fire, as well as hitting several oil trucks at a state-owned fuel depot.[31] In December 2020, the Saudi-led coalition revealed that the Houthis had fired more than 850 attack drones and 400 ballistic missiles at the kingdom in the past seven years, killing a total of 59 civilians.[32]

American military officials in Iraq remain deeply concerned by the continual attacks by Iran-backed militias that use UAVs, which can evade detection warning systems around military bases and diplomatic facilities. Rather than rockets, the militias have begun to deploy small, fixed-wing UAVs that fly too low to be identified by defensive warning systems. An American official with the American-led coalition conceded the evolving drone threat represented "the military mission's biggest concern in Iraq."[33] In addition, ISIS also had a significant drone program in Syria and Iraq. It launched 60 to 100 drone attacks every month in 2017 alone.[34]

The proliferation of technology portends no end of risk. Almost any actor, even "lone-wolf" terrorists, with access to commercial technology can develop drones capable of wreaking havoc. Nuclear sites, power generation stations, stadiums, any venue with mass crowds, government buildings, etc., are vulnerable and can become killing zones. As an example, in 2015, a drone containing radioactive material landed on Japanese Prime Minister Shinzo Abe's office. In 2018, in Caracas, Venezuela, President Nicolas Maduro was almost assassinated when two explosive-laden UAVs detonated in the proximity of where he was giving a speech. Finally, in November 2021, an explosives-laden drone landed on the residence of Iraqi Prime Minister Mustafa al-Kadhimi, injuring seven of his bodyguards.[35]

Compounding the lethality of easily procured UAVs is the threat of "swarming," which would allow an adversary to overload the defensive capabilities of their opponent. In Xi'an, China, 1,374 drones were flown by the Ehangh Company in a coordinated fashion to form complex shapes and designs for a light show. Another company called "Intel" also demonstrated the ability to control increasingly larger numbers of drones. In 2017, it flew 300 drones together. The following year it deployed 1,218 UAVs together and later in the year 2,018.[36]

What makes the issues of UAV, particularly drone swarms, more concerning is the fact that in 2018, the U.S. National Academy of Sciences concluded that modern hobby drones operate increasingly without radio. They noted that these drones utilize automated target recognition and tracking, GPS chips, obstacle avoidance and other software. These factors make the UAVs relatively invulnerable to jamming and as a result more survivable.[37]

Of concern is the fact that proliferation will continue. As more rogue states gain access to CBRN munitions the likelihood of nefarious actors, proxies or sponsored groups, gaining access to weapons of mass destruction and the vehicles required to deploy them becomes exponentially greater.

Precision and Lethality

The proliferation of technology becomes even more disquieting when one considers the precision and lethality of modern munitions. The advent of a new generation of advanced weapons systems including hypersonic missiles, UAVs, and other unmanned systems, augmented by AI, machine learning, and other information technologies makes conflict a daunting prospect. The formidable capabilities of current and emerging technology and munitions makes the fielding of large conventional armies and their platforms laden with risk. The threat environment does not end there. The jamming of communications, anti-satellite technology, EW and cyber-attacks that target networks and the vulnerable software programs that represent the backbone of societal and military operations will only increase risk and consequence of strategic competition, much less a high-intensity war. The increasing development and deployment of autonomous systems only adds to this complexity.[38] The 2022 Russian invasion of Ukraine provides a stark example. Ukrainian UAVs identifying targets and controlling fires, as well as modern shoulder mounted anti-tank missiles are but two factors that have shocked the Russians and

outside observers to the destruction that can be wrought on state-of-the-art armour.[39]

Destructive capability is not limited to land. On 14 April 2022, the Ukrainians sank the Russian flag-ship cruiser *Moskva* with a pair of Neptune anti-ship missiles. The lethality of modern missile systems has prompted defence officials to ponder the way ahead. Traditionally, a military has developed an army built around tanks, a navy built around ships, and an air force built around aircraft. All these platforms are technologically advanced and extremely expensive. However, the Ukrainian conflict has revealed that "the signature land weapon hasn't been a tank but an anti-tank missile: the Javelin. The signature air weapon hasn't been an aircraft, but an anti-air missile: the Stinger. And as the sinking of the *Moskva* showed, the signature maritime weapon hasn't been a ship but an anti-ship missile: the Neptune."[40] The effectiveness of relatively inexpensive missiles and drones against expensive legacy platforms begs the question of how to invest limited resources.

In this light, the prognosis for a high-intensity, traditional war scenario is ominous, if not downright appalling once one discounts the obvious Russian miscalculation in Ukraine.[41] In an armed conflict, China and Russia will attempt to achieve physical stand-off by employing layers of anti-access and area denial systems designed to rapidly inflict unacceptable losses on the U.S. and its allies "to achieve campaign objectives within days, faster than the U.S. can effectively respond."[42]

Globalization, the proliferation of technology and its exponential, consistently increasing capability has made a traditional war almost incomprehensible. An increasing number of nations with substantial nuclear arsenals, as well as the global propagation of stand-off precision missile systems and platforms, including highly manoeuvrable cruise missiles, as well as hypersonic weaponry (weapons that travel at five times the speed of sound and that can dodge and weave during flight to avoid interceptors) and glide vehicles, matched with networked sensors are capable of delivering large payloads of munitions (with nuclear or conventional warheads) at increased ranges so that targets can be engaged and destroyed almost anywhere with accuracy within a short period of discovery and decision-making.[43] Space based weapons, lasers, directed-energy munitions and high-powered microwaves will only increase lethality and reach.

Recent advances by Russia and China highlight the threat. American officials were apparently "rattled" by the November 2021 Russian missile test that struck a defunct space satellite bringing the fear of a militarized space one step closer.[44] Similarly, China has demonstrated its capability as well. One top American military official acknowledged, "They [China] launched a long-range missile. It went around the world, dropped off a hypersonic glide vehicle that glided all the way back to China, that impacted a target in China."[45] Its accuracy was disturbingly precise. Unlike intercontinental ballistic missiles that travel in a predictable arc and are trackable by long range radars, a hypersonic missile moves much closer to the earth, making it difficult for radars to detect.[46] Compounding the concern is the fact that China has accelerated the pace of its nuclear expansion. Experts predict the PRC will have up to 700 deliverable nuclear warheads by 2027.[47] These weapons systems limit the amount of time decision-makers have to assess the required response options or to intercept the attack.

These advancements are not unexpected. Already in early 2018, American intelligence agencies warned that Russia sought to advance and operationalize anti-satellite capabilities including directed-energy weapons and potentially dual-purpose satellites that could conduct offensive strikes in space against an adversary's satellite network.[48] In fact, Russia announced continued progress on its A-235 "Nudol" anti-satellite missile, "which aims to provide enhanced range (compared with previous technology) while enabling kinetic, non-nuclear strikes against adversary missiles and satellites."[49]

Furthermore, President Putin heralded the existence of the Zircon missile, which he claimed can cover 1,000 km at Mach 9 speed. The Zircon cannot be tracked by any radar or intercepted by any air defense system in existence.[50] Moreover, Russian surface ships and submarines carry the Kalibr family of sea-launched cruise missiles, which can house conventional or nuclear warheads and have a range of thousands of kilometres. These lethal munitions ensure no adversary has sanctuary from attack.[51]

The dual capability of conventional or nuclear warheads also brings the issue of lethality to an entirely new level. Disturbingly, it is more and more common to hear of the consideration of using tactical nuclear ordnance in conflict. The combination of miniaturized low-yield warheads combined with accurate deliver systems makes the option of a "limited" nuclear war frightening. The idea that a limited nuclear war could be fought without triggering a larger exchange, borders on wishful thinking.[52]

Importantly, there are relatively few problems with accurate delivery of ordnance. As innumerable analysts have identified, the world has become one big sensor, making masking military deployments or actions virtually impossible. As one researcher observed:

> The amount of data generated by networked devices, is on pace to triple between 2016 and 2021. More significant, the proliferation of low-cost, commercial sensors that can detect more things more clearly over greater distances is already providing more real-time global surveillance than has existed at any time in history. This is especially true in space. In the past, the high costs of launching satellites required them to be large, expensive, and designed to orbit for decades. But as access to space gets cheaper, satellites are becoming more like mobile phones—mass-produced devices that are used for a few years and then replaced. Commercial space companies are already fielding hundreds of small, cheap satellites. Soon, there will be thousands of such satellites, providing an unblinking eye over the entire world. Stealth technology is living on borrowed time.[53]

Making the battlespace even more challenging is the advancements in the miniaturization of cameras and satellites. New microsatellites are relatively cheap, small, and effective. A single rocket launch can deliver 80 small photo reconnaissance satellites into orbit. This capability has permitted the American company "Planet" to photograph any corner of the globe with one of its 200 satellites. Furthermore, it can update images daily with two-meter resolution. Actors need only project coverage over their objective areas. They can achieve this by deploying 300 to 500 microsatellites over their areas of interest or concern. Remarkably, these satellites can generate imagery of one-metre resolution and transmit data every five to ten minutes. The point is, this satellite array will have complete photo coverage of a conflict zone or area of interest and be able to spot any aircraft or ship entering into the battlespace and provide exact targeting data.[54]

An example of the danger of sensor to shooter timeliness and accuracy was demonstrated by the Russians in the Ukraine since 2014. They had "shortened to mere minutes the time between when their spotter drones first detected Ukrainian forces and when their precision rocket artillery wiped those forces off the map."[55]

In addition, the observation on stealth technology is not an idle thought. As noted earlier, the proliferation of technology is bound to continue. As an example, Russia is supplying Iran with an advanced satellite system, the Kanopus-V, which will give it an unprecedented ability to track potential military targets across the Middle East and beyond. The Russian system is equipped with a high-resolution camera that allows continuous monitoring of facilities ranging from Persian Gulf oil refineries and Israeli military bases to Iraqi barracks that house American troops. Military experts explain, "This capability will allow Iran to maintain an accurate target bank, and to update that target bank within a few hours" every day. Equally concerning, Tehran can share the information with pro-Iranian militia groups across the region.

With increased sensing and identifying capability and the ability to rapidly process information and cue sensors to shooting platforms through AI, the deployment and manoeuvre of forces becomes extremely challenging. Additionally, the lethality of modern weapon systems makes survivability more tenuous.

Increased lethality is also a function of advancements in other weapon technology. Next-generation high-power radio frequency-directed energy weapons[56] that can disrupt electronic controls and shut off vessel engines without harming occupants, as well as millimetre wave active denial–directed energy technology further complicate the battlespace. The U.S. DoD defines directed energy weapons as those using concentrated electromagnetic energy, rather than kinetic energy, to "incapacitate, damage, disable, or destroy enemy equipment, facilities, and/or personnel."[57] For example, during a border standoff between China and India in the western Himalayas, analysts have warned of the use of a "micro-wave" weapon that sent a high-frequency blast through Indian soldiers, forcing them to withdraw from strategic mountain top positions. Chinese professor Jin Canrong from the Renmin University in Beijing, revealed that two contested mountain tops were deliberately turned "into a microwave oven."[58]

These high energy laser (HEL) weapons can be used by ground forces to conduct such operations as short-range air defence (SHORAD); counter-unmanned aerial vehicles (C-UAV); and counter-rocket, artillery, and mortar (C-RAM) missions. The weapon systems can also be used to "dazzle" (i.e., temporarily disable) or damage satellites and sensors, which in turn can disrupt and impede ISR operations, military communications and GPS systems used for targeting.[59]

Additionally, UAVs as previously discussed, are widespread across the battlespace. Ominously, they have augmented the level of lethality already present on the battlefield. UAVs, especially when deployed in swarms, can inflict extensive damage at an extremely low cost. Experts have determined that tamper-proof features of blockchain for UAV swarms provides strong effective protection of mission-critical data, which makes disruption and / or interference with deployed UAVs extremely difficult.[60]

The U.S. and British militaries have programs to build "swarms" of small UAVs that operate as a group using advanced AI. The swarms can be launched from aircraft and ships. They can be used to overwhelm adversary defenses. Experts have postulated the deployment of swarms of hundreds, if not thousands of UAVs.[61] In 2020, a Chinese state-owned company released a video showing a Hummer-like vehicle that launched a swarm of 48 drones, each carrying a high-explosive warhead. The following year, the Indian army demonstrated the capability of launching 75 drones, with plans to increase it up to 1,000 UAVs. Drones deployed in swarms can overwhelm any defensive system that may be deployed. For instance, as early as October 2020, China revealed new airborne loitering munitions that can be launched from the back of a truck and which use swarming behaviour to attack targets. It represented an extremely potentially lethal and low-cost threat to expensive Western military hardware.[62]

Importantly, military-grade UAVs can fly themselves to a specific location, select their own targets and destroy targets without the assistance of a remote human operator. Such weapons known as a lethal autonomous weapon system (LAWS) are now in play. Their use adds yet another layer of capability and lethality.[63] After all, loitering munitions, also known as kamikaze drones, are totally autonomous and can "find, decide to engage, and engage targets on their own" without the need for human intervention.[64] Once launched, kamikaze drones fly to a specific target area, where they "loiter," scanning for targets. When they detect a target, they simply fly into it, detonating their onboard payload of explosives.[65]

For example, Turkish-backed forces of the UN-recognized Libyan government, using Turkish supplied drones, hunted down and killed soldiers loyal to the Libyan strongman Khalifa Hifter as they tried to retreat. The operated without human control to destroy Hifter's soldiers as they fled.

Finally, the development of motor-powered exoskeleton suits that increase human capacity to carry weight or cover distances already exist. The use of armour plate, weapon suites and jet-packs for flight are just a matter of time.[66]

So too is neurowarfare, which is defined as "the strategic takedown of a competitor through the use of neuroweapons that remotely target the brain or central nervous system to affect the targeted person's mental state, mental capacity and ultimately the person's behavior in a specific and predictable way."[67] Similar to cyber warfare, neurowarfare has both a defensive and offensive capability. Researchers explain that in "a defensive capacity, neurowarfare could prevent conflict before it starts, easing tensions by shaping attitudes and perceptions about the potential adversary. In an offensive capacity, neurowarfare could manipulate the political and social situation in another state, thus destabilizing the adversary, either as a stand-alone tactic or in conjunction with a military strike."[68]

Apparently, neurowarfare testing has already begun. In December 2016, CIA officers and American and Canadian diplomats stationed in Havana, Cuba, reported hearing pulsing sounds, sometimes accompanied by pressure sensations in their heads. Neurological symptoms such as headaches, dizziness, cognitive difficulties, fatigue, and hearing and vision loss followed. In total, over 40 U.S. government employees were affected, 24 being diagnosed with brain damage. Similar reports have emerged from U.S. personnel in China, Russia, Uzbekistan, and CIA officers working in several different countries. Two separate cases in Washington D.C. area are also currently under investigation. Investigators determined that "this is intentional, this is directed, this seems to be a beta test of some type of a viable neuroweapon."[69]

Command & Control

When it comes to the concept of command and control (C2) there are a number of issues to deal with such as military C2 in the battlespace, inter-agency cooperation and the impact of social media. Conflict, particularly against a peer or near-peer adversary, will entail operating in a degraded and severely contested communications / electronic environment. For instance, Chinese and Russian electronic warfare, cyber, and counterspace capabilities represent an existential threat to critical command, control, communications, computer, intelligence, surveillance, and reconnaissance capabilities.

Disruption to these critical warfighting functions will severely limit combat effectiveness.[70]

This reality compounded by the speed of sensor-to-shooter platforms and the lethality of modern weapon systems means that military forces must conduct dispersed / decentralized operations. To accomplish this effectively, C2 must rest on robust communications suites, but more importantly, allow for highly decentralized decision-making processes that provide tactical commanders both the authorities and the methodologies to deliver the required combat effects. Strong and clear commander's intent must drive tactical decision-making without the need to request permission from higher authorities at all times. Trust and mutual understanding between commanders and sub-ordinates will become key factors in success.

These attributes will not magically take hold on "game-day." Leaders at all levels must be trained and educated to fight with degraded information and disrupted command. They must be developed to be comfortable operating with "loose, decentralized peer-to-peer command, control, and communications structures in degraded, disrupted, or contested environments." They must also be comfortable operating independently and being self-sufficient for extended periods of time. The employment of mission command and other forms of decentralized and delegated command philosophies, particularly when command systems are disrupted will become paramount. As former Secretary of Defense, General James Mattis explained, "The more we anticipate . . . the less we have to improvise in combat."[71]

Nonetheless, despite the need for dispersed operations and increased authorities to tactical commanders based on clear commander's intent, there will still be a requirement for robust informational and communications systems that are "to gather, transmit, process, understand, and act on information faster and with greater accuracy than an opponent." Researchers have argued:

> Advantage in peace and victory in war will demand a mixture of technical information systems and cognitive functions such as command decision-making. Every effort should be expended to attain an advantage by degrading adversary systems and protecting friendly systems while disrupting the enemy's cognitive command processes and sustaining one's own. These imperatives create a "techno-cognitive confrontation" that is continual and widespread, crossing delineations between peace and war. Within this context,

> great-power warfare would be far more chaotic, lethal, and contested than the conflicts of the post–Cold War period.[72]

Conflict is not the only sphere where C2 will need to be carefully examined. Even within the Gray Zone sub-threshold competition space, C2 can be easily compromised. Jamming, hacking, cyber-attacks, disinformation, particularly "deep fakes" can disrupt, degrade and compromise C2.

Moreover, effectiveness in the Gray Zone requires a whole-of-government approach, enabling cooperation between various government departments and agencies working together in a seamless fashion to create collective, synchronized / harmonized actions to stymie our adversaries. However, as one senior SOF officer observed, "The sectoral structure of Western governments leads to an often observed inability to collaborate, or even to coordinate efforts, between governmental agencies." He added, "There is no integration between big [governmental] organizations facing the same security problem."[73]

Frank Hoffman, an expert in Hybrid Warfare agrees. He emphasized that "defeating the hybrid adversary will require alterations in how military and national security organizations think about strategy and how leaders are educated. It will require commanders throughout the military that can work across organizational boundaries, with coalition members, international organizations, and non-military agencies of government."[74]

However, the change in the C2 landscape also presents opportunities. Social media is used by some actors, notably non-state actors, for internal communication, information sharing, coordination, and synchronization of actions. Groups that are dispersed over large areas or that have no formal technical backbone to their structure utilize cell phone technology and social media as a means of C2. For instance, during the Arab Spring social media was used to generate swarms of protestors at specific locations.

Although the use of social media as a C2 mechanism does not allow for an attack on a centralized network, nodes or HQs, it does expose these adversaries to intercept and interference.[75] That being said, these actors can also practice defensive activities that make the use of encryption, anti-tracking, and/or IP-concealing software in connection with social network media. Nonetheless, many non-state actors have shown a clear lack of appreciation or knowledge of operational security (OPSEC). They have demonstrated

a lack of awareness about basic cyber-security, which has allowed a large number of terrorists and insurgents to be taken off the battlefield.[76]

Another concern with C2 and social media is the fact that any action in a conflict zone, or anywhere else, can be uploaded in real time and become viral. The issue of disinformation, incorrect context, and / or deep fakes makes the requirement to respond equally quickly problematic for traditional, hierarchical military establishment. An event posted spreads rapidly. The ability of the chain-of-command to seek clarification through its hierarchical structure, process the information, craft a response, and then approve its distribution simply cannot compete with the current speed of information. As such, C2 requires the ability to allow tactical commanders at the ground level to respond as quickly as possible to correct, refute and / or explain the context of the allegations. The longer the lag time, the lesser the impact of the response.

Freedom of Manoeuvre & Concealment

Freedom of manoeuvre is yet another aspect in the changed security landscape. Unlike the past two decades where the U.S. and its NATO allies have had the luxury of dominating any combat zone with ISR, precision fires, communications and freedom of movement on land, sea and air, any deployment in a future conflict, as well as in the environment of strategic competition, will be challenging. Satellite surveillance, advanced sensors and radars networked to shooting platforms, as well as state-of-the-art A2/AD networks will challenge even the most advanced technologically advanced militaries to maintain secrecy of manoeuvre. Moreover, the proliferation of drone technology, as has been seen in recent conflicts, has allowed even small state as well as non-state actors to possess an extremely capable ISR capability.

Even movement in non-conflict, below the threshold of conflict Gray Zone activities, will be constrained. The proliferation of smart phones virtually makes any person a potential sensor. Posting on social media platforms and the internet makes any action taken potentially distributed in real time.

Moreover, the proliferation of close-circuit TV (CCTV) and facial recognition at airports and other transit points makes concealment increasingly difficult. SOF individuals transiting airports around the world can become identified based on their presence during specific events or crises or simply from visiting embassies or training bases. This information can be uploaded and used

to identify individuals as they enter specific countries. As noted earlier, the Chinese Road & Belt initiative that has witnessed China build airports and ports for Third World Countries also included the installation of surveillance suites that allow China to monitor travelers, thus allowing them to build a large data-bank of facial images and information.

In addition, the digital footprint of individuals using their smartwatches and fitbit devices, as well as their social media platforms provides another potential vulnerability to freedom of movement and manoeuvre. For example, U.S. personnel using personal fitness trackers unwittingly revealed the location of secret bases, as well as patrol routes in theatres of operation such as Iraq and Afghanistan.[77] Intelligence analysts have warned:

> the biggest danger may come from potential adversaries figuring out "patterns of life," by tracking and even identifying military or intelligence agency personnel as they go about their duties or head home after deployment. These digital footprints that echo the real-life steps of individuals underscore a greater challenge to governments and ordinary citizens alike: each person's connection to online services and personal devices makes it increasingly difficult to keep secrets.[78]

Artificial Intelligence (AI)

AI is "the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."[79] The Joint Special Operations University (JSOU) defines AI as "a specific field within computer science that explores how automated computing functions can resemble those of humans."[80]

AI has demonstrated that it can rapidly and effectively furnish reliable data analysis to assist, if not empower, decision-making. AI's biggest advantage comes from its ability to find patterns that would otherwise be indecipherable to human analysts.[81] Quite simply, AI analyzes and assesses data and subsequently can recommend potential decision options. A RAND report revealed:

> Unlike in past technological developments, such as atomic weapons and stealth aircraft, the United States will not have a monopoly, or even a first-mover advantage, in the competition for military AI.

> China is aggressively developing robotic systems and an assortment of other systems to integrate data from a wide variety of sensors to identify hidden targets, provide a common operating picture to commanders, and enable rapid decision-making. Russia also has an advanced robotics program but is more actively pursuing other areas, such as defensive systems, decision-making and planning tools, electronic warfare, cyber warfare, and AI-driven disinformation campaigns. Russia is already using AI technologies in support of its hybrid, gray-zone, and information warfare operations abroad.[82]

The RAND observation is important since as the *Final Report* of the National Security Commission on Artificial Intelligence concluded, "The ability of a machine to perceive, evaluate, and act more quickly and accurately than a human represents a competitive advantage in any field—civilian or military. AI technologies will be a source of enormous power for the companies and countries that harness them."[83] Experts believe that AI-enhanced capabilities will be the tools of choice in the renewed era of strategic competition as competitors (e.g., peer, near-peer, rogue states, non-state actors) develop and / or acquire AI concepts and technologies (through cheap and commercially available AI applications) to achieve their objectives.

Notably, both the Chinese and Russians have placed great effort into developing AI capabilities. President Putin proclaimed, "Artificial intelligence is the future of not only Russia, but of all mankind," and "whoever becomes the leader in this sphere will become the ruler of the world."[84]

Experts tend to agree. They insist that defending against an AI-enabled adversary without the use of AI was an "invitation to disaster." In essence, "AI can compress decision timeframes from minutes to seconds, expand the scale of attacks, and demand responses that will tax the limits of human cognition."[85] Human operators will not be able to contend with, much less defend against, AI-enabled cyber or disinformation attacks, drone swarms or missile attacks without the assistance of AI-enabled technology. As one expert asserted:

> Even the best human operator cannot defend against multiple machines making thousands of manoeuvres per second at hypersonic speeds and orchestrated by AI across domains. Humans cannot be everywhere at once, but software can – it can augment human capability and can have enormous benefits. It can defend society

and democracy, it can enable operational advantage, and remove humans from harm's way.[86]

The power of AI is easy to understand. So too, are the enormous military applications that AI can assist. Military uses of AI include:

1. Processing and Managing Intelligence – with the proliferation of sensors, UAVs, and other surveillance technology, AI allows for an efficient and effective method to cull images and information collected from these systems. Importantly, AI can rapidly process a flood of data from varied ISR platforms operating in multiple domains and flag important information such as missile systems, military vehicles, troops, and intelligence information. It allows the user to move faster than their adversary, thus enhancing offensive mobility and defensive posture, thus, increasing force protection. Equally, early identification and engagement enhances the element of surprise and minimizes exposure to enemy fire.

2. Speed of Decision-Making – AI can process enormous amounts of data faster than a human. Utilizing AI allows one to sequence through the observe-orient-decide-act (OODA) cycle faster than one's adversaries, thereby bestowing clear advantage by driving events rather than reacting. This advantage will deny adversaries the ability to act effectively in a timely manner whether on the offensive or defensive.

3. Improved Targeting and Situational Awareness – the myriad of cameras conducting surveillance globally and generating images can easily create data overload. With all of this data being generated, AI can analyze incoming video and imagery and flag activity and images of interest rapidly, thereby allowing for precipitous targeting and / or increasing situational awareness.

4. Decision-Making Support – As noted above the ability to process information, video and images swiftly allows AI to recommend options to decision-makers faster or in some cases it can furnish an array of higher-quality options to choose from compared to those that humans could generate in the same timeframe. For example, AI is able to take routing technology that can process complete maps and real-time or projected traffic information and develop multiple options for travel.

5. Mitigation of Manpower Issues – The military is almost always faced with personnel shortfalls. AI allows for some tasks (e.g., image analysis, translation) to be done without humans. Moreover, AI is instrumental to robotics, which will further alleviate personnel issues on the battlefield in a multitude of ways (e.g., shortage of personnel, risk to personnel, deprivation issues. Moreover, robotics can increase accuracy and precision compared to humans, as well as increasing efficiency since robots do not get tired, bored, stressed or frightened.

6. ISR – The ability to autonomously collect intelligence by way of drones, from ground and space-based sensors, as well as in cyberspace will generate even greater amounts of data that will need to be processed. AI is a key factor in both processes – collecting and analyzing.

7. Operating in Denied / Hostile Environments – adversaries have invested heavily in A2 / AD technology and networks to deny the ability of opposition to project force into regions that they wish to control. These systems are increasingly lethal to personnel and equipment. General Mark Milley explained, "strategic competitors like Russia and China are synthesizing emerging technologies with their analysis of military doctrine and operations. They are deploying capabilities to fight the US through multiple layers of stand-off in all domains – space, cyber, air, sea, and land. The military problem we face is defeating multiple layers of stand-off in all domains in order to maintain the coherence of our operations."[87] AI-driven autonomous systems will assist in operating in environments that are increasingly non-permissive for humans. For example, swarms of UAVs / drones can be launched to overwhelm defences and allow follow-on forces penetrate defensive barriers with fewer casualties.[88]

Tempo

The development and proliferation of advanced technologies has accelerated the speed and complexity of war.[89] Conflict between belligerents, particularly great powers, will be fast-paced, extremely lethal, and exceptionally chaotic. Precision weaponry networked with a multitude of ground and space-based sensors will allow for accurate long-range engagements, which will force

dispersion and rapidity in manoeuvre to avoid becoming a target. AI generated data, as well as decision-support will assist in creating relative clarity quickly prompting continual decision cycles resulting in perpetual motion of both planning staffs and manoeuvre forces. The use of AI will press tempo to limits not yet experienced in conflict. Decision-cycles will be collapsed and decision-making pressed to extremes as belligerents try to make sense of what is occurring and what capabilities still exist.

In addition, the introduction of robotics and exoskeletons will enhance endurance and drive greater tempo. China has already developed a motor-powered exoskeleton that can carry ammunition boxes weighing 50 kilograms (kg). The light-weight exoskeleton suit, known as the portable ammunition support assist system for individual soldiers, can provide 20 kg of assisted strength to its user, relieve more than 50 per cent of the burden and greatly reduce risks of waist injury. It takes less than 40 seconds to put on the suit and take it off. The suit's motor gives a reacting force to its user every time the user gets up after bending over, so the user can get up faster with less effort. Optional hooks can be used when carrying ammunition boxes, and they can not only help the user with a better grasp, but also give assisted strength. With the help of the exoskeleton suit, one person can carry ammunition boxes weighing 50 kg without much effort, and two people can carry more than 75 kg with ease.

The impact of increased tempo has also driven the U.S. concept of the SOF Hyper Enabled Operator (HEO), which is designed to counter tempo, but ironically will also drive-up tempo. The intent of the HEO system is to provide the right information to the right person at the right time without overloading them. Empowering the operator by technologies that enhance the operator's cognition to increase situational awareness, reduce cognitive load, and accelerate decision-making is admirable, but will also fuel faster and potentially longer operations."[90]

Enhancement can be categorized into three main areas. First, neuropharmacology, which utilizes drugs designed to target specific areas of the brain. Second, brain stimulation, which uses electric currents to invigorate specific areas of the brain. Third, brain-computer interfaces (BCI), which pertain to "opening up pathways to connect the brain to a computer in order to allow the two-way flow of information, either to program new behaviors or control external machines and devices." These technologies have the ability

"to improve warfighter performance by enhancing memory, concentration, motivation, and situational awareness while negating the physiological ills of decreased sleep, stress, pain, and traumatic memories."[91]

Finally, the ability of modern technology to see through periods of poor visibility will further drive the will of commanders to continue operations regardless of time of day / night or weather conditions. In sum, combat, which has always been exhausting to its participants will enter an even more demanding era.

Cyber

Cyber warfare, according to the RAND Corporation, "involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."[92] General Sir Patrick Sanders, the head of UK's Strategic Command, underscored the importance of cyberwarriors. "These cyberwarriors," he explained, "will be as vital to our defences as an F-35 pilot, a special forces operator or a submariner – and in contact with the enemy more frequently and persistently than any of them."[93] As one researcher noted:

> Everything is connected to everything else – systems, machines, people. Everything can be damaged, disrupted or put out of service practically from anybody anywhere. Defenders don't know when an attack is being launched, where it will strike and how. The resulting ambiguity makes an adequate reaction difficult, in particular for societies or multinational organizations that operate on the principle of consensus such as the European Union and NATO.[94]

Chinese military strategists argue that "whoever controls space will control the earth."[95] Experts agree and believe that the opening salvo of conflicts are most likely to be cyber weapons and electromagnetic radiation with their primary targets being space operations centres, satellites, and ground-control stations rather than military bases, ships or ground units. A PLA spokesman revealed, "In information systems combat operations, the side that seizes control of the electromagnetic spectrum…will control the course of the war."[96]

Similarly, Russian military strategists stress the importance of establishing "information dominance on the battlefield."[97] Major General Yuriy Lastochkin,

head of the Russian Defense Ministry's radio-electronic warfare force relatedly proclaimed, "EW is the most effective, fast-moving and cost-effective means of neutralizing the technical advantages of the opposing side… In the near future, qualitative changes in the development of EW [electronic warfare] forces and means will make it possible to decide the fate of all military operations."[98] Experience has shown that Russia skillfully utilized cyber-attacks to destabilize Georgia in 2008 and the Ukraine in 2014, as well as in 2022 prior to its military invasion.

The 2018 United States National Cyber Strategy declared, "persistent engagement in cyberspace is already altering the strategic balance of power." Moreover, in 2021, the U.S. Intelligence Community's Annual Threat Assessment report asserted that its greatest concern with regard to cyber warfare was about China, Russia, Iran and North Korea. Specifically, their intent to gain access to critical infrastructure and to undermine, through digital influence campaigns, the American public's confidence in institutions and the confidence of Allies and partners in American foreign policy commitments.[99]

Quite simply, cyber warfare is, and will continue to be, a decisive weapon in both Gray Zone operations and overt conflict by peer, near-peer and other state and non-state actors. For instance, a hacker, using the handle "Cyber-Caliphate," who self-declared as a member of ISIS / Daesh in January 2015, used the Twitter page of the *Albuquerque Journal* to post addresses, phone numbers, arrest records, and other sensitive personal information stolen from various databases. Subsequently, the CyberCaliphate struck the Twitter account of the U.S. CENTCOM and sent threatening messages to American service members. Some internal documents also appeared on CENTCOM's public Twitter feed.[100]

Similarly, the hacker group of the Syrian Electronic Army attacked the Twitter account of the Associated Press news agency. It published a tweet that reported that the White House had been bombed and that the president was injured. This tweet resulted in a $1,365 billion USD plunge in the S&P 500 index within three minutes.[101]

A final example, Colonial, which transports more than 100 million gallons of gasoline and other fuel daily from Houston to the New York Harbor, was the target of a cyber ransomware attack (that consists of malicious software that locks out a victim from their computer and renders it unusable) that forced

them to halt operations. Colonial, transports through 8,800 km of pipeline, approximately 45 per cent of all fuel consumed on the East Coast.[102]

The advent of cyber warfare has proven to be a major game changer. It allows an adversary to shape the environment and achieve political objectives below the threshold of violence, and / or set the stage for actively commencing hostilities. Denial of service attacks can destabilize a target country by attacking banking institutions, government services and utilities, thus creating possible agitation, protests and domestic upheaval. Hijacking social media and internet platforms can seed disinformation and deep fakes, which can further aggravate internal governance. Additionally, attacks on C2 nodes as well as satellite services can cripple an adversary's ability to communicate, control and / or support forces, as well as utilize their full inventory of capabilities.

Influence Activities

The term influence activities refers to organized attempts to achieve a specific effect among a target audience. These "attempts" include public diplomacy, strategic communications, information operations, and other methodologies that can be utilized to influence attitudes, behaviors, and decisions (i.e., "win hearts and minds") of a specific target audience. RAND Corporation researchers in 2009 defined influence operations as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives.[103]

The RAND researchers explained that influence activities "primarily consist of non-kinetic, communications-related, and informational activities that aim to affect cognitive, psychological, motivational, ideational, ideological, and moral characteristics of a target audience."[104] A 2019 RAND research team expanded the construct of influence activities to a concept they entitled Virtual Societal Warfare, which can involve any combination of a broad range of techniques including:

- deploying classic propaganda, influence, and disinformation operations through multiple channels, including social media;
- generating massive amounts of highly plausible fabricated video and audio material to reduce confidence in shared reality;

- discrediting key mediating institutions that are capable of distinguishing between true and false information;
- corrupting or manipulating the databases on which major components of the economy increasingly rely;
- manipulating or degrading systems of algorithmic decision-making, both to impair day-to-day government and corporate operations and to intensify loss of faith in institutions, as well as increase social grievances and polarization;
- using the vulnerabilities inherent in the connections among the exploding IoT to create disruption and damage;
- hijacking virtual and augmented reality systems to create disruption or mental anguish or to strengthen certain narratives; and
- inserting commands into chatbot-style interactive systems to generate inefficiencies and in some cases personal frustration and anxiety.[105]

The analysis suggests that Virtual Societal Warfare has characteristics that will have a direct impact on operations. RAND researchers contend these include:

- National security will increasingly rely on a resilient infosphere and, even more fundamentally, a strong "social topography." This resilient infosphere will require strong mediating institutions and a population continuously inoculated against the techniques of social manipulation;
- The barrier between public and private endeavours and responsibilities is blurring; national security will rely on the cooperation of private actors as much as public investments. This cooperation is especially required since technologies and techniques of this form of conflict are increasingly available to a wide range of actors both state and non-state. Importantly, private power in this realm matches and, in some cases, exceeds public power; and
- Conflict will increasingly be waged between and among networks. This reality is already evident, for instance, in the complex, international network of hackers, activists, and informal propagandists being employed by Russia as part of its information campaigns, and in China's use of Chinese citizens and ethnic Chinese abroad to further its control over key narratives.[106]

Regardless of the term used, influence activities / virtual societal warfare, the end result is a far more complex and difficult security environment to navigate. As previously stated, Russian thinking has reemphasized Soviet beliefs that the "initial period of war, which they perceive to be the period of time directly preceding the conflict, as well as the opening days of combat, will decide the outcome of the conflict. The Russians have shown an ability and intent to utilize "aggressive information-psychological operations in order to coerce adversaries, shape the environment, and prepare for conflict." Russian military strategists believe "in the pre-conflict or crisis phase of modern warfare, non-military means such as information will weigh in at a ratio of 4 to 1 with military means." Similarly, other Russian analysts insist that "success in modern warfare is predicated on information superiority above all else."[107]

They are not wrong. In October 2020, an American Joint Force wargame demonstrated how the U.S. and its allies could lose a conflict. The Vice Chairman of the Joint Chiefs of Staff, General John E. Hyten, conceded that the U.S. Joint warfighting concept "failed miserably" when the red team denied U.S. forces in the information environment, impairing communications and command and control, and rendering useless many key capabilities.[108]

For this reason, Lieutenant General Francis Beaudette, a former commander of the U.S. Army Special Operations Forces Command, explained, "We want every fight to be unfair as we pressure our adversaries from every angle and across all domains. It has never been more important to understand the cognitive, social, economic, and physical influences that affect human behavior. This is why we are aggressively training in the information space."[109]

The concept of cognitive warfare represents the most advanced form of manipulation to date, allowing the influence of an individual or a group of individuals on their behavior, with the aim of gaining a tactical or strategic advantage. The NATO Innovation Hub explained, "in this field of action, the human brain becomes the theater of operation. The objective is to act not only on what the target individuals think, but also on how they think, and ultimately, how they act."[110]

Cognitive warfare poses a daunting challenge. Researchers have identified that it:

> disrupts the ordinary understandings and reactions to events in a gradual and subtle way, but with significant harmful effects over

> time. Cognitive warfare has universal reach, from the individual to states and multinational organizations. It feeds on the techniques of disinformation and propaganda aimed at psychologically exhausting the receptors of information. Everyone contributes to it, to varying degrees, consciously or sub consciously and it provides invaluable knowledge on society, especially open societies, such as those in the West. This knowledge can then be easily weaponized. It offers NATO's adversaries a means of bypassing the traditional battlefield with significant strategic results, which may be utilized to radically transform Western societies.[111]

Cognitive warfare and the pursuit of influence operations to shape the attitudes and beliefs of a respective target audience is not a uniquely Russians pursuit. China does not hesitate to disclose that their goal of psychological warfare is "to sap the enemy's morale, disintegrate their will to fight, ignite the anti-war sentiment among citizens at home, heighten international and domestic conflict, weaken and sway the will to fight among its high-level decision makers, and in turn lessen their superiority in military strength."[112]

Not surprisingly then, analysts argue that the non-kinetic fight is reshaping conflict and that it will eventually overshadow the kinetic battlefield. Disinformation, fake video and deep fakes, which are AI algorithms that create convincing fake images, represent only the tip of the proverbial iceberg.[113] A NATO report cautioned:

> Among the many areas of concern around the technology, perhaps one of the most widely discussed has been the threat posed by "deep-fakes": synthetic audio, images, and video generated with artificial intelligence. Deepfakes are often strikingly realistic and sometimes challenging to distinguish from the genuine article.[114]

The Russians employed all the above techniques, including a deep-fake of Ukrainian President Zelensky urging Ukrainians to surrender.[115] And, the tool is not simply for state use. Vladimir Voronkov, the Under-Secretary-General of the UN Office of Counter-Terrorism, cautioned, "The ability to use artificial intelligence to generate high-quality fake videos or images—so-called deepfakes—is a powerful new tool that could be used by terrorists for misinformation and to undermine trust in governments and political figures."[116]

The world is experiencing a crisis with regard to what comprises the established truth, a phenomenon that RAND researchers refer to as Truth Decay, which they define as "a shift in public discourse away from facts and analysis that is caused by four interrelated drivers: 1. an increasing disagreement about facts and analytical interpretations of facts and data 2. a blurring of the line between opinion and fact 3. an increasing relative volume, and resulting influence, of opinion and personal experience over fact 4. a declining trust in formerly respected sources of factual information." The RAND report notes that Truth Decay is a serious threat to both domestic U.S. and international security, one that is being exacerbated by malign efforts from a variety of national bad actors.[117]

Social media provides one example of how one platform can be manipulated by influence activities to support military operations independently or in concert with physical activities on the ground. Supporting activities include:

- Targeting – social media can be used to identify potential targets (based on geo-tagged pictures or on-going conversations in social media). For example, Google Maps and cell phones were used in Libya to map regime positions that were then passed on to NATO, which used the information to identify targets and strike them with air power. In addition, the U.S. Air Force attacked an ISIS / Daesh headquarters building a mere twenty-two hours after commencing to track its social media posts. In addition, https://liveuamap.com/ provided an up-to-the-minute updated map showing disposition of Russian forces based on Ukrainians who were filming with their smart phones and uploading the photographs / images onto the site.[118]
- Intelligence Collection – social media can allow for the search and analysis of information (content and conversations) from social media networks and profiles. Analysis can include intelligence collection (e.g., trend, network, sentiment, geo-, content, behavioural, systemic, and information analysis), which can contribute to target audience analysis (TAA), and support psychological warfare or the selection of targets for operations both on- and offline. Social media allows analysts to obtain detailed information about actors, networks, and related communication, which in turn allows for a better understanding of the information environment and the respective target group.[119]

Influence activity campaigns, synchronized effectively with military action, can make a significant contribution to mission success. Conversely, a lack of focus on influence activities (offensively or defensively) can create insurmountable problems for military forces in the battle space, as well as with domestic and external audiences. Researchers insist that the global expanding digital infrastructure and networks will become "a defining landscape in human competition and conflict." They believe that the "diffusion of powerful capabilities across states, companies, and communities" will result in populations becoming "the common targets, subjects, and the medium of competition and conflict between actors."[120]

The increased use of, if not reliance on, AI, will only further complicate an already complex environment. AI can generate disinformation "in a way that brings real concern," according to Anne Neuberger, the White House deputy national security adviser for cyber and emerging technology.[121] Influence activities, such as media manipulation can be used to mobilize and manipulate supporters through mass communications, social networks, and online networks; shape public opinion, distort the truth, stoke social tensions, undermine support for governments, as well as to goad, provoke or trick an adversary into inflicting disproportionate civilian casualties or property damage and then exploit such errors with domestic and external audiences.

Societies are extremely vulnerable to persistent disruption and manipulation. Experts caution that advanced societies are "becoming perilously dependent on networks of information and data gathering, exchange, communication, analysis, and decision-making."[122] This dependence can have serious consequences if disrupted. For all these reasons, influence activities can create great opportunities, but also substantive hurdles, for governments and their military forces.

Climate Change

The UN defines climate change as the "long-term shifts in temperatures and weather patterns." Although these shifts may be natural, the UN highlighted that since the 1800s, "human activities have been the main driver of climate change, primarily due to the burning of fossil fuels (i.e. coal, oil and gas), which produces heat-trapping gases."[123] Reports from U.S. Federal science agencies and the Intergovernmental Panel on Climate Change concluded that "the burning of fossil fuels has increased the concentration of greenhouse gases in the atmosphere and raised global average surface temperatures about

1.1 degrees Celsius (°C) over pre-industrial levels." Moreover, they note that temperature rise has accelerated resulting in every decade since the 1960s being hotter than the previous one."[124]

The impact of climate change has been clearly evident. It has resulted in increased heat, heavy precipitation and flooding, drought, sea level rise, Arctic ice melt, Tropical cyclones, coral reef decay and biodiversity (50 per cent of terrestrial mammals and 25 per cent of birds are already affected by climate change).[125] These changes are expected to continue to damage and destroy infrastructure, ecosystems, and social systems around the globe. Moreover, continuing worsening climate change is expected to further disrupt communities and regions by exacerbating existing challenges of aging and deteriorating infrastructure, stressed ecosystems, and economic inequality. Experts believe that the impacts of climate change within and across regions will not be distributed equally.[126]

American researchers conclude that "climate change will increasingly exacerbate risks to US national security interests as the physical impacts increase and geopolitical tensions mount about how to respond to the challenge."[127] Researchers have established "that rises in temperature and prolonged precipitation – both environmental phenomena linked to climate change – increases the probability of conflict by four to five times in populations up to a radius of 550 km."[128]

Debate over action required and the competition over controlling the growth of clean energy, as well as the competition for increasingly scarce resources (e.g., fresh water) will increase the risks of instability and need for humanitarian assistance around the globe. Experts argue that the increasing physical effects of climate change will likely ignite geopolitical flashpoints as states manoeuvre to secure their interests. The reduction in sea ice in the Arctic has already kindled strategic competition in the Arctic over access to its natural resources. As temperatures rise and more extreme weather effects manifest themselves, there will be a growing risk of conflict over scarce resources and human migration.

The impact on international resource scarcity, security and stability is concerning in its own right. Climate change will severely impact military operations as well. Changes to weather patterns and their impact on geographical landscape and regions will require adaptation. Hotter temperatures, expanding deserts, unpredictable super-storms, flooding, and increased

access to remote regions such as the Arctic will all require technological and logistical adaptation to allow extended operations (i.e., communications, movement, survival, resupply, casualty evacuation) in potentially hostile / harsh physical environments.

Summary

The major changes in the security environment are daunting. Any refusal to acknowledge these changes and adapt accordingly will court disaster. However, it is critical to balance the changing security environment with those elements that remain constant. After all, great power competitors, rivals, rogue states, non-state actors and VEOs will continue to wage "war" to gain political objectives such as increased influence, access, economic gain, military advantage and power. They will utilize the full gamut of resources available to them whether proxy forces, cyber attacks, economic and political coercion, as well as disinformation meant to disrupt and divide societies. As such, a focus on purely traditional war fighting scenarios and an abandonment of current realities is a cataclysmic mistake.

West Africa, specifically the Sahel, is a case in point. Any desire to withdraw from Africa to focus on GPC misses the entire point of the current competitive battle space.[129] Former American Secretary of Defense Esper confirmed, "Mission No. 1 is to compete with Russia and China."[130] But to relax the focus on the smoldering state of the globe is arguably irresponsible, not to mention it defies the actual great power competition underway.

For example, initially, it is important to look at what has been done by the Americans, French and their allies and coalition partners in West Africa. They have deployed an impressive array of troops in the Sahel since 2014: 1,500 plus American; 6,100 French; 5,000 G5 Sahel Joint Force; 13,289 UN troops and 1,920 police under UN Multidimensional Integrated Stabilization Mission in Mali (MINUSMA); 7,500 Multinational Joint Task Force (MNJTF) military and non-military personnel; and 3,000 African Union (AU) emergency contingency troops, for an approximate total force of 38,000 personnel.[131] Yet, despite this enormous effort, the Western Sahel has experienced unprecedented terrorist violence, with more than 4,000 deaths reported in 2019, a five-fold increase in the number of fatalities caused by terrorist attacks since 2016. Burkina Faso alone accounted for 1,800 of the deaths reported last year, an increase of 2,150 percent over four years.[132] In the last two years alone, violence by terrorist groups in West Africa soared

250 percent. Moreover, the violence has displaced well over three million people in the Sahel.[133] Significantly, extremist groups are now creeping south from the Sahel toward coastal countries such as Benin, Togo, Ghana and Côte d'Ivoire.[134] One analyst observed:

> The Islamist militants who have rampaged through the heart of West Africa in recent years are now spreading toward the Gulf of Guinea coast, including some of the continent's most stable and prosperous countries, according to African and U.S. officials. The past year has seen an uptick in violence instigated by al Qaeda affiliates along the northern borders of Benin and Togo, with militant cells infiltrating as far as Ghana and Ivory Coast, the world's top cocoa producers. The attacks on countries along the bend in Africa's Atlantic coast appear to confirm warnings that U.S. military commanders have issued for several years: Unless stopped, militant violence won't remain contained in the landlocked nations of the Sahel, the semiarid expanses directly south of the Sahara.[135]

The growth and expansion of the terrorist groups and the apparent inability to defeat or even constrain them is worrisome in its own right. Additionally, the terrorists and militants have shown a disturbing ability to learn from their mistakes. They have taken on a more "complex" approach to attaining power. They destroy infrastructure, assassinate local leaders and loot key army bases in coordinated strikes, all resulting in the separation of the people from the government. The militants are attempting to inculcate their view of Islamist values into one of the youngest and fastest-growing populations on earth. Furthermore, they share their lessons learned worldwide with the fraternity of terrorists.[136]

The French withdrawal for example, has opened the way for Russia's proxy mercenary band, the Wagner Group, to propel Russian interests in Mali. In fact, both Russia and China have quickly tried to back-fill the apparent French and American desire to withdraw from the Sahel.[137] Both nations have extended offers of military equipment and training to the struggling West African countries. Additionally, China has invested heavily economically in the region. In Senegal, Beijing paid local farmers a premium to buy the bulk of their harvest. In Mauritania, China is building ports and other infrastructure, as well as investing in local fisheries.[138] In Somalia, China has provided military aid.[139] Furthermore, China has been offering African countries "smart cities" technology equipped with facial recognition technology (and

using that information for itself before delivering it to the host countries).[140] Indeed, Johns Hopkins University research indicates that China has wooed African nations with an estimated $5 billion per year.[141]

Chinese interest in Africa is not surprising. Africa represents an important playing field in the great power competition, mainly due to its resources, economic and demographic potential. It is a continent rich in raw materials such as diamonds, gold and rare earth minerals. It has excellent farmland, and other natural resources including oil and vast, flowing rivers. Economically, Africa is the second-fastest-growing continent in the world. From a population perspective, it already represents 16 percent of the world population with 1.3 billion people, projected to grow to 2.5 billion by 2050 and perhaps 4.5 billion by the century's end.[142] A senior British official noted the potential danger. "We Europeans," he explained, "have already seen potentially only the very tip of the human volcano that Africa, if left unattended, could represent."[143]

The point is, despite the desire to "pivot," the world has not dramatically changed. Great power competition focusing on traditional war fighting scenarios represents a small component of the actual "competition." The major moves and flashpoints remain in the shadows; clandestine in nature and most often in the difficult human terrain, where fighting the war of information and competing narratives for the support of the people remains omni-important.

The continued existence and global expansion of the Islamic State and al-Qaeda, as well as the explosion of Iranian-supported popular mobilization forces in Iraq; slow burning insurgencies in a myriad of at-risk states; and, not to mention, the festering conflict in Ukraine, Syria and Libya, are but a few examples of the current state of affairs, which will not go away simply because great powers decide to rekindle Cold War-like military sabre rattling. For instance, in 2019 there were approximately 8,500 terrorist attacks, which caused over 20,000 fatalities.[144]

All of these issues cannot be left to fester unattended, as the consequence, as was seen by the rise of Daesh in Syria and Iraq has global implications. Significantly, the Global Coalition to Defeat ISIS reported that terror activities by Jihadist militants "have increased in recent years, killing tens of thousands and displacing millions — creating a humanitarian crisis."[145] Similarly, General Clarke emphasized, "The threat, I think a good description is metastasized. It's gone into areas of Africa, where they could seek sanctuary and

where there may be some areas of sanctuary that we have to look at. And when I say it is not diminished, I think it's actually expanded."[146]

Clarke was not mistaken. Christopher Miller, a top American counter-terrorism official conceded that the Islamic State group continues to expand globally with some 20 affiliates, despite being forced out of Syria and the killing of many of its leaders. He explained, ISIS "has repeatedly demonstrated the ability to rebound from severe losses over the past six years by relying on a dedicated cadre of veteran mid-level commanders, extensive clandestine networks, and downturns in CT (counter-terrorism) pressure to persevere."[147] Similarly, General Townsend cautioned of the "wildfire of terrorism" that is sweeping across a band of Africa and needs the world's attention.[148]

Not surprisingly, the Americans are redeploying to Somalia. The Biden administration has decided to maintain its 27 operational military outposts in Africa. Moreover, AFRICOM is once again prioritizing counter-terrorism objectives in the Horn of Africa and the Sahel regions. The U.S. is also establishing a presence in other strategically important regions, such as the Red Sea and the Gulf of Guinea. Reportedly, the Americans are spending $330 million for base construction and related infrastructure projects.[149] The point is, GPC / strategic competition has not negated the need for continuing CT and COIN operations. In fact, our adversaries continue to fuel insurgency, terrorism and instability as a means to further their interests in the Great Game. The smoldering state of the world with its growing instability, extremism and insurgencies simply cannot be ignored. Allowing small fires to smolder, as has been shown throughout history, can lead to larger, costlier campaigns. Despite the overwhelming challenge of containing peer rivals such as China and Russia, the West cannot ignore the "brush fire" conflicts.

CHAPTER 7

Implications for SOF - GPC & The Gray Zone

In assessing this challenging abstruse international arena many pundits advocate that SOF must significantly transform to adapt to the renewed GPC. They argue that SOF must stop being a crisis response / reactive element and become more focused on sub-threshold proactive activities such as gathering information and participating in "Phase Zero" operations. This narrative is flawed, however, for a number of reasons. First, although SOF do crisis response due to their high-readiness, highly trained, agile force, they have historically (and are currently), been heavily engaged in sub-threshold activities such as military assistance, special reconnaissance and special force assistance (SFA).[1]

Secondly, the world remains an unstable place. VEOs, terrorism, insurgencies have not and will not go away. Africa, the Middle-East, as well as other geographic locations remain in turmoil. For example, in the Sahel, a former U.S. SOF commander lamented that "the Sahel is lost" because too little attention and too few SOF resources were applied to the problem. As a result, it is now in "free fall and it's continuing to deteriorate."[2] And, herein lies the issue. In many cases, these smoldering and raging fires are part of the GPC. Therefore, SOF are still required to continue with CT and COIN to deter, disrupt and defeat attempts at destabilizing friendly and at-risk states.[3] SOF are required to continue to do what it has done for decades, sub-threshold, Phase Zero work developing deep networks and relationships with partner nations to assist with stabilizing regions and states that are at risk of succumbing to violence and extremism.

Third, SOF tasks / employment principles in the renewed GPC remain largely the same. Circumstances and situations may change but employment principles for the large part remain interminable. For example, the task of special reconnaissance to gain information, situational awareness and ground

truth, or in current jargon to "illuminate," whether in peace, competition, conflict or war remains constant. Tactics, techniques and procedures (TTPs) may need to be adapted based on the geographic location, adversary, climatic conditions, etc., but the task remains the same. Too often, individuals who are ignorant to SOF history or force employment try to introduce new terms to explain a "required transformation" in the guise of advancing new concepts and thinking, when in fact they failed to understand SOF employment and capability in the first place. Nonetheless, the nature of the renewed GPC does have implications for SOF and will require adjustments to thinking and operating.

Gray Zone / Sub-Threshold Operations

In view of a competition battlespace in which competitors try very hard to remain under the threshold of a shooting / hot-war, the struggle for access, influence, political and economic advantage will remain in the shadows. Irregular warfare will be a dominant methodology. Disinformation campaigns meant to sway, alienate and / or divide populations; cyber-attacks; use of proxy forces; agitation; and support for political opposition and insurgent movements, will be predominant, as will economic and political strategies. As a result, SOF will remain an influential military instrument for governments to employ in strategic competition. After all, "the world is more dangerous than it's been before with a lot of potential threats out there," Steven Bucci, director of the Center for Foreign Policy Studies at the Heritage Foundation, cautioned, "and SOCOM [SOF] is offering policymakers ways to address those threats at a very low level with a low footprint in ways that can hopefully defuse those threats before they turn to violence."[4]

This theme was reinforced by former USSOCOM Commander General Raymond "Tony" Thomas, who, insisted that the murky domain between hot and cold war, "is arguably the most important phase of deterrence."[5] And, he noted, this is where SOF excels. A report from the Fort Leavenworth Army Lessons Learned Center echoed his thoughts. It stated:

> Pure military skill is not enough. A full spectrum of military, paramilitary, and civil action must be blended to produce success. The enemy uses economic and political warfare, propaganda and naked military aggression in an endless combination to oppose a free choice of government, and suppress the rights of the individual by terror, by subversion and by force of arms. To win this struggle, our

> officers and men must understand and combine the political, economic and civil actions with skilled military efforts in the execution of this mission. Regardless of the name we use—special warfare, counterinsurgency warfare, irregular warfare—one thing is for certain: it characterizes the nature of warfare we are experiencing, and will experience, for the foreseeable future. We must recognize that "pure military skill" will not be enough. While the ability to conduct high-end, direct action activities will always remain urgent and necessary, it is the indirect approaches, working through and with others in building a global network of partners, that will have the most decisive and enduring effects.[6]

This rationale is why SOF will always maintain a pivotal role in the GPC. Its characteristics and skill-sets are perfectly geared to irregular warfare and war in the shadows. SOF operations, and those who carry them out, are positioned to conduct clandestine, time-sensitive, high risk (i.e., political and to force) missions in hostile, denied, or politically sensitive environments. Much of the GPC is taking place in the obscure domains and in regions around the world where gaining access and influence to populations and regional governments is key. On this playing field, information warfare, the competition over narrative and gaining acceptance goes hand-in-hand with having impact (i.e., economic, military, political, social) on the ground. Dr. Jonathan Schroden elucidated, "access equals influence; influence equals alignment; and alignment equals power."[7]

SOF, through its military assistance / special warfare / irregular warfare programs such as SFA, Foreign Internal Defense (FID)[8] and UW allow for a low cost (both in personnel and financial terms) methodology of developing favourable foreign relations with friendly and at-risk states to further political objectives. Their ability to train foreign security forces to deal with real or potential threats also works to pre-empt crises before they become out of control or trigger larger conflagrations.

SOF operations around the globe also act to create networks and important "lily-pads" should the larger conventional joint force require basing options in times of crisis or war. In short, SOF programs develop access and influence that furthers advantageous foreign relations in support of national objectives.

Moreover, SOF's situational awareness around the globe through the cultivation of long-term partnerships and creation of networks provides

comprehension of emerging trends and threats worldwide. It also allows for influencing actors and events to coincide with desired outcomes. Admiral McRaven asserted, "SOF are rapidly deployable, have operational reach, are persistent and do not constitute an irreversible policy commitment." He emphasized that "military success in today's environment is about building a stronger network to defeat the networks that confront us." He underscored that "the [SOF global] network enables small, persistent presence in critical locations, and facilitates engagement where necessary or appropriate."[9]

In essence, SOF allows for continual competition under the threshold of war through its non-kinetic activities and targeting of key actors and audiences. Admiral Eric Olsen, another former USSOCOM commander, underscored the non-kinetic activities and targeting of friendly and at-risk states. He argued that "Direct Action is important, not decisive; Indirect Action is decisive."[10] He was not alone. "While the direct approach captures everyone's attention," acknowledged McRaven, "we must not forget that these operations only buy time and space for the indirect and broader governmental approaches to take effect. Enduring success is achieved by proper application of indirect operations, with an emphasis in building partner-nation capacity and mitigating the conditions that make populations susceptible to extremist ideologies."[11] He insisted that "The 'dead of night' direct-action operations will be fewer in number, while the more touchy-feely missions 'by, through and with' partner nations will increase."[12]

It is SOF's ability to excel at their non-kinetic mission sets that create security capability within partner nations; develop relationships and networks; target hostile agents, agitators, insurgents and terrorists; as well as promulgate a narrative that counters opponent disinformation; that makes SOF an important player in the GPC. As two SOF strategists assessed:

> SOF is uniquely positioned, across the globe to thoughtfully combine intelligence, information, space and cyber operations to affect an opponent's decision making, influence diverse audiences, and unmask false narratives. Furthermore, SOF can coordinate operations, activities, and actions in the information environment with those across the other operational domains and, as a matter of routine, fuse "cognitive" and lethal effects to obtain favorable outcomes. The SOF enterprise can inform more comprehensive understanding of adversary global operating systems and develop options that exploit vulnerabilities in those systems. Especially when paired with

> capabilities in the cyber and space domains, special operations allow the Joint Force to gain positional, political, or informational advantage in competition and enable a rapid transition to combat operations should the need arise.[13]

David Gompert, a former acting Director of (U.S.) National Intelligence, asserted, "any force prepared to address hybrid threats would have to be built upon a solid professional military foundation, but it would also place a premium on cognitive skills to recognize or quickly adapt to the unknown."[14] To this end, the special operator of today possesses the knowledge, skills, and essential abilities that are effective in counter-Hybrid Warfare. They tend to be well-educated, mature, flexible, resilient, adaptable and through experience able to operate and coordinate with other organizations under virtually any condition. Special operators, due to their exceptional physical qualities, skills and training, are adept at conducting no to low notice, high-precision, and high-risk tactical operations.[15]

And so, within the context of GPC and Gray Zone operations SOF fulfills a number of important roles:

Crisis Response

Crisis response remains a core task that SOF will continue to perform in the GPC. Unexpected, potentially hazardous events that occur often require highly-trained and educated operators who can work well in chaos and ambiguity. As such, SOF's characteristics position it to provide high-readiness, rapidly deployable SOF teams or Special Operations Task Forces (SOTFs) that can address a wide range of threats or problems and provide governments with situational awareness, intelligence, as well as kinetic and non-kinetic policy options to achieve political objectives.[16] SOF capability and low cost (i.e., fiscal and potential risk due to small footprint, high level of training and education of operators) provide decision-makers an immediate and effective tool to address crisis and chaos.[17]

Sensor

SOF expertise at Special Reconnaissance enables it to provide covert surveillance, observation and reconnaissance to provide governments and their militaries with ground truth and situational awareness. In contemporary jargon, SOF can provide "illumination" which in essence is clarity on what

is happening / has happened or what is likely to transpire. This function is extremely important since adversary actions are often shrouded with ambiguity and deceit. In addition, although alliance members and friendly nations share information and intelligence, each actor has its own particular national interests so it is essential that a country can determine ground truth for themselves, which allows them to make the necessary decisions based on credible information.

This SOF "sensor" role is also essential for information gathering, collating and processing into intelligence. It assists as a warning mechanism and individually or, in cooperation with partners, can assist in constructing a clear picture of occurrences in the security environment. As a function of the sensor role, SOF can also provide clear culpability with regard to actor(s) responsibility for security events and transgressions. Furthermore, through persistent surveillance and observation, SOF can also assist with the determination of adversary "intent."

SOF's sensor role can also extend to preparing / developing an environment for future special or conventional operations. SOF missions can develop a better understanding of key characteristics of a specific region, its population and physical attributes. This knowledge can assist with strategic messaging, countering disinformation, developing key networks, as well as targeting and enhancing potential future operations.[18] For example, in the six-year period prior to the outbreak of the war in Lebanon in 2006, a joint effort between the Mossad and the Israeli Defense Forces (IDF), which involved about 40 special operations, led Israel to glean intelligence concerning Hezbollah's strategic arsenal and command and control centres. This information proved vitally important in determining the success of Operation Density on the second night of the war (12 July 2006), during which the IDF destroyed about 90 per cent of Hezbollah's rocket arsenal.[19]

In sum, the SOF sensor role in the shadows of the GPC is instrumental in assisting governments understand what is transpiring in the security environment, who is responsible and to what end they are manoeuvring. This information is critical in determining policy options and decisions for governments. As an example, British SOF were sent to Kabul to monitor events as well as protect hundreds of British soldiers as they prepared to leave Afghanistan after twenty years.[20] SOF were also deployed to the Ukraine and other Baltic states to monitor events during the Russian 2022 invasion.

Signaler

Another role for SOF in the sub-threshold landscape of the GPC is to act as a signaler. SOF have become a universal representation of a nation's military elite. As such, SOF deployment carries a number of nuances, if not overt indicators. Specifically, the employment of SOF demonstrates intent, namely, the seriousness of a situation and the desire of a government to address the issue(s). This manifestation expresses intent to take action / respond; ability to deploy quickly with highly capable forces; and high level of support to alliances / coalitions / partner nations.

SOF scholars Will Irwin and Dr. Isaiah Wilson III explained:

> SOF can help to detect, monitor, and report on the covert and overt gray-zone activities of adversaries, illuminating their actions to better inform geographic combatant commands, country teams, JIIM-C partners, and national decision makers. This early warning function helps to eliminate strategic blind spots and improve situational understanding, reducing response time and creating course-of-action consideration and decision space.[21]

Similarly, other analysts have argued that "the overt forward deployment of SOF working with allies and partner forces in combat and on training missions communicates commitment on a very high level and affords access to information that would otherwise be obscured." They explained, "a continued forward SOF presence limits the threat posed by a strategic competitor by ensuring that would-be aggressor states consider de-escalation. Partnership commitment is clearly communicated to allies and adversaries alike."[22]

SOF can also "signal" warning of threat(s), as well as changes in the geopolitical environment to their national governments, the Joint Force, Other Government Departments (OGDs) and allies, which allows for timely, responsive decision-making and policy formulation. Moreover, SOF's ability to determine ground truth can be instrumental in assisting with the strategic narrative to ensure the proper accurate messaging is undertaken to disarm adversary disinformation and deceptive accounts, as well as take disruptive action if required.

Integrator

SOF, due to its activities, relationships and networks within both the national security and national defence domains, are positioned to act as an efficient

and effective integrator between SOF elements, the Joint Force, OGDs and allies. They provide the capacity to bring various actors together in either a leading or supporting role. SOF's understanding of, and experience working with, partners in both the national security and defence domains also allow them to become an important enabler by sharing contacts, doctrinal issues, TTPs and SOPs, as well as liaison and interoperability capacity. Additionally, SOF can "translate" capability and effects between partners and across the national security and defence domains. They can identify vulnerability gaps through their pan-domain knowledge and experience and enhance national security protection by assisting in coordinating capabilities and effects of all actors.

The integrator role is of the utmost importance as national resilience is increased through the cooperative, integrated "whole-of-government" approach, which is further augmented through alliance partners. Importantly, it allows for more rapid and comprehensive mitigation of crises by allowing for the integrated approach to mitigate damage caused by adversary action through the existence of experienced and tried C2 concepts, liaison officers and staff processes tested by practice and exercises.

Mark Mitchell, the American principal deputy assistant secretary of defense for special operations / low-intensity conflict, argued that the greatest role for SOF was "being in position globally as tensions rise [and] having a deep network in place on day one." He explained, "working with our partners and allies, training, collaborating, we've been able to nip a lot of things in the bud."[23]

Trainer

Another instrumental role for SOF in the GPC shadow wars is that of trainer. Highly capable and experienced SOF operators have conducted this function for decades. It is an essential task that provides huge dividends. Training partner nations:

- assists at risk nations to develop a more robust and capable security apparatus;
- cultivates deep networks and relationships across the globe;
- advances national and host nation capabilities (i.e., both military, as well as cultural);
- enhances interoperability within the SOF Global Network;

- demonstrates intent, commitment and capability, which also functions as deterrence;
- stymies adversaries from making in-roads into strategic geo-political areas of interest;
- creates resistance cells; and
- increases partner state national resilience.

The training function, specifically engagement with at-risk or partner nations, enriches deterrence by demonstrating commitment and capability. Researcher Evgeny Finkel in his 2015 work on Jewish Resistance in WWII, observed that urban resistance networks that possessed specific pre-war training and subsequent "toolkit" were more likely to operate effectively against superior forces as compared to groups that lacked such knowledge and experience. Finkel explained that the "toolkit" consisted of such capabilities as: communicating securely, possessing/acquiring weapons covertly, creating safe havens, conducting effective forging and identifying and neutralizing informers and infiltrators.[24]

A more recent 2021 study focused on WWII French resistance networks similarly determined that "resistance networks that were organized locally and later supported by coalition forces are more likely to be successful than those resistance networks that were organized during the conflict by foreign operatives inserted covertly into France." The researchers asserted operational security was a key element of a resistance network's survival and was in essence the necessary condition for success. They argued that pre-war local networks were more proficient in security measures than those organized by foreign operatives during the war, which led to a higher success rate in case of the former.[25]

The 2022 war in the Ukraine provides a contemporary example. SOF operators from the U.S. and other NATO countries had been in Ukraine for nearly a decade, establishing training centres, initiating training cadres, and building a capability that is credited with significantly disrupting the Russian advance on Kyiv. Ukrainian SOF operated behind Russian lines, effectively disrupting and destroying Russian equipment and personnel on their lines of communication.[26]

Importantly, the assistance continued as the war progressed. A covert network of SOF operators provided weapons, intelligence and training. Much

of the activities are occurring outside Ukraine, at bases in Germany, France and Britain. Although, a small number of operators from some NATO countries such as Britain, France, Canada and Lithuania, as well as CIA operators, continue to work inside Ukraine.[27]

SOF as a trainer during the pre-conflict period of an at-risk state is critical in fostering resistance networks and the relevant "toolkits" that will enable them to effectively combat numerically and potentially technologically superior adversaries.[28] There is substantial evidence to suggest that military partnering activities can not only build the tactical military capabilities of partner nations but also make them more resilient to instability or political subversion by hostile actors.[29] Therefore, SOF becomes an important enabler by consistently, and routinely, training and exercising with partner states and their resistance networks. This relationship building will develop trust, enrich mutual understanding and enhance interoperability, which in turn will maximize effectiveness and the ability to confront and repel armed confrontation.

Weapon System

The final SOF role in the shadowy GPC is that of a weapon system. Despite the American pivot to GPC to focus on great geo-political rivals China and Russia, the reality remains that the world is on fire. Terrorism and insurgency have not abated. In fact, terrorist movements persist to flourish and in locations such as Africa are continuing to grow and expand. In many instances, terrorist organizations and insurgents are supported, armed and encouraged by rivals as part of the strategic competition that is playing out worldwide. As a result, SOF capabilities in conducting CT, Counter-Violent Extremist Organization (CVEO) and Maritime CT (MCT) are very much relevant in the GPC, as is their expertise in COIN. The rise of ISIS and the devastation it wrought after the large-scale withdrawal by the Americans in Iraq and the reluctance of Western nations to re-engage after the fatigue from fighting in Iraq and Afghanistan in 2015 is evidence of the consequences of turning a blind eye to terrorism and insurgency. As former U.S. Secretary of Defense General James Mattis explained, "Terrorism is an ambient threat, it's out there just like the air we breathe. It's going to be something we're going to have to deal with throughout our lifetime and probably through the lifetime of our children's generation. It's a reality in the globalized world."[30]

Another potential role for SOF as a weapon system in the GPC is to conduct agitation, and subversion. These actions can be used to harass and / or distract adversaries, as well as degrade their political will. The 2014 Russian campaign in Ukraine is a contemporary example. "Little Green Men" undertook various missions agitating and assisting with protests to destabilize the government, blocking police and military garrisons, as well as working with separatist elements to destroy the credibility of the government and stability of the country.[31] Ukrainian sources also stated that approximately 150 GRU and Russian SOF operators had been in the city of Sloviansk for almost a month before the Donbas anti-Kyiv rebellion became full blown.[32]

SOF agitation and subversion can also work to undermine adversary relationships with other nations by discrediting their commitment or capability. For example, the discovery of a billboard with Chinese characters accompanying a photo of the southern Port of Harcourt triggered a Special Forces Operational Detachment-Alpha (3rd Special Forces Group) and a Psychological Operations Detachment (7th Psychological Operations Battalion) to take disruptive action. The billboard revealed a Chinese BRI initiative to construct a deep-water port in the Niger Delta. As a result, the SOF detachments undertook an influence campaign to discredit Chinese activities and impede the Chinese from purchasing land by igniting long-standing friction between Nigerian workers and Chinese companies. Their actions sparked protests around Chinese businesses in Abuja and within two weeks the Chinese construction company lost sixty per cent of its required labor pool for the port expansion. Importantly, the SOF team worked with the U.S. Embassy, USAID, and local NGOs to establish a job fair near the protest areas to provide disaffected Nigerian workers with employment.[33]

SOF can also actively work with resistance cells and / or local populations and host nation forces to disrupt and deny adversary attempts at gaining a foothold / access to areas of interest.[34] U.S. and NATO SOF are focusing on creating resistance networks that make invasions by Russia or China too costly for those powers to even attempt. The successful efforts of Ukrainian SOF demonstrate the value proposition of developing this capability. Not surprisingly, U.S. SOF are working with their Taiwanese counterparts to develop a similar capability.[35]

SOF can also undertake sabotage missions in the shadowy GPC Gray Zone. Avril Haines, director of national intelligence, explained that "sabotage

behind enemy lines is a fundamental element of special operations warfare. It's an integral tool for an insurgency or an army facing an opponent with superior numbers or equipment, as is the case in Ukraine." She explained, "such operations are designed to telegraph a capability that can be expanded across Russia and target platforms of increasing sensitivity and value to Putin. Strategically, sabotage operations offer Ukraine, the United States, and its partners the decided advantage of flexibility in ratcheting pressure up or down. With few overt options short of going to war, covert sabotage operations might prove to be a critical deterrent - if not the best and only remaining one."[36]

Sabotage was a key element of the Cold War where sabotage plans were a part of bigger strategy. Critical Energy Infrastructure (CEI) was the main objective of U.S. and Soviet agents who intended to destabilize an adversary's economy and disrupt their social stability.[37] For example, During the 1960s Soviet reconnaissance assessed that the Kerr Dam on the Flathead River in Montana was the largest power supply system in the world. In 1967, they developed Operation Doris, which was designed to find a vulnerability to attack the dam and simultaneously sabotage the Hungry Horse Dam on the Flathead River.[38]

The Soviets also developed Operation Target Granit which was a two-step plan designed to initially disrupt power lines and pipelines in specific areas of the United States. The Soviets believed this would create a massive black-out in the East and Midwest as well as massive pipeline fires in Texas and California. The second step would have entailed a strike against New York City. The plan was to attack a network of piers and warehouses that lined the Port of New York, which included ships' berths, warehouses, communications systems and port personnel.[39]

The final example during the Cold War was Operation Operation Kedr-Cedar, which took place between 1959 and 1971. The operation, conducted from the Soviet embassy in Ottawa, was a twelve-year mission that amassed a detailed plan of Canada's oil refineries, as well as oil and gas pipelines from British Columbia to Montreal. The potential targets were photographed and vulnerable points were identified. The intent was to be prepared to sabotage the oil and gas facilities in the event of war.[40]

The Russians continued to use sabotage as a key tool in the GPC. The first GRU operative was arrested on Ukrainian soil by the Ukrainian security service

SBU in March 2014. He was arrested together with three others while gathering intelligence on Ukrainian military positions on the Chongar Peninsula just north of Crimea.[41] Another Russian-GRU agent was killed in Kharkov in September 2014 during the execution of a sabotage mission. He was suspected of blowing up train wagons with air fuel at Osnova railway station. Ukrainian officials also claimed a combined groups of rebels and Spetsnaz-GRU agents increased their activities in Ukrainian rear areas in the summer of 2015. This activity included mine-laying and attacks at poorly guarded Ukrainian transport convoys.[42]

The possibility of sabotage during the GPC has pressed countries to increase their ability to detect, disrupt and stop adversary sabotage activities. For example, U.S. Navy SOF operators regularly work with Coast Guard personnel to practice defending critical infrastructure.[43]

Another potential role for SOF is the placement of sensors to provide real time visibility on adversary actions, as well as targeting information (as in the case of the killing of Iranian Quds commander Qasem Soleimani). In this latter example, U.S. SOF operators posed as airport maintenance staff at Baghdad Airport to coordinate the air strike that assassinated Iran's top commander. One report noted that they were joined on the ground by Kurdish special force personnel and assisted by remote help from phone-tracking experts in Israel.[44]

Importantly, SOF can also operate in the counter-SOF role to detect, disrupt, repulse and if necessary, destroy adversary SOF. This line of tasking also includes counter-UW operations to thwart adversary assistance to insurgent groups, influence target populations and remove nefarious actors that represent a threat to national security and global stability. Examples include the Israeli assassination of Colonel Sayad Khodayee, the IRGC's commander of Unit 840, responsible for assassinations and kidnappings. This killing was designed as a warning to Tehran to stop the operations of that covert military unit.[45] Israeli SOF also eliminated Mohsen Fakhrizadeh, the chief of Iran's nuclear program. Another example is the U.S. Delta Force raid that killed ISIS leader Abu Ibrahim al-Hashimi al-Qurayshi in Syria.[46]

Research has shown that decreases in leader availability and communications undermines organizational cohesion. The reductions in senior leader activity undermined al-Qaeda's organizational effectiveness, including its ability to retain personnel.[47] In a speech at the National Defense University in 2010

outlining his administration's counter-terrorism strategy, President Obama argued that al-Qaeda's "remaining operatives spend more time thinking about their own safety than plotting against us."[48]

Significantly, SOF as a weapon system can also contribute to deterrence through its ability to provide governments with a viable, credible (yet relatively restrained) counter-threat to adversary actions that test the "below the threshold of violence" benchmark. The ability to conduct covert or clandestine precision kinetic operations to strike adversary vulnerabilities as a retaliatory measure can have a restraining effect on adversaries.

In summary, SOF due to their characteristics and capabilities, provide governments with a versatile and effective means to both conduct operations and counter adversary actions in the shadowy Gray Zone of strategic competition. SOF's long-standing roles and tasks remain extant in the GPC environment. The myriad of challenges and changes to the operating environment have, and will continue to, require changes to, and constant review of, TTPs, SOPs and employment concepts. However, the core functionality of SOF, particularly because of their adaptability and reliance on the highly trained and educated operator, make them an effective actor, as well as key partner, in the GPC.

CHAPTER 8

Implications for SOF - GPC & High-intensity / Conventional War

The idea of the onset of a high-intensity conventional war is unfathomable to most, despite the shocking Russian invasion of Ukraine on 24 February 2022. Reasons to discount the incomprehensible march to war are normally anchored on a number of factors. First, a "hot" war would severely impact the stability and prosperity of the interconnected world that globalization has enhanced.[1] For that reason, the most current iteration of strategic competition, namely the struggle for access and influence to further national political objectives and disrupt, deny and defeat those of adversaries, as noted already, focuses mainly on activities below the threshold of armed conflict (e.g., cyber and informational attacks, leveraging economic power, sabotage, subversion, agitation, use of proxy forces).[2] The argument posits that no-one benefits from a conventional war, particularly against a major power such as the U.S..

Another argument under-cutting the credence of the possibility of a high-intensity war is based on the belief that the accessibility and proliferation of technology make the prospect of conflict so devastating that no state would risk engaging in all-out war. An increasing number of nations with substantial nuclear arsenals, as well as the global propagation of stand-off precision missile systems and platforms, including highly manoeuvrable cruise missiles, as well as hypersonic weaponry and glide vehicles, matched with networked sensors that are capable of delivering large payloads of munitions at increased ranges so that targets can be engaged and destroyed almost anywhere with accuracy within a short period of discovery and decision-making, make a high-intensity conflict a losing proposition for all belligerents.

In short, as already noted, the future battlefield will be characterized by augmented lethality, improved speed and boosted tempo of operations,

augmented informatization empowered through AI, increased complexity, and the forfeiture of traditional Western supremacy in all domains. Quite simply, conflict between belligerents using modern weaponry will be disconcertingly quick and horrendously destructive.

The formidable capabilities of current and emerging technology and munitions makes the fielding of large conventional armies and their platforms laden with risk. Augmenting the difficulty is the proliferation of EW, cyber-attacks and weaponry capable of destroying operation-critical space satellites. The development and deployment of AI and autonomous systems only adds to the difficulty.[3] As such, for most, the prospect of a high-intensity war is highly unlikely, if not negligible.

However, never say never. Through design or miscalculation, the occurrence of a major conflict between peer, near-peer and / or regional powers can never be discounted. History is replete with instances of unexpected attack. Examples include: the German invasion of the Soviet Union on 22 June 1941; the North Korean assault on its southern neighbour on 25 June 1950 and the Chinese engagement later in October; the Egyptian crossing of the Suez Canal and assault on Israeli forces in the Occupied Sinai Peninsula on 6 October 1973; the seizure of the British Falkland Islands by Argentina on 2 April 1982; the invasion of Kuwait by Iraq on 2 August 1990 leading to the First Gulf War; and finally, the Russian invasion of Ukraine on 24 February 2022. Moreover, the continuing tensions and Chinese provocations across the Taiwan Strait, provide another recent disturbing example of how through design or miscalculation a high-intensity conflict could erupt.[4]

The point is, discounting a possible eventuality leads to punishing consequences. It is always important to anticipate possible events, which allows for quicker adaptation and change should the inconceivable occur. Having considered, brain-stormed, and war-gamed possible scenarios, organizations and institutions have, at a minimum, a conceptual idea of what the challenges, as well as possible roles, tasks and requirements will be.

With regards to SOF and high-intensity war, this contemplation and planning is extremely important. Afterall, for the SOF community the previous two decades have been focused almost primarily on CT and COIN. Importantly, these activities were conducted with virtual overmatch in every domain. SOF forces had freedom of manoeuvre on the ground, sea and air. They had technological and informational overmatch, as well as supremacy in

intelligence gathering and firepower. In short, they held advantage in virtually every aspect of the conflicts in which they were engaged. This prolonged advantage and sense of superiority tends to build strong habits and can blind organizations to systemic weaknesses and / or shortfalls. It builds a false sense of security, if not capability, particularly for engagement in operations that have not been conducted for decades against peer or technologically advanced and equipped adversaries.

It is for this reason, that as unlikely as many feel the prospect of a "hot" war between major international actors may be, SOF must expend some intellectual effort in understanding high-intensity conflict and the corresponding implications, particularly the challenges and potential requirements, as well as determining possible roles and tasks, so that SOF can best provide employment options to senior political and military decision-makers.

The role of SOF in a high-intensity war is not without precedent. Although every conflict has its own unique characteristics, or in Clausewitzian terms "grammar," four examples from contemporary military history provide some insight into SOF roles and tasks during high-intensity war (albeit not between two great powers). The first example is the 1982 Falklands War between Great Britain and Argentina over the Falkland Islands in the South Atlantic. Throughout this relatively short conflict Argentinian special forces, as well as both the British 22 Special Air Service Regiment (SAS) and the Special Boat Service (SBS) conducted operations.

The Argentinians utilized their special forces (SF) to initiate the assault and capture of the islands with attacks on Moody Brook Barracks and Government House. They also used their SF for aggressive patrolling, as well as attacks on designated highly-important objectives throughout the conflict.

Similarly, the British Task Force Commander utilized the SAS, as well as the SBS for a myriad of tasks during the conflict. During the Falklands campaign British SOF conducted:

- Strategic and tactical intelligence gathering (by conducting active fighting patrols and covert observation posts);
- Close target reconnaissance of identified facilities and targets;
- Direct Action assaults against static targets and targets of opportunity;
- Diversionary raids to confuse, delay or inhibit enemy movement;
- Domination of no-man's-land between enemy positions;

- Sabotage or destruction of critical facilities (active airfields, communication lines, fuel storage areas, command and control locations); and
- Direct forward air control of fighter aircraft and naval gunfire support against identified targets.[5]

The first mission the SAS undertook was Operation Paraquat, the recapture of South Georgia Island. In atrocious weather conditions "D" Squadron (Sqn), as part of a small subordinate Task Force that included a company of Royal Marines and SBS personnel, sailed south to retake the British possession. South Georgia itself was of little military consequence, however; the task itself was of great strategic importance. After a number of British ships were sunk by Argentinian aircraft, the British Government needed a quick victory. Therefore, South Georgia became an important political requirement. After a number of set-backs, elements of "D" Sqn conducted a hasty attack, captured the Argentinian garrison and reclaimed the island, providing the British Prime Minister with the immediate "win" she required.

British SOF were also instrumental in establishing observation posts (OPs) to monitor and conduct surveillance on Argentinian movements of troops, aircraft and equipment in the Falkland Islands. The information they provided was quickly transformed into critical intelligence that assisted the Task Force Commander's battle plans. In the same vein, aggressive patrolling by both the SAS and SBS fulfilled a similar function.[6]

In fact, SOF reconnaissance and observation brought to light the potential danger of an Argentinian airfield on Pebble Island. This air base essentially provided the Argentinian forces the ability to strike naval, land and air targets (such as Sea Kings) in the San Carlos operational area within minutes of taking off from their airfield. This advanced base ensured British forces operating in the area would have very little warning. As a result, the SAS launched a raid, which harkened back to SAS airfield raids in North Africa during WWII. The daring raid destroyed all eleven enemy aircraft, as well as demolishing the runway and a fuel depot.[7]

Additionally, British SAS and SBS elements conducted beach reconnaissance, supported the main Task Force landings at San Carlos, conducted diversionary attacks at Goose Green and Wireless Ridge to support 2 Parachute Regiment, and led the initial assault on the strategic heights of Mount Kent.

Another task that was initially intended for British SOF was Operation Mikado, the plan for SAS operators to destroy Argentinian Étendard strike fighters and their Exocet missiles on their mainland airbase at Rio Grande, Tierra del Fuego. The British Director Special Forces, General Sir Peter De La Billiere, was a staunch protagonist for the mission. He envisioned landing two British C-130 Hercules transport aircraft loaded with approximately 60 SAS operators and their vehicles directly onto the tarmac at Rio Grande airbase. The SAS would then disgorge from the aircraft, similar to the Israeli mission at Entebbe years earlier, and destroy the Étendard fighters, the remaining Exocet missiles, as well as the pilots in their quarters.[8] The aircraft and SAS "B" Sqn deployed to the staging base at Ascension Island, but the British Prime Minister did not authorize the raid in the end.[9] In all, British SOF played an instrumental role in the Falklands campaign.

SOF was once again employed in a high-intensity conflict between 2 August 1990 and 28 February 1991, during the First Gulf War. Coalition SOF conducted:

- Special reconnaissance;
- Foreign Internal Defence (i.e., training allies and partner forces);
- Liaison / Joint Terminal Attack Controller (JTAC) activities;
- Direct Action;
- Diversionary activities;
- Visit, Board, Search and Seizure in the Persian Gulf; and
- Unconventional Warfare.

Special reconnaissance, particularly OPs along Saudi-Kuwaiti border to monitor Iraqi movements, was the first SOF task that was undertaken. SOF also penetrated into Iraq and they ensured the route for the "left flanking" of the Iraqi positions was suitable to support the movement of Abrams heavy tanks.

Equally important, SOF trained Coalition partners, particularly non-NATO members, to ensure they could operate in a coalition setting. This task was especially important to hold together the multi-national partnership. As such, SOF was also embedded in coalition units to serve as liaisons, primarily to coordinate close-air-support.

In addition, SOF conducted Direct Action. They seized oil platforms, destroyed Iraqi fiber-optic communication cables, blew up microwave relay

towers and communication bunkers and attacked enemy vehicles, "painted" enemy targets for close-air-support, recaptured the British embassy in Kuwait City and in what is probably their most well-known public mission, hunted SCUD missile Transporter-Erector-Launchers (TEL), a strategically essential task that was critical to maintaining the Coalition by keeping Israel from retaliating against Saddam Hussein's continued SCUD missile attacks on Israeli soil.[10] SOF were given the difficult task of locating and destroying the mobile launchers.[11]

SOF also conducted diversionary raids on the coast to deceive the Iraqis into thinking that a large-scale amphibious operation was looming. Additionally, U.S. SEALs conducted VBSS operations in the Persian Gulf, often raiding suspicious ships. Finally, SOF teams were also assigned to work with Kuwaiti resistance, rescue key civilians trapped behind enemy lines and capture Iraqi military personnel.[12]

SOF was also employed in high-intensity conflict in the Second Gulf War, namely the invasion of Iraq on 19 March 2003. During this conflict Coalition SOF conducted:

- Special Reconnaissance;
- Direct Action;
- JTAC activities;
- Support to Conventional Forces;
- Sensitive Site Exploitation (SSE);
- Hostage Rescue Operations; and
- Unconventional Warfare.

Similar to the previous two examples, SOF was instrumental in conducting special reconnaissance to identify Iraqi positions and movements, particularly to monitor the Karbala Gap. Additionally, Direct Action was a key activity for SOF. At the onset of hostilities, they eliminated Iraqi border observation posts and once again, hunted down SCUD TEL launchers in the Western desert. Furthermore, SOF seized the Haditha Dam complex, conducted ambushes on the highway to Tikrit to tie up Iraqi forces, "painted" enemy targets and vehicles for close-air-support and they captured high value targets (HVTs) attempting to flee to Syria. SOF also eliminated Uday and Qusay Hussein, captured their father Saddam Hussein and killed the al-Qaeda

in Iraq (AQI) leader, Abu Musab al Zarqawi. They also captured or killed over 100 AQI members including at least eight high value targets. In addition, Coalition SOF seized national oil production facilities, as well as capturing key infrastructure and transport nodes. A Naval Task Group also seized Umm Qasr, Iraq's only deep-water port, the oil production facilities of the Al Faw Peninsula and two off shore platforms that the pipelines fed.[13]

Support to conventional forces was also a significant undertaking. SOF conducted screening tasks in support of conventional forces, captured strategic sites to allow follow-on conventional forces to deploy, supported the seizure of Rumaylah oilfields and worked with local Sheikhs and their militiamen to capture a key town infrastructure, as well as to establish a police service and restore 80 percent of the town's electricity within a fortnight. They also reopened schools and hospitals all in support of conventional force thrusts in the area.

SOF were also instrumental in conducting a number of high priority SSEs, particularly in suspected Weapons of Mass Destruction (WMD) sites. Furthermore, Coalition SOF successfully conducted hostage rescue operations, saving Private Jessica Lynch, three Italian contractors, as well as three NGO workers. Finally, SOF worked with local Kurdish Peshmerga forces to draw Iraqi forces away from reinforcing Baghdad, as well as capturing strategic sites to allow follow-on conventional forces to deploy.[14]

The final example is the Russian invasion of Ukraine in February 2022. Although at time of writing the invasion is still relatively in its early days and as such verifiable, comprehensive data is not completely possible, what information has percolated reveals SOF have played a part in that war as well. Preliminary information points to SOF being used for:

- Providing special reconnaissance;
- Shaping the ground for follow-on forces (penetration of Kyiv);
- Man-hunting (attempts to assassinate Ukrainian and other high value targets);
- Targeting (both opponents);
- Disrupting lines-of communication (Ukrainian SOF); and
- Sabotage.

Russian SOF figured prominently at the beginning of the invasion. Intelligence sources reported that Russian SOF entered Kyiv, some dressed in

Ukrainian uniforms, far in advance of their invading columns. Their task was to both storm the government district and capture, or kill, Ukrainian President Volodymyr Zelenskyy and his entourage.[15]

In addition, during the initial 48 hours of the invasion, Russian Spetsnaz and airborne forces exerted a great effort in attempting to seize the Hostomel Air Base near Kyiv. Although they captured it quite quickly, they were not reinforced and a Ukrainian counter-attack almost reversed the initial success.[16]

Ukrainian SOF also played an important role both undertaking sabotage and direct action, as well as working with resistance cells. Reports of sabotage, attacks and subversion behind Russian lines surface every few days. Events included the destruction of an armoured train, a grenade attack on a command post, the demolition of railway tracks, the explosion of a radar station, as well as a collaborator's house, and a pro-Ukrainian rally. Ukrainian officials claim its partisans have killed more than 100 Russian soldiers behind enemy lines in Melitopol alone. Additionally, mysterious fires and explosions at military facilities inside Russia itself have also occurred. Not surprisingly, Ukrainian special forces are also targeting Russia's lines-of-communication, as well as Russian long-range artillery and other weapon systems.[17]

Ukraine's underground resistance in occupied territories is coordinated by a special forces unit called the *Sily spetsial'nykh operatsiy* (SSO), which was formed in 2015 after attempts at partisan activity failed disastrously in the early stages of the war in the Donbas. The SSO is responsible for military action, support operations and psychological warfare. The SSO spent considerable effort preparing potential partisans prior to the invasion. The current resistance cells mix professional soldiers and volunteers in a 60-40 ratio. Moreover, a network of secret arms dumps, safe houses and potential sympathizers exists across the entire country. In some cases, criminal networks have been co-opted.[18]

The results have been noteworthy. Communication intercepts by Ukrainian security services revealed the level of impact the resistance movement has had. "Every fucking night we're fighting with diversionary groups who come into the village," one Russian soldier related in a call home. "Some of us have had enough. We're getting the fuck out of here," he asserted.[19]

In all, the missions conducted by SOF in these four conflicts were in essence largely the same tasks as SOF performed in WWII (e.g., raids, reconnaissance,

deception, unconventional warfare). Granted the examples reflect a great power (i.e., U.S., Britain and Russia) against regional powers and not peer or near-power adversaries. Nonetheless, the belligerents in all four examples had access to state-of-the-art weaponry and technology. As such, the conflicts in question provide insight into potential SOF employment and tasks.

Potential Tasks

Despite the mostly dated examples, and although circumstances have changed (i.e., the availability and proliferation of advanced munitions, sensors, weapon systems, as well as ISR capabilities) most, if not all, the enduring SOF tasks remain relevant. If SOF were to become involved in a contemporary or future high-intensity war between peer, near-peer or regional power adversaries they could expect to undertake the following potential tasks:

- Special Reconnaissance;
- Advanced Force Operations (AFO);
- Preparation and Shaping of the Operational Environment (e.g., staging, reception, navigation aids, establish austere airfields);
- Theatre Break-in;
- Direct Action;
- Target Designation;
- Battle Damage Assessment;
- Hard Target Defeat;
- Contingency Operations;
- Deception / Diversion / Disruption;
- Sabotage;
- Irregular Warfare (i.e., UW, CT, COIN);[20]
- Second Front / Horizontal Escalation;
- Counter-SOF;
- Counter-Shipping;
- Chemical, Biological, Radiological, Nuclear (CBRN) SSE;
- Role in Phase IV (stabilization);
- Psychological Operations (PSYOPS); and
- Economy of Effort operations.

SOF through their high readiness, rapid-deployability, superlatively trained and educated personnel and integral proficiencies, techniques and methods of employment make them an ideal partner to assist the Joint Force fight. Their ability to conduct special reconnaissance, as well as AFO, in hostile, denied, or highly sensitive environments allow them to "sense" (i.e., determine changes within a theatre, confirm events, specifically threats) and "signal" (i.e., provide ground truth and warning) to governments and military commanders.[21] In addition, they are adept at shaping and preparing, as well as breaking-in to theatres in support of the Joint Force. Although ISR assets are irreplaceable, clever camouflage and deception of armaments and weapon systems by adversaries, as well as physical destruction of, or electronic interference with, friendly ISR assets can create a veil of darkness. SOF can "illuminate" these gaps and provide decision-makers and the Joint Force with the necessary information for planning, deployment and actual operations.

Additionally, SOF are highly-capable of conducting Direct Action against critical infrastructure, command and control nodes, weapon systems (e.g., A2/AD, nuclear weapon launchers) and lines-of-communication. Specifically, SOF become an essential enabler for the Joint Force by eliminating hard targets (e.g., fixed defences, missile batteries, nuclear launchers, headquarters), as well as disrupting enemy lines-of-communication through either Direct Action or through target designation by JTACs.[22] Equally important, SOF can conduct battle damage assessment (BDA) to determine effectiveness of friendly strikes to ensure the necessary results have been achieved.

For example, during the 2006 Lebanon War the IDF employed SOF for raids against Hezbollah's command and control structure. The raids were designed to disrupt C2, destroy enemy capability, as well as to capture senior Hezbollah officials. On 4 August, Shayetet 13 conducted a seaborne assault and took control of a compound in the city of Tyre, which resulted in the annihilation of an enemy unit. Three days later, Shayetet 13 conducted another similar operation in the village of Ras al-Biyad, where an apartment complex was targeted. Additionally, Sayeret MATKAL assaulted a Hezbollah headquarters in the Beka'a Valley for intelligence-gathering purposes and once again in an attempt to capture operatives of the organization. In each of the cases, the capture or killing of high-ranking Hezbollah officials was a primary task.[23]

SOF can also conduct contingency operations that require a rapid response, precision and high reliability of success. SOF's characteristics position them to be highly responsive to situations that occur that were unforeseen (and

no contingency plans in place to address) or that create such a threat or crisis that immediate action is required for either existential, operational or political / morale reasons.

SOF operations can also assist the Joint Force through deception, diversion and / or disruption operations. By staging feints, holding attacks, diversionary strikes or harassment in adversary rear areas or lines-of-communication, SOF can tie down enemy forces, divert their attention away from critical areas and disrupt their intended operations. Moreover, sabotage of key infrastructure, as well as disruption of their lines-of-communication can curtail enemy capability and tie down enemy forces for vital point / rear area security.

Yet, another important task SOF can conduct in a high-intensity conflict is irregular warfare, defined as a "violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s)."[24] Irregular warfare is an important tool for friendly forces. After all, irregular warfare concentrates on indirect and asymmetric approaches to avoid the military strengths of an adversary. From a U.S. doctrinal perspective, irregular warfare includes the specific missions of UW, stabilization, FID, CT and COIN.

SOF conducting irregular warfare act as both a force enabler, as well as an economy of effort capability. Leading UW operations (i.e., working with host-nation forces behind enemy lines) SOF can tie down adversary troops needed for rear-area security, disrupt enemy operations and activities, destroy adversary infrastructure, equipment and their war effort in general.[25] UW operations can also be used to create "second fronts" or horizontal escalation by inserting small teams, who, working with resistance cells / guerrilla groups, can foment new theatres of operations to which adversaries must devote resources.

Irregular warfare operations also represent a critical ongoing, enduring task for SOF. A high-intensity war will not create a pause in undertakings for the myriad of global terrorist organizations that exist. In fact, many would probably increase their attacks believing major powers will be consumed by the larger conflict. As such, FID, CT and COIN all become critical activities to assist allies, friendly or at-risk nations deal with internal security issues that could evolve into larger security issues for not only single states, but allies and partners as well. For instance, as the current tranche of strategic competition smolders, insurgency and terrorism remain rampant in Africa and the Middle East. SOF conducting irregular warfare operations can have

both an offensive and defensive function, as well as an economy-of-effort effect by keeping these threats in check.

Undeniably, irregular warfare is a formidable means of striking at an adversary. It is one methodology that both the Chinese and Russians wield authoritatively. Therefore, "counter-SOF" becomes another important task. Ensuring enemy SOF are unable to conduct UW behind friendly lines, interfere with lines-of-communication, and / or interfere with command and control are extremely essential. Additionally, denying enemy SOF the freedom of movement to conduct special reconnaissance, AFO, break-in operations, direct action and / or targeting becomes imperative. Although conventional forces can certainly undertake rear area security tasks and vital point security, enemy SOF that have been similarly selected, trained and equipped, with analogous TTPs and operating methodologies to their Western counterparts, will pose a substantial test.[26]

As an example, North Korean special-operations doctrine emphasizes speed and surprise. Pyongyang's SOF have two fundamental missions: to infiltrate South Korea and conduct unconventional warfare and sabotage on the U.S. and South Korean rear lines-of-communications, and to defend North Korea against U.S. or South Korean SOF. On the onset of war, North Korean would quickly cross the Demilitarized Zone and flood South Korea with troops. Meanwhile, North Korean SOF would conduct operations in the rear or on the flanks, attacking supply lines, C2 centres, as well as other strategic facilities. They would also attempt to strike against South Korea's leadership, seeking to decapitate the South Korean government and sow confusion in the initial hours of the conflict.[27]

The capability of adversary SOF should never be underestimated. Therefore, counter-SOF operations will require significant planning, coordination and mitigation strategies for the plethora of challenges that will pose hurdles to success. Anticipation of these potential quandaries and contingency plans that allow for adaptation and rapid response are the first step. Counter-SOF employment, particularly for high-value infrastructure, events / operations and / or geographically vital areas, etc., will be necessary.[28]

For this reason, some steps have already been taken. Shemya Island, Alaska, which is in the Aleutian Islands and is home to the AN/FPS-108 Cobra Dane early warning and tracking radar used to spot incoming ballistic missile strikes provides an example. It possesses a strategic 10,000 foot airfield

with associated infrastructure and ample ramp space. Together, they would be a prime target during a conflict as it is also the closest military facility to Russia's eastern flank. With adversary SOF in mind, Special Operations Command NORTH (SOCNORTH) operators, in conjunction with Army Green Berets from the 10th Special Forces Group, deployed to Shemya to practice defending the island in cooperation with the local security forces.[29] The concept of counter-SOF operations must be considered on a larger scale.

SOF can also undertake a host of other tasks. Counter-shipping to interfere with adversary maritime operations or supply can have a seriously detrimental impact on the enemy's war effort. For nations that embed PSYOPS with their SOF forces, this task can have serious consequences on targeted adversary forces and / or populations, as well as on affected populations in theatres of operations and international targeted audiences that may be neutral or wavering on support.

SOF can also play a valuable role in conducting SSE on high value objectives, particularly headquarters, CBRN facilities (e.g., storage sites, laboratories, launch vehicles) and communication hubs. Finally, SOF can also contribute to post-hostility Phase IV Stabilization operations. Working with friendly or at-risk states, SOF can employ FID to assist with the reconstruction and / or establishment of the necessary security infrastructure to ensure a stable and secure environment for reconstruction and development.

Although the enduring nature of these SOF tasks is not surprising, the difference lays in the daunting challenges that the proliferation and access to modern precision munitions and technology available to adversaries pose to SOF operations.

Challenges

Undoubtedly, there would be innumerable challenges to SOF operations in a high-intensity conflict. As mentioned earlier, the proliferation of accessible, relatively cheap, advanced satellite, informational, sensor and weapon technology has levelled the playing field between belligerents in many aspects. Remaining hidden and simply moving has become extremely difficult. Precision, range and lethality of munitions, as well as the efficacy of sensors and radars, has become frighteningly effective. The decades-long advantage of technological, informational and firepower overmatch is no longer a given. Neither is freedom of manoeuvre on land, sea or air. SOF must examine

carefully the impediments they will face and the means to overcome those obstacles.

In short, similar to the challenges articulated as part of the greater GPC, some of the challenges that SOF will encounter in high-intensity include:

- Command, Control, Communications and Computers (C4);
- AI / machine learning;
- Speed / tempo;
- Capacity;
- Cooperation with the Joint Force;
- Self-image / failure to evolve;
- Lethality / Advanced technology;
- Direct Energy Weapons;
- A2/AD (theatre entry / manoeuvre);
- Freedom of manoeuvre / mobility;
- Aerospace Control;
- Concealment (i.e., sensors, CCTV, cell phones);
- Risk Acceptance;
- CBRN battlespace;
- Supporting fires;
- Adversary SOF;
- Influence Activities / Influence local populations;
- Domestic support / trust; and
- Mental health.

A major concern will be the nexus of C4 (command, control, communications and computers), AI / machine learning and speed / tempo of operations. The use of AI will press tempo to limits not yet experienced in conflict. Decision-cycles will be collapsed and decision-making pressed to extremes as belligerents try to make sense of what is occurring and what capabilities still exist. Jamming, cyber-attacks as well as the destruction of satellites and relay stations will stress communications, endanger the ability to utilize supporting fires, as well as the capacity to control operations at all once they have crossed the "start line." The recent successful test of a Russian ground-launched missile that destroyed a defunct space satellite should raise

alarm since this advancement jeopardizes the ability to potentially use satellites that enable much of society and the military.[30] SOF will be required to operate for extended periods of time disconnected and on their own.

Capacity will also pose issues for SOF in high-intensity warfare. With the myriad of potential tasks how will SOF missions be prioritized? There just simply isn't enough SOF capacity to deal with all the required missions.[31] Once casualties are factored in the issue becomes even more difficult. A clear prioritization of tasks, as well as a concerted effort to educate commanders to fully understand the best utilization of SOF to avoid needless casualties must be in place. This requirement raises the issue of cooperation with the Joint Force. A robust framework and deep understanding of how the conventional force and SOF can complement one another, as well as a concerted effort at ensuring inter-operability, are required prior to any conflict erupting. Working together the Joint Force and SOF can provide effective capability, however, to achieve this outcome a clear and cogent understanding of requirements, strengths and limitations of all actors must be in place prior to conflict.

Without diminishing the aforementioned challenges, arguably, the greatest test facing SOF in a high-intensity conflict will be the issue of lethality due to advanced technologies. Hypersonic missiles, such as the one tested by China, which flew around the world at more than five times the speed of sound, then dropped off a hypersonic glide vehicle that struck a target in China, pose huge threats. Importantly, unlike intercontinental ballistic missiles that travel in a predictable arc and are trackable by long range radars, a hypersonic missile moves much closer to the earth, making it difficult for radars to detect.[32]

Furthermore, the exponential proliferation of precision missiles with ever-increasing destructive power, directed energy weapons and autonomous systems capable of loitering and swarming targets bodes ill for forces that are discovered in the battlespace.[33] The increased precision, payload and density of munitions make concealment, manoeuvre and access into theatres or specific objective areas increasingly difficult and deadly. Moreover, mobility itself becomes a critical concern as outright superiority in any one domain is questionable. Bereft of outright superiority, adversaries will struggle for control over specific corridors for restricted periods of time and even that will be difficult to achieve. One analyst explained:

> Some specialized methods of insertion may remain viable, such as

> subsurface delivery, but even here the target may be well inland, while maritime deployment limits the equipment that can be taken ashore. Long-range patrols will need to mitigate observation from enemy radar, electronic warfare units, and unmanned aerial vehicles with mounted thermal cameras. While it may be comforting to hope that technology will shield special operations forces from enemy attention it seems more realistic to minimize signature rather than attempt to conceal it.[34]

The overarching threat becomes the marriage of sensor / detection to shooter / munition precision and lethality. The danger of sensor to shooter timeliness and accuracy was demonstrated by the Russians in the Ukraine since 2014. They had "shortened to mere minutes the time between when their spotter drones first detected Ukrainian forces and when their precision rocket artillery wiped those forces off the map."[35] The use of AI, space-based weapons, lasers, directed-energy technology and high-powered microwaves, as well as CBRN munitions, will only increase lethality and reach. Importantly, well-timed and accurate delivery of ordnance has become increasingly possible since the world has become one big sensor, making masking military deployments or actions virtually impossible. As such, SOF may need to survive unsupported, which will require a recalibration of the force's training, equipment, and mindset.[36]

In addition, next-generation high-power radio frequency-directed energy weapons that can disrupt electronic controls and shut off vessel engines without harming occupants, as well as millimetre wave active denial–directed energy technology further complicate the battlespace. Additionally, motor-powered exoskeleton suits that increase human capacity to carry weight or cover distances already exist. The use of armour plate, weapon suites and jet-packs for flight are just a matter of time.

In the final analysis, the future battlespace, or engagement space to use the most current lexicon, will be characterized by amplified lethality, heightened speed and tempo of operations, magnified informatization empowered through AI, increased complexity, and the forfeiture of traditional Western supremacy in all domains. Conflict between belligerents using modern weaponry will be ominously swift and dreadfully destructive. Adding to the enormity of the challenges are a myriad of other difficulties. Risk acceptance will have to be reviewed. In the context of the past two decades a premium has been placed on low casualties to friendly forces as well as limiting, if not negating, collateral damage. In the context of a high-intensity war, the

reservation of "causing harm" will need to be reviewed. Restraint in undertaking operations because of probable cause in death and destruction can put success against adversaries, as well as lives of friendly forces, at great peril.

Related to potential casualty rates and collateral damage is the issue of influence activities. Whether involved in irregular warfare or in operations in direct support of the Joint Force, SOF will need to place emphasis on gaining / maintaining the support of domestic and local populations, as well as influencing host-nation / local populations and international opinion / support. Support and trust of societies and their governments equals freedom of manoeuvre. It also translates into direct support in the way of passage of information, denial of the same to the enemy, as well as acceptance of set-backs and errors. The challenge lies in the difficulty of earning trust, particularly of alien cultures. The proliferation and sophistication of disinformation and "deep fakes," that is "highly realistic and difficult to detect digital manipulations of audio or video" is making it easier than ever to disseminate false information purporting to portray someone doing something or saying something that is detrimental to their credibility or reputation. As technology develops and spreads, deep fakes will push disinformation to an entirely new level.[37] Within this environment SOF will be required to win "hearts and minds" while combating aggressive disinformation campaigns.

In response to this requirement, U.S. Marine Forces Special Operations Command (MARSOC) issued clear direction. It stated, "Our units must be able to thoughtfully combine intelligence, information, and cyber operations to affect opponent decision making, influence diverse audiences, and counter false narratives." It added, "Furthermore, we must be able to synchronize operations, activities, and actions in the information environment with those across operational domains and, when necessary, fuse cognitive and lethal effects.[38] The MARSOC direction noted:

> [Marine SOF] Raiders must be able to seamlessly integrate a wide range of complex tasks; influencing allies and partners; developing an understanding of emerging problems; informing decision makers; applying national, theater, and interagency capabilities to problems; and fighting as adeptly in the information space as the physical.[39]

Additionally, adversary SOF will also pose a significant challenge. As mentioned earlier, enemy SOF will be employed comparably to friendly SOF both in an offensive and defensive context. Forces that have been similarly selected, trained and equipped, with analogous TTPs and operating meth-

odologies, will pose a substantial threat. Operations will require significant planning, coordination and mitigation strategies for the plethora of challenges that will pose hurdles to success. Anticipation of these potential quandaries and contingency plans that allow for adaptation and rapid response are the first step.

The final challenge to be discussed is that of SOF self-image and a failure to evolve. For the past two decades SOF have been regularly touted as the "Force of Choice." Media in its fullest form (e.g., television, movies, social media, books, internet, video games, etc.,) have all created a larger than life image of SOF warriors. Much of this has been deserved as SOF have been a significant, if not overpowering, contributor to the "war on terror" and the spate of COIN and CT operations in the new millennium. However, an acknowledgement of the theoretical construct of SOF involvement in a high-intensity war is not enough. Habits die hard, particularly when they have been rooted in success. As such, the past twenty years of dominance in all aspects and domains of conflict can have a numbing effect on what changes are required to succeed in a new paradigm. As one analyst observed:

> The high tempo of Western special operations forces' activity over the past two decades has led to repetitive behaviors and the formation of a set of persistent patterns. Before operators arrived in Sana'a, for example, specialist kit would often be flown in by C-130 and picked up by the embassy, giving Yemeni customs workers a fairly reliable indicator that something was going to happen...the widespread collection of biometrics and the pervasive surveillance and archiving of data from public spaces, combined with the existing target decks established through the observation of counterterrorism operations, mean that theater entry in a covert posture against a great power competitor requires careful planning, novel techniques, and a credible digital past to support any false identities…Against a peer adversary long-range standoff will force back insertion capabilities so that special operations forces will need to conduct an extended approach to the objective. They will need to look after themselves for a prolonged period in the field. They will need to minimize their emissions, which will require them to be unplugged from support by the joint force and necessitate that commanders are comfortable with only intermittent updates on their progress. The detailed planning necessary to operate undetected in an electronically contested environment will require a slow and deliberate tempo of opera-

> tions. As with the challenges in covert operations there are cultural implications to how units prepare for fighting unplugged. Special operations forces have become accustomed to multiple successive short operations, rather than prolonged periods in the field. This is reflected in equipment: significant advances in the ergonomics of tactical gear, for example, have not been matched by advances in systems for carrying heavy loads long distances. It is even evident in the physiology of personnel. Within many units it is noticeable that operators who became lean to pass the endurance tests they faced in selection rapidly bulk up their upper bodies upon joining their units. While this allows for speed and power—ideal for raids—it comes at the expense of endurance. And there is a reflexive tendency to reach for technology to observe adversaries, such as the use of unmanned aerial systems that necessarily have a significant electronic signature. If units must increasingly operate at reach then dependence upon technological tools also risks exposure. Finally, as with the problems with pattern forming in a discreet posture leading to the exposure of covert forces, communications patterns used during exercises will form a set of expectations among adversaries. As a result, operators cannot simply rely on communications procedures that emphasize the usual equipment, but should design them with a conscious assessment of the mission, the threat, and the enemy's expectations.[40]

The observations are a stark reminder of the challenges that exist. As the researcher explained, "The high tempo of Western special operations forces' activity over the past two decades has led to repetitive behaviors and the formation of a set of persistent patterns."[41] Quite simply, old habits die hard. After almost twenty years of CT and COIN operations, where they held overmatch in every domain, SOF have "fallen into predictable patterns, become overly reliant on technological solutions, and grown accustomed to short operations enabled by overwhelming support." As a number of analysts have warned, "Failure to recognize the changes in the operating environment may carry a heavy price."[42]

Importantly, since you cannot build SOF capability overnight, SOF cannot afford to "learn through experience," which normally entails casualties in a high-intensity conflict. Therefore, careful consideration and thought must be applied to this issue, including the aspect of mental health, which will undoubtedly be a major factor in the high-stress, high-tempo, lethal, battle-space of high-intensity conflict. As a MARSOC future employment

assessment notes, "Forces that cannot thrive in chaotic, complex operating environments will find the future to be an unforgiving place. To succeed organizations will be required to change their modes of thinking about problems, how they see themselves, and their willingness to pursue adaptations."[43]

Summary

It is impossible to predict the future. Although history provides cautionary tales, trends and possible outcomes, there is no crystal ball that can foretell events. The observations of renowned historian Michael Howard are apropos. He asserted, "No matter how clearly one thinks, it is impossible to anticipate precisely the character of future conflict. The key is to not be so far off the mark that it becomes impossible to adjust once that character is revealed."[44] Although the notion held by many that a high-intensity war is unfathomable, this belief must not allow SOF to become blinded to possible future outcomes. As Howard emphasizes, organizations must be able to adjust to realities on the ground. This ability requires forethought and an open-mindedness.

History has shown that through design or miscalculation, the occurrence of a major conflict between peer, near-peer and / or regional powers can never be discounted. A failure to anticipate the possibility of a high-intensity war could lead to punishing consequences. It is fundamentally important to anticipate possible events, which then enables quicker adaptation and change should the inconceivable occur. Having pondered, brain-stormed, and war-gamed potential developments, SOF, at a minimum, can develop a conceptual picture of what the possible roles, tasks and challenges, as well as requirements will be.

After two decades of COIN and CT operations, in which SOF have held advantages in virtually every domain, the potential change in mind-set, behaviour and TTPs to operate in a high-intensity warfare environment is daunting. This challenge can only be met by a proactive approach that puts the necessary effort and horse power behind anticipating future scenarios in the fullest sense and determining SOF contributions in those circumstances. In the end, as unlikely as many believe that the possibility of a conventional war between major international actors may be, SOF must expend some intellectual effort in understanding high-intensity conflict and the implications for SOF, particularly the challenges and potential requirements, as well as determining possible roles and tasks, so that it can best provide employment options to senior political and military decision-makers.


N
W
E
S

CONCLUSION

SOF will always maintain a pivotal role in the GPC. Their characteristics and skill-sets are perfectly geared to irregular warfare and war in the shadows. SOF operations, and those who carry them out, are positioned to conduct clandestine, time-sensitive, high risk (i.e., political and to force) missions in hostile, denied, or politically sensitive environments. Much of the GPC is taking place in obscure domains and in regions around the world where gaining access and influence to populations and regional governments is key. On this playing field, information warfare, the competition over narrative and gaining acceptance goes hand-in-hand with having impact (i.e., economic, military, political, social) on the ground.

For this reason, Lieutenant General Tovo stated, "We're looking for people who are empathetic, adaptive problem-solvers, who don't freak out in the complexity of chaotic situations." He explained, "Our job is to wade into chaos and manage it. Our missions are often undefined – go in and figure it out, you tell us what the mission is."[1]

SOF, through its timeless military assistance / special warfare / irregular warfare programs of SFA, FID and UW allow for a low cost (both in personnel and financial terms) methodology of developing favourable foreign relations with friendly and at-risk states to further political objectives. Their ability to train foreign security forces to deal with real or potential threats also works to pre-empt crises before they become out of control or trigger larger conflagrations. Importantly, SOF have always, are currently, and will continue to, perform these tasks.

SOF operations around the globe also act to create deep relationships and networks, as well as important "lily-pads" should the larger conventional joint force require basing options in times of crisis or war. In short, SOF programs develop access and influence that further favourable foreign relations in support of national objectives. Moreover, SOF's situational awareness around the globe through the cultivation of long-term partnerships and creation of networks provides comprehension of emerging trends and threats worldwide. It also allows for influencing actors and events to coincide with desired outcomes. Admiral McRaven asserted, "SOF are rapidly deployable, have operational reach, are persistent and do not constitute an irreversible

policy commitment." He emphasized that "military success in today's environment is about building a stronger network to defeat the networks that confront us." He underscored that "the [SOF global] network enables small, persistent presence in critical locations, and facilitates engagement where necessary or appropriate."[2] McRaven insisted, "Enduring success is achieved by proper application of indirect operations, with an emphasis in building partner-nation capacity and mitigating the conditions that make populations susceptible to extremist ideologies."[3]

It is SOF's ability to excel at their non-kinetic mission-sets that create security capability within partner nations; develop deep relationships and networks; target hostile agents, agitators, insurgents and terrorists, as well as promulgate a narrative that counters opponent disinformation, that makes SOF an important player in the GPC. Notwithstanding SOF's non-kinetic capabilities, SOF are able to transition to kinetic action (or warfighting ability) seamlessly. Their ability to undertake kinetic actions as part of UW, COIN or CT tasks, as well as direct action missions or special reconnaissance, on order without delay, also make them an indispensable tool. As much as many would like to close the door on CT and COIN, it is just not a viable option if global stability is desired.

In sum, although SOF core tasks and functions have not changed dramatically, the operating locations, circumstances and priorities have evolved and will require continual assessment and adaptation. Globalization and the proliferation of relatively cheap and accessible advanced informational and armament technologies, enhanced by AI, have made the battlespace a more lethal, complex and difficult environment to operate in. The dominance and freedom of manoeuvre that Western forces held over their adversaries in the first two decades of the new millennium can no longer be taken for granted.

These changes require SOF to adapt their TTPs and operating constructs to meet operational requirements as they present themselves. Importantly though, SOF remain an instrumental military capability in the renewed era of GPC / strategic competition. Their ingrained flexibility and adaptability, as well as its strength of operating in the face of adversity and ambiguity position them to be a major actor in the GPC. Moreover, SOF's reliance on highly trained and educated operators add an important element of trust and reliability. SOF can fulfill a variety of critical tasks in the shadowy Gray Zone operations within the context of the GPC. They provide government with key capabilities such as:

- Crisis Response;
- Sensor;
- Signaler;
- Integrator;
- Trainer; and
- Weapon System.

In essence, SOF's characteristics (i.e., high-readiness, rapidly deployable, small footprint / operate in small teams; capable of operating in politically sensitive or denied environments; capable of working independently or in conjunction with other forces or government agencies; operate clandestine, covert or overt; proficient with, and enabled by, advanced technologies) make them the pre-eminent choice for Gray Zone operations.

However, SOF's contribution to strategic competition goes well beyond simply operating in Gray Zone activities. In the worst case of a high-intensity / conventional conflict, SOF can also play a major role. For example, SOF can undertake the following potential tasks:

- Special Reconnaissance;
- AFO;
- Preparation and Shaping of the Operational Environment;
- Theatre Break-in;
- Direct Action;
- Target Designation;
- Battle Damage Assessment;
- Hard Target Defeat;
- Contingency Operations;
- Deception / Diversion / Disruption;
- Sabotage;
- Irregular Warfare (i.e., UW, CT, COIN);[4]
- Second Front / Horizontal Escalation;
- Counter-SOF;
- Counter-Shipping;

- CBRN SSE;
- Role in Phase IV (stabilization);
- PSYOPS; and
- Economy of Effort operations.

Importantly, SOF represent a hard-wired military capability in peace, competition, conflict and war. Their earlier manifestation of filling "gaps and seams" during periods of crisis to buy time for conventional forces to configure themselves to deal with a military emergency is no longer applicable. SOF have proven themselves to be a reliable, consistent, integral military capablility that offer decision-makers a myriad of capabilities and policy options that allow for efficient, effective and timely responses. Within the context of GPC / strategic competition, SOF remains the force of choice.

After all, SOF will remain an essential, if not pivotal, tool in a government's arsenal because it can deliver:

1. High readiness, low profile, task-tailored Special Operations Task Forces (SOTFs) that can be deployed rapidly, over long distances and provide tailored proportional responses to a myriad of different situations;

2. A wide spectrum of special operations options, lethal and non-lethal, to deter, disrupt, dislocate, and when necessary, destroy those that would do harm to the nation, its allies and friends, or its national interests;

3. Highly trained technologically enabled forces that can gain access to hostile, denied, or politically sensitive areas;

4. Discrete forces that can provide discriminate precise SOF kinetic and non-kinetic effects throughout the entire spectrum of competition (i.e., "peace" through high-intensity combat);

5. A deployed capable and internationally recognized force, yet with a generally lower profile and less intrusive presence than larger conventional forces;

6. An economy of effort foreign policy implement that can be used to assist coalition and / or allied operations;

7. A rapidly deployable force that can assess and survey potential crisis areas or hot spots to provide "ground truth" and situational awareness for governmental decision-makers;

8. A highly trained, specialized force capable of providing a response to ambiguous, asymmetric, unconventional situations that fall outside of the capabilities of law enforcement agencies, conventional military or OGDs;

9. A force capable of operating globally in austere, harsh and dangerous environments with limited support. SOF are largely self-contained and can communicate worldwide with organic equipment and can provide limited medical support for themselves and those they support;

10. A culturally attuned SOTF or teams that can act as a force multiplier through the ability to work closely with regional civilian and military authorities and organizations, as well as populations through Defence, Diplomacy and Military Assistance / Security Force Assistance initiatives;

11. A force capable of preparing and shaping environments or battlespaces (i.e., setting conditions to mitigate risk and facilitate successful introduction of follow-on forces);

12. An enabler to foster inter-agency and inter-departmental cooperation through its ability to serve as a catalyst to unify, extend the reach and maximize the effects of other instruments of national power; and

13. A highly trained and educated, adaptive, agile-thinking force capable of dealing with the threat that has not yet been identified.

Renowned strategist, the late Colin Gray, declared, "Special operations forces are a national grand-strategic asset: they are a tool of statecraft that can be employed quite surgically in support of diplomacy, of foreign assistance (of several kinds), as a vital adjunct to regular military forces, or as an independent weapon."[5] He captured the essence of SOF. Simply put, SOF are / have indispensable relevance to decision-makers, providing them with a wide scope of cost-efficient, low-risk and effective options is precisely the driving

force behind SOF power. Their ability to produce on short notice, courses of action and desirable outcomes, in a number of domains, regardless of location, with a high probability of success, give them great saliency to political and military decision-makers. After all, arguably, the acid test of strategic utility is what an organization contributes to national power and the ability to project or defend national interests.

ABOUT THE AUTHOR

Colonel (Retired) Bernd Horn, OMM, MSM, CD, PhD

Colonel (Retired) Bernd Horn, OMM, MSM, CD, PhD is a former infantry officer who has held key command and staff appointments in the Canadian Armed Forces, including Deputy Commander of Canadian Special Operations Forces Command (CANSOFCOM), Commanding Officer of the 1st Battalion, The Royal Canadian Regiment and Officer Commanding 3 Commando, the Canadian Airborne Regiment. He is currently the CANSOFCOM Command Historian, an appointment he fills as a civilian. Dr. Horn is also an adjunct professor of history at the Royal Military College of Canada and a non-resident senior fellow at the Joint Special Operations University in Tampa. He has authored, co-authored, edited or co-edited 50 books and numerous monographs / chapters / articles on military history, Special Operations Forces, leadership and military affairs.

GLOSSARY OF ABBREVIATIONS

5G	Fifth Generation
9/11	11 September 2001 terrorist attack
A2/AD	Anti-Access / Area Denial
ADIZ	Air Defence Identification Zone
AFRICOM	Africa Command
AI	Artificial Intelligence
AQI	Al-Qaeda in Iraq
ARSOF	Army Special Operations Forces
ASAT	Antisatellite
AU	African Union
BCI	Brain Computer Interface
BDA	Bomb Damage Assessment
BRI	Bridge and Road Initiative
C2	Command & Control
C4	Command, Control, Communications, Computers
CANSOFCOM	Canadian Special Operations Command
CBRN	Chemical, Biological, Radiological, Nuclear
CCP	Chinese Communist Party
CCTV	Close Circuit Television
CEI	Critical Energy Infrastructure
CENTCOM	Central Command
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CAN	Center for Naval Analyses
COIN	Counter Insurgency
C-RAM	Counter Rocket, Artillery and Mortar
CRI	China Radio International
CSA	Canadian Space Agency
CSE	Communications Security Establishment

CSIS	Canadian Security Intelligence Service or *Center for Strategic and International Studies* (depending on context)
CT	Counter-Terrorism
C-UAV	Counter Unmanned Aerial Vehicles
CVEO	Counter Violent Extremist Organizations
DA	Direct Action
DE	Direct Energy
DIA	Defense Intelligence Agency
DNI	Director National Intelligence
DoD	Department of Defense
EDPAC	EDP audit, control and security
ERC	Education & Research Centre
EU	European Union
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FID	Foreign Internal Defense
FSB	*Federal'naya sluzhba bezopasnosti Rossiyskoy Federatsii* (Federal Security Service)
GPC	Great Power Competition
GPS	Global Positioning System
GRU	*Glavnoye Razvedyvatelnoye Upravlenie* (Military Intelligence Directorate)
GSPIA	Graduate School of Public and International Affairs
HBV	Hypersonic Glide Vehicle
HEL	High Energy Laser
HEO	Hyper Enabled Operator
HVT	High Value Target
ICBM	Intercontinental Ballistic Missile
IDF	Israeli Defense Force
IRGC	Islamic Revolutionary Guard Corps
ISIS	Islamic State in Syria (see also Daesh, Islamic State)
ISR	Intelligence, Surveillance, Reconnaissance

JCS	Joint Chiefs of Staff
JSOC	Joint Special Operations Command
JSOU	Joint Special Operations University
JTAC	Joint Terminal Attack Controller
Kg	Kilogram
Km	Kilometre
KSO	Komanda spetsialnogo naznacheniya (Russian Special Operations Command)
LAWS	Lethal Autonomous Weapon System
MARSOC	Marine Forces Special Operations Command
MCF	Military-Civil Fusion
MCT	Maritime Counter Terrorism
MINUSMA	Multidimensional Integrated Stabilization Mission in Mali
MND	Minister of National Defence
MNJTF	Multinational Joint Task Force
MoD	Ministry of Defence
MOIS	Ministry of Intelligence and Security
NATO	North Atlantic Treaty Organization
NCTV	National Coordinator for Security and Counterterrorism
NDS	National Defense Strategy
NGO	Non-Governmental Organization
NSS	National Security Strategy
OCAO	Overseas Chinese Affairs Office
OGD	Other Government Department
OODA	Observe-Orient-Decide-Act
OP	Observation Post
OPSEC	Operational Security
PAP	People's Armed Police
PLA	People's Liberation Army
PLAAF	People's Liberation Army Air Force

PLAN	People's Liberation Army Navy
PRC	People's Republic of China
PSC	Private Security Companies
PSYOPS	Psychological Operations
RCMP	Royal Canadian Mounted Police
REE	Rare Earth Elements
S&T	Science and Technology
SACEUR	Supreme Allied Commander Europe
SAR	Synthetic Aperture Radar
SAS	Special Air Service
SBS	Special Boat Service
SecDef	Secretary of Defense
SEAL	Sea, Air, Land
SF	Special Forces
SFA	Security Force Assistance
SFG	Special Forces Group
SHORAD	Short-Range Air Defence
SOCNORTH	Special Operations Command North
SOF	Special Operations Forces
SOP	Standard Operating Procedures
SOTF	Special Operations Task Force
Sqn	Squadron
SR	Special Reconnaissance
SSE	Sensitive Site Exploitation
SSO	*Sily spetsial'nykh operatsiy*
SVR	*Sluzhba vneshney razvedki Rossiyskoy Federatsii* (Foreign Intelligence Service)
SW	Special Warfare
TEL	Transporter-Erector-Launcher
TTP	Tactics, Techniques and Procedures
U.S.	United States
UAE	United Arab Emirates
UAV	Unmanned Aerial Vehicle
UK	United Kingdom

UN	United Nations
USD	United States Dollars
USNS	United States Navy Ship
USSOCOM	United States Special Operations Command
UW	Unconventional Warfare
VDV	Russian Airborne Forces
VEO	Violent Extremist Organizations
WHO	World Health Organization
WMD	Weapons of Mass Destruction
WWII	World War II

ENDNOTES

INTRODUCTION

1 United States Special Operations Command defines this level of competition as "the interaction among actors in pursuit of the influence, leverage, and advantage necessary to secure their respective interests." USSOCOM, *On Competition: Adapting to the Contemporary Strategic Environment*. *JSOU Report 21-5* (Tampa: JSOU Press, 2021), xi.

2 Pulitzer Prize-winning columnist Charles Krauthammer declared, "The most striking feature of the post–Cold War world is its unipolarity. No doubt, multipolarity will come in time." Brandon J. Archuleta and Jonathan I. Gerson, "Fight Tonight Reenergizing the Pentagon for Great Power Competition," *Joint Forces Quarterly (JFQ)100*, 2021, 83.

3 DoD, *Irregular Warfare Annex to the National Defense Strategy* (Washington D.C.: DoD, 2020), 5.

Definitions are as follows:

CT is defined as "Activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals."

COIN is defined as "Comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes."

DoD, *Department of Defense Dictionary of Military and Associated Terms Joint Publication 1-02* (Washington D.C.; DoD, 2010 as amended through 31 January 2011), 53, 54, 145, 383.

4 Cited in Melia Pfannenstiel and Louis L. Cook, "Disinformation and Disease," *JFQ 98*, 2020, 25.

5 David Kilcullen, *The Dragons and the Snakes. How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020), 175.

CHAPTER 1

1 Ronald O'Rourke, *Renewed Great Power Competition: Implications for Defense – Issues for Congress* (Washington D.C.: Congressional Research Service, 4 March 2021), 1.

2 The terms "peer and near-peer" competitors often create push back with detractors citing the fact that none of those entities listed are actually peers or near-peers and none could militarily defeat the U.S.. However, all of those states, as well as a number of non-state actors have the capability, and have in reality, undertaken actions that have frustrated, delayed and in some cases prevented the U.S. and its allies being able to realize their political objectives.

3 DoD, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington D.C.: DoD, 2018), 1. (henceforth *2018 NDS*).

4 DoD, *A Vision for 2021 And Beyond* (Fort Bragg, NC: 1st Special Forces Command (Airborne) ND), 3.

5 Jeff Seldin, "US Noncommittal on Keeping Troops in Africa," *VOA*, 27 January 2020, https://www.voanews.com/africa/us-noncommittal-keeping-troops-africa, accessed 6 February 2020. Not surprisingly then, the strategy document advocates enhancing the lethality of American military forces through such means as greater deployment of autonomous robotic weapons, the modernization of missile defense and nuclear weapons, as well as the deployment of U.S. forces to fight from smaller, dispersed bases.

6 President Joseph R. Biden, Jr., *Interim National Security Strategic Guidance* (Washington D.C.: White House, March 2021), 6-8. DoD had identified the PRC's ambitions of becoming a "great power" (i.e., strong, modernized, unified, and wealthy nation) already two decades ago in a detailed report to the U.S. Congress. Many analysts believe that China will achieve its ambition to field a "world-class" military by 2049.

7 Teresa Chen, Alana Nance, Han-ah Sumner, "Water Wars: AUKUS Goes Hypersonic," *Lawfare*, 22 April 2022, https://www.lawfareblog.com/water-wars-aukus-goes-hypersonic, accessed 4 May 2022.

8 Brad Lendon and Ellie Kaufman, "US military gets 'laser focused' on keeping up with China," *CNN*, 11 June 2021, https://www.msn.com/en-ca/news/world/us-military-gets-laser-focused-on-keeping-up-with-china/ar-AAKWa68, accessed 13 June 2021.

9 NATO Reflection Group, *NATO 2030: United for a New Era* (Brussels: NATO, 25 November 2020), 16.

10 In accordance with American doctrine, "Traditional warfare is characterized as a violent struggle for domination between nation-states or coalitions and alliances of nation-states… traditional warfare typically involves force-on-force military operations." Conversely, Irregular Warfare (IW) "is characterized as a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force." DoD, *Joint Publication 1. Doctrine for the Armed Forces of the United States* (Washington D.C.: DoD, 25 March 2013 incorporating Change 1, 12 July 2017), x. file:///J:/Doctrine%20for%20the%20Armed%20Forces%20of%20the%20USA.pdf, accessed 21 March 2020.

11 Robert Farley, "Welcome to the All-Consuming Great Power Competition," *The Diplomat*, 23 February 2021, https://thediplomat.com/2021/02/welcome-to-the-all-consuming-great-power-competition/, accessed 24 February 2021.

12 For example, it was reported that American policymakers increasingly see the U.S.-Chinese rivalry not as a traditional great-power competition but as a struggle pitting democracy against communism. In July 2020, then Secretary of State Mike Pompeo delivered a speech that cast the U.S.-Chinese antagonism in ideological terms. Christopher Layne, "Coming Storms. The Return of Great-Power War," *Foreign Policy*, November/December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/coming-storms, accessed 3 November 2020.

13 Jim Garamone, "Dempsey: U.S. Forces Must Adapt to Deal with Near-Peer Competitors," *DoD News,* https://www.jcs.mil/Media/News/News-Display/Article/613868/dempsey-us-forces-must-adapt-to-deal-with-near-peer-competitors/, accessed 2 February 2020.

14 Kaley Scholl, "The Use of US Special Operation Forces in Great Power Competition: Imposing Costs on Chinese Gray Zone Operations," *Small Wars Journal*, 7 December 2020, https://smallwarsjournal.com/jrnl/art/use-us-special-operation-forces-great-power-competition-imposing-costs-chinese-gray-zone, accessed 8 December 2020.

15 Cited in Meghann Myers and Shawn Snow, "After decades focused on terrorism, special operations is broadening its horizons," *Military Times*, 12 February 2020, https://www.militarytimes.com/news/your-military/2020/02/12/after-decades-focused-on-terrorism-special-operations-is-broadening-its-horizons/, accessed 13 February 2020.

16 David Oakley, "The Problems of a Militarized Foreign Policy for America's Premier Intelligence Agency," *War on the Rocks*, 2 May 2019, https://warontherocks.com/2019/05/the-problems-of-a-militarized-foreign-policy-for-americas-premier-intelligence-agency/, 2 May 2019.

17 Cited in Ibid.

18 Brandon et al, "Fight Tonight Reenergizing," 84.

19 USSOCOM, *On Competition*, xi.

20 U.S. Army Training and Doctrine Command (TRADOC), *The U.S. Army in Multi-Domain Operations 2028*, Pamphlet 525-3-1, (Fort Eustis, VA: TRADOC, 2018), vi, 6–7.

21 The term strategic competition vice GPC is viewed by many to be more accurate as it allows for the inclusion of regional powers, rogue states and non-state entities.

22 Cited in Joe Miller and Monte Erfourth, "SOF in Competition: Establishing the Foundation of Strategy," *Small Wars Journal*, https://smallwarsjournal.com/jrnl/art/sof-competition-establishing-foundation-strategy-v13, accessed 8 March 2020.

23 Strategists Joe Miller and Colonel Monte Erfourth argued, "The U.S. has developed a threat-centric culture, focused on the development of capabilities, defined within individual warfighting cultures. When paired with the different institutional cultures and interests of the military services, threat-centrism risks the development of capability-driven strategy rather than strategy-driven capabilities." Miller and Erfourth, "SOF in Competition."

24 See Christian Brose, "The New Revolution in Military Affairs," https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs, accessed 25 April 2019. Notably, even Iran's Islamic Revolutionary Guard Corps (IRGC) has long-range ballistic missiles that travel 1,800 km and hit their designated targets. Maziar Motamedi, "Iran's Revolutionary Guard tests long-range missiles, drones," *Al Jazeera*, 16 January 2021, https://www.aljazeera.com/news/2021/1/16/irans-revolutionary-guards-test-long-range-missiles-drones, accessed 18 January 2021.

25 Chris Dougherty, *More than Half the Battle. Information and Command in a New American Way of War* (Washington D.C.: Centre for a New American Security, 2021), 4.

26 Richard Uber, "Penetrating Artificial Intelligence enhanced Anti Access / Area Denial," *Journal of Indo-Pacific Affairs*, Winter 2020, 57.

27 Millimeter wave technology, also known as "millimeter band, is the band of spectrum with wavelengths between 10 millimeters (30 GHz) and 1 millimeter (300 GHz). It is also known as the extremely high frequency (EHF) band by the International Telecommunication Union (ITU)," https://www.techtarget.com/searchnetworking/definition/millimeter-wave-MM-wave, accessed 15 October 2021.

28 Uber, "Penetrating Artificial Intelligence," 57.

29 Sandor Fabian, "Building and Enabling Urban Resistance Networks in Small Countries - A Crucial Role for U.S. Special Forces in Great Power Competition," *Small Wars Journal*, 11 April 2021, https://smallwarsjournal.com/jrnl/art/building-and-enabling-urban-resistance-networks-small-countries-crucial-role-us-special, accessed 21 April 2021.

30 The Turkish use of drone swarms to engage Syrian bases and chemical weapon depots in March 2020, as well as the South Korean demonstration of 1,218 autonomous drones equipped with lights collaborating to form intricate images in the night sky over Pyeongchang during the opening ceremonies of the 2018 Olympics provide a preview of what drone swarms are capable of achieving. See Seclan Hacaoglu, "Turkey's Killer Drone Swarm Poses Syria Air Challenge to Putin," *Bloomberg*, 1 March 2020. https://www.bloomberg.com/news/articles/2020-03-01/turkey-s-killer-drone-swarm-poses-syria-air-challenge-to-putin, accessed 2 March 2020; and Brose, "The New Revolution."

31 The Stockholm International Peace Research Institute published a report on 13 June 2022 that stated that the world's nuclear-armed states (i.e., U.S., Russia, the U.K., France, China, India, Pakistan, Israel and North Korea) will likely increase their nuclear weapons over the next decade. Monique Beals, "Nuclear arsenals expected to grow for first time since Cold War: think tank," *The Hill*, 13 June 2022, https://msn.com/en-ca/news/politics/nuclear-arsenals-expected-to-grow-for-first-time-since-cold-war-think-tank/ar-AAYp9Ak?ocid=sapphireappshare, accessed 14 June 2022.

32 András Rácz, Russia's *Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*. The Finnish Institute of International Affairs, FIIA Report 43, 41. The Americans use a term called "Gray Zone Conflict" to describe Hybrid Warfare. Gray Zone Conflict is defined "as competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks." USSOCOM White Paper, *The Gray Zone*, 9 September 2015, 1.

33 Kerry K. Gershaneck, *Political Warfare. Strategies for Combating China's Plan to "Win without Fighting,"* (Quantico, VA: Marine Corps University Press, 2020), 26. The concept of Hybrid Warfare, also known as "Gray Zone operations" in American doctrine, is not new. The concept of "political warfare," which is the term George Keenan coined in 1948, stating that political warfare encompassed "all the means at a

nation's command, short of war, to achieve its national objectives." In the 1990s, the term military operations other than war (MOOTW) became in vogue. The concept was based on "deterring war, resolving conflict, promoting peace, and supporting civil authorities." Specific operations included arms control, counterterrorism, humanitarian assistance, peace operations, and show-of-force operations. This concept combined the concept of the application of military power combined with other levers of national power to achieve political objectives. "Keenan Long Telegraph," https://digitalarchive.wilsoncenter.org/document/116178.pdf, accessed 6 July 2021; and David A. Broyles and Brody Blankenship, *The Role of Special Operations Forces in Global Competition* (Arlington, VA: CNA Analysis & Solutions, 2017), 10.

34 Ministry of Defence (UK), *Strategic Trends Programme: Future Character of Conflict*, 13.

35 Frans-Paul van der Putten, Minke Meijnders, Sico van der Meer and Tony van der Togt, eds., *Hybrid Conflict: The Roles of Russia, North Korea and China* (Wassenaar, NL: Clingendael Institute, 2018), 1.

36 Cited in Stefan Hadjitodorov and Martin Sokolov, "Blending New-Generation Warfare and Soft Power: Hybrid Dimensions of Russia-Bulgaria Relations," *Connections: The Quarterly Journal*, Vol 17, No. 1, 2018, 11.

37 David Knoll, Kevin Pollpeter and Sam Plapinger, "China's Irregular Approach To War: The Myth Of A Purely Conventional Future Fight," *The Modern War Institute*, 27 April 2021.

38 Broyles and Blankenship, *The Role of Special Operations Forces,* 13-14.

39 Ibid.

40 Ibid. Further insight on how Russia views contemporary conflict was provided by Colonel S.G. Chekinov and Lieutenant-General S.A. Bogdanov in a 2013 article entitled "The Nature and Content of a New-Generation War." Similar to General Gerasimov, they extracted lessons from how the West, particularly the Americans, have conducted their military campaigns. As a result, they identified eight particular steps of new-generation warfare:

1. Non-military measures that blend moral, information, psychological, ideological, and economic measures that aim at establishing a more favorable political, economic, and military environment;
2. Media, diplomatic channels, and top government and military agencies carry out coordinated special operations so as to mislead political and military leaders. This can include leaking false data, orders, directives, and instructions;
3. Bribing, deceiving, and/or intimidating government and military officers, to force them to abandon their duties;
4. Fueling discontent among the population. This can be further enhanced by the arrival of Russian "volunteers";
5. Establish no-fly zones and blockades over the targeted country. Cooperation between private military contractors and armed opposition;

6. Initiate large-scale reconnaissance and subversion operations that are initiated immediately followed up upon with military action;
7. Launch a combination of information, electronic warfare, and air force operations that are complimented with high-precision weapons; and
8. Eliminate the last points of resistance through reconnaissance operations, special operations, and artillery and missile bombardment.

Cited in Hadjitodorov and Sokolov, "Blending New-Generation Warfare," 12-13.

41 Cited in Tom Wilhelm, "A Russian Military Framework for Understanding Influence in Competition Period," *Military Review*, July-August 2020, 36.

42 Ibid.

43 For a detailed study of Hybrid Warfare see Colonel Bernd Horn, *On Hybrid Warfare* (Kingston, ON: CANSOFCOM PDC Press, 2016).

44 Maria Snegovaya, "Putin's Information Warfare in Ukraine Soviet Origins of Russia's Hybrid Warfare," *Institute for the Study of War*, September 2015, 7, 10.

45 Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *JFQ 79*, 2015, 47.

46 Travis Clemens, *Special Operations Forces Civil Affairs in Great Power Competition JSOU Report 20-4* (Tampa, FA: JSOU, 2020), 22. The Congressional Research Service has noted that key features of the current situation of renewed great power competition include but are not necessarily limited to the following:

- the use by Russia and China of new forms of aggressive or assertive military, paramilitary, information, and cyber operations—sometimes called Hybrid Warfare, gray-zone operations, ambiguous warfare, among other terms, in the case of Russia's actions, and salami-slicing tactics or gray-zone warfare, among other terms, in the case of China's actions;
- renewed ideological competition, this time against 21st-century forms of authoritarianism and illiberal democracy in Russia, China, and other countries;
- the promotion by China and Russia through their state-controlled media of nationalistic historical narratives, some emphasizing assertions of prior humiliation or victimization by Western powers, and the use of those narratives to support revanchist or irredentist foreign policy aims;
- challenges by Russia and China to key elements of the U.S.-led international order, including the principle that force or threat of force should not be used as a routine or first-resort measure for settling disputes between countries, and the principle of freedom of the seas (i.e., that the world's oceans are to be treated as an international commons); and
- additional features alongside those listed above, including:
    - continued regional security challenges from countries such as Iran and North Korea;
    - a continued focus (at least from a U.S. perspective) on countering transnational terrorist organizations that have emerged as significant non-state

actors (now including the Islamic State organization, among other groups); and

- weak or failed states, and resulting weakly governed or ungoverned areas that can contribute to the emergence of (or serve as base areas or sanctuaries for) non-state actors, and become potential locations of intervention by stronger states, including major powers.

O'Rourke, *Renewed Great Power Competition*, 22.

47 Abraham Mahshie, "General wields influence delicately in Chinese play for military foothold in Africa," *Washington Examiner*, 26 April 2021, https://www.washingtonexaminer.com/policy/defense-national-security/townsend-china-military-africa, accessed 27 April 2021.

CHAPTER 2

1 Biden, *Interim National Security Strategic Guidance*, 8.

2 Emily Harding, "The Intelligence Community's Annual Threat Assessment and he Senate Intelligence Committee's Worldwide Threats Hearing," *Center for Strategic and International Studies* (CSIS), 19 April 2021, https://www.csis.org/analysis/intelligence-communitys-annual-threat-assessment-and-senate-intelligence-committees, accessed 20 April 2021.

3 Ibid.

4 Seth Jones, "The Future of Competition: U.S. Adversaries and the Growth of Irregular Warfare," *CSIS*, 4 February 2021, https://www.csis.org/analysis/future-competition-us-adversaries-and-growth-irregular-warfare, accessed 5 February 2021.

5 Ibid.

6 Cleo Paskal, "The world doesn't realize it's already at war with China," *Foundation for Defense for Democracies*, 23 January 2021, https:// www.fdd.org/analysis/2021/01/23/world-doesnt-realize-already-at-war-china/, accessed 27 January 2021.

7 Michael Beckley, "Enemies of My Enemy." How Fear of China Is Forging a New World Order," *Foreign Affairs*, March/April 2022, https://www.foreignaffairs.com/articles/2021-02-14/china-new-world-order-enemies-myenemy?utm_medium=promo_email&utm_source=pre_release&utm_campaign=special_preview_021422_prospects&utm_content=20220214&utm_term=promo-email-prospects, accessed 14 February 2022.

8 Director National Intelligence (DNI), *Annual Threat Assessment of the U.S. Intelligence Community* (Washington D.C.: DNI, 2022), 6.

9 For example, China spent decades waging political warfare in Thailand. The CCP used intimidation, kidnapping, bribery, working through surrogates, backing insurgents, blackmail, extortion, co-opting/manipulating/buying local media, infiltrating education systems, high level visits, cyber infiltration, and social media manipulation. Paskal, "The world doesn't realize."

10 Ibid.

11 Ibid.

12 Bonny Lin, Cristina L. Garafola, Bruce McClintock, Jonah Blank, Jeffrey W. Hornung, Karen Schwindt, Jennifer D. P. Moroney, Paul Orner, Dennis Borrman and Sarah W. Denton, *A New Framework for Understanding and Countering China's Gray Zone Tactics* (Santa Monica, CA: RAND, 2022), 2. The RAND report defined Chinese Gray Zone tactics as "coercive Chinese government geopolitical, economic, military, and cyber and information operations (cyber/IO) activities beyond regular diplomatic and economic activities and below the use of kinetic military force. We further differentiate by mechanism, or how China uses its power to pressure the target, dividing

- geopolitical, economic, and cyber/IO tactics into international (indirect external pressure, such as by leveraging regional fora), bilateral (direct external pressure), and grassroots (direct activities on the ground in the target country or region, such as by leveraging local proxies).
- military tactics into military domains, specifically air, maritime, land, and general (multiple PRC military services or general threats)."

13 James P. Farwell, *Adversarial Tactics to Undercut US Interests in New Generation Warfare 2019*, Strategic Multilayer Assessment Future of Global Competition & Conflict, 3 May 2019, 14-15, https://nsiteam.com/social/wp-content/uploads/2019/05/Farwell_Adversarial-Tactics.pdf, accessed 20 April 2021.

14 Scholl, "The Use of US Special Operation Forces."

15 See Peter Mattis and Matthew Brazil, *Chinese Communist Espionage. An Intelligence Primer* (Annapolis: Naval Institute Press, 2019).

16 Harding, "The Intelligence Community."

17 Jones, "The Future of Competition." Critics argue that unlike during the Cold War, the U.S. government and its allies, as well as the private sector have failed to invest in the language skills and expertise to effectively compete with the Chinese Communist Party. As a result, they fail to properly understand how China, Russia, and Iran view competition with the U.S. and the West at large.

18 See Fiona Quimbre, Peter Carlyon, Livia Dewaele and Alexi Drew, *Exploring the opportunities and challenges of research engagement with China* (Santa Monica, CA: RAND, 2022).

19 Ibid.

20 Karen Guttieri, "Accelerate Change or Lose the Information War," *AEther. A Journal of Strategic Airpower & Spacepower*, Vol 1, No. 1, Spring 2022, 97.

21 Putten et al, *Hybrid Conflict*, 36.

22 Michael J. Mazarr, Bryan Frederick, John J. Drennan, Emily Ellinger, Kelly Eusebi, Bryan Rooney, Andrew Stravers and Emily Yoder, *Understanding Influence in the Strategic Competition with China* (Santa Monica, CA: RAND, 2021), x.

23 For example, MI5 identified a Chinese lawyer, Christine Ching Kui Lee, who used her cover of representing the British Chinese community to obscure her activities on the behalf of the Chinese government. MI5 stated she "knowingly engaged in political interference activities" on behalf of Beijing in the U.K. Parliament. Specifically, Lee was found to be involved in the "facilitation of financial donations to political parties," lawmakers and potential candidates for public office in Britain and to "political entities" on behalf of foreign nationals. In fact, she had "extensive engagement with individuals across the U.K. political spectrum," and she had been involved in informal cross-party groups run by lawmakers known as All-Party Parliamentary Groups. Isabella Kwai, "Britain's Security Agency MI5 Warns Lawmakers of China's Political Interference," *The New York Times*, 13 January 2022, https://www.nytimes.com/2022/01/13/world/europe/britain-mi5-china-agent-parliament.html, accessed 13 January 2022.

24 Putten et al, *Hybrid Conflict*, 35.

25 Ibid., 34.

26 For example, this was done in response to the named EU member states hosting the Dalai Lama.

27 Putten, et al, *Hybrid Conflict,* 35.

28 Ibid., 35.

29 Seth G. Jones, *Three Dangerous Men. Russia, China, Iran and the Rise of Irregular Warfare* (New York: W.W. Norton & Company, 2021), 195.

30 Putten, et al, *Hybrid Conflict,* 3, 33-34.

31 Ibid., 3, 33-34.

32 Kirsty Needham, "Chinese censorship found at Australian universities - rights group," *Reuters*, 30 June 2021, https://www.msn.com/en-ca/news/world/chinese-censorship-found-at-australian-universities-rights-group/ar-AALAvNH, accessed 2 July 2021.

33 Jones, *Three Dangerous Men,* 149.

34 Farwell, *Adversarial Tactics*, 14-15.

35 Ibid., 14-15.

36 Ibid., 14-15.

37 "How technology helped turn the great power competition 'grey'," *The Rule of Law Post*, 5 December 2019, https://www.law.upenn.edu/live/news/9621-how-technology-helped-turn-the-great-power, accessed 29 October 2020.

38 Department of Justice, "Five Individuals Charged Variously with Stalking, Harassing and Spying on U.S. Residents on Behalf of the PRC Secret Police," *Office of Public Affairs*, 16 March 2022, https://www.justice.gov/opa/pr/five-individuals-charged-variously-stalking-harassing-and-spying-us-residents-behalf-prc-0, accessed 17 March 2022.

39 Katelyn Polantz, Kara Scannell and Hannah Rabinowitz, "Justice Department charges 5 people with helping Chinese government to spy on dissidents in US," *CNN*, 16 March 2022, https://Katelyn Polantz, Kara Scannell and Hannah Rabinowitz, accessed 16 March 2022.

40 Farwell, *Adversarial Tactics, 14-15*.

41 US-China Economic and Security Review Commission, "PRC Representation in International Organizations," May 2021, https://www.uscc.gov/sites/default/files/2021-05/PRC_Representation_in_International_Organizations_May2021.pdf, accessed 15 October 2021.

42 Kathy Gilsinan, "China's Bargain on Global Influence Is Paying Off," *The Atlantic*, 6 May 2020, https://www.theatlantic.com/politics/archive/2020/05/china-global-influence-who-united-states/611227/, accessed 7 May 2020; and Dinko Hanaan Dinko, "China's 'mask diplomacy' wins influence across Africa, during and after the pandemic," *The Conversation*, 10 March 2021, https://theconversation.com/chinas-mask-diplomacy-wins-influence-across-africa-during-and-after-the-pandemic-153048, accessed 11 March 2021.

43 Stephen Olson and Clyde Prestowitz, *The Evolving Role of China in International Institutions* (Washington D.C.: The Economic Strategy Institute, 2011), 4.

44 Brad Lendon and Ellie Kaufman, "US military gets 'laser focused' on keeping up with China," *CNN*, 11 June 2021, https://www.msn.com/en-ca/news/world/us-military-gets-laser-focused-on-keeping-up-with-china/ar-AAKWa68, accessed 13 June 2021.

45 Dinko, "China's 'mask diplomacy'."

46 Abhisnek Mishra, "China's Growing Security Activism in Africa," *Observer Research Foundation*, 7 October 2020. Abhishek Mishra, https://www.Orfonline.Org/Expert-Speak/Chinas-Growing-Security-Activism-In-Africa/, accessed 10 October 2020.

47 Lucy Craymer, "Analysis-Alarmed by Solomon Islands-China pact, NZ finds its voice on security," *Reuters*, 16 May 2022, https://www.msn.com/en-ca/news/world/analysisalarmed-by-solomon-islandschina-pact-nz-finds-its-voice-on-security/ar-AAXlCoE?ocid=sapphireappshare, 18 May 2022; and Chen et al "Water Wars."

48 Nick Perry, "China wants 10 Pacific nations to endorse sweeping agreement," *Canadian Press*, 25 May 2022, https://wwwmsn.com/en-ca/news/world/china-wants-pacific-nations-to-endorse-sweeping-agreement/ar-AAXJGTS?ocid=sapphireappshare, accessed 27 May 2022. The draft agreement stipulates that the Pacific countries "firmly abide" by the one-China principle and that they "non-interference" principle with regard to its human rights record.

49 Cited in Scholl, "The Use of US Special Operation Forces."

50 Ibid.

51 For example, Michael McCaul, the ranking Republican on the House Foreign Affairs Committee, observed, "Countries like Honduras are under pressure to switch diplomatic recognition from Taiwan to China in order to receive much-needed vaccines

from the CCP (Chinese Communist Party)." Dan De Luce and Laura Strickler, "China is using Covid-19 vaccine to flex its muscles in America's backyard, experts say," *NBC News*, 23 May 2021, https://www.msn.com/en-ca/news/world/china-is-using-covid-19-vaccine-to-flex-its-muscles-in-americas-backyard-experts-say/ar-AAKhWoD, accessed 23 May 2021.

52 Anchal Vohra, "Russia, China expanding Middle East sway with COVID-19 vaccines Moscow and Beijing using coronavirus shots in a soft-power move to extend influence in Middle East countries," *AlJazeera*, 9 February 2021, https://www.aljazeera.com/news/2021/2/9/russia-china-seek-to-expand-mena-influence-through-vaccines, accessed 10 February 2021.

53 "Two US Navy aircraft carriers conduct South China Sea drills," *CNN*, 9 February 2021, https://www.msn.com/en-ca/news/world/two-us-navy-aircraft-carriers-conduct-south-china-sea-drills/ar-BB1dww5F, accessed 10 February 2021.

54 Cited in Jones, *Three Dangerous Men*, 17.

55 Mazarr et al, *Understanding Influence,* x.

56 Farwell, *Adversarial Tactics*, 14-15. China is responsible for 82 per cent of the counterfeit goods seized in the EU, 80 per cent in Canada and 76 per cent in the U.S.. Annual losses to the U.S. from China's IP theft are estimated at $360 billion. Nicolas Eftimiades, *Chinese Espionage. Operations and Tactics* (State College, PA: Vitruvian Press, 2020), 36.

57 Farwell, *Adversarial Tactics,* 15.

58 Michael Beckley, "'Enemies of My Enemy.' How Fear of China Is Forging a New World Order," *Foreign Affairs*, March/April 2022, https://www.foreignaffairs.com/articles/2021-02-14/china-new-world-order-enemies-myenemy?utm_medium=promo_email&utm_source=pre_release&utm_campaign=special_preview_021422_prospects&utm_content=20220214&utm_term=promo-email-prospects, accessed 14 February 2022.

59 Chris Arsenault and Philippe Le Billon, "Internal DND study calls green technology minerals 21st-century 'oil weapon'," *CBC News*, 20 June 2022, https://Internal DND study calls green technology minerals 21st-century 'oil weapon', accessed 21 June 2022. China controls about 90 per cent of the world's supply of REE, which places it in a dominant position to control the market.

60 Shannon McGurk, "The Future of China's Belt & Road Initiative," in Air Force Warfighting Integration Capability (AFWUC), *Global Futures Report*, June 2020, 30; and Jones, *Three Dangerous Men*, 166.

61 The U.S. government has been a vocal critic of the BRI. Former Secretary of State Rex Tillerson labelled China a predatory lender. Former National Security Advisor Ambassador John Bolton claimed, "uses bribes, opaque agreements, and the strategic use of debt to hold states in Africa captive to Beijing's wishes and demands. He described, the BRI as "a plan to develop a series of trade routes leading to and from China with the ultimate goal of advancing Chinese global dominance." Deborah Brautigam, "A Critical look at Chinese 'debt-trap diplomacy': the rise of a meme," *Area Development and Policy*, Vol. 5, No.1, 2020, 4.

62 Clemens, *Special Operations Forces Civil*, 60.

63 David L. Fogel, "I helped defend against China's economic hybrid war. Here's how the US can respond," The *Atlantic Council*, 25 April 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/i-helped-defend-against-chinas-economic-hybrid-war-heres-how-the-us-can-respond/, accessed 18 May 2022. Uganda's Entebbe International Airport appears to be next on the acquisition list.

64 To optimize its gains through the BRI initiative, the PRC has also created a new generation of Chinese private security companies to protect its citizens and businesses in Africa. These private security companies provide China with a useful tool to protect its interests without forcing it to intervene militarily. César Pintado, "Chinese Mercenaries in Africa," *Small Wars Journal*, 5 June 2021, https://smallwarsjournal.com/jrnl/art/chinese-mercenaries-africa, accessed 10 June 2021.

65 JoAnne Wagner, "'Going Out.' Is China's skillful use of Soft Power in Sub-Sahara Africa a Threat to US Interests?" *JFQ 64*, 2012, 102.

66 Ibid., 103.

67 Don Murray, "Why France is losing its 'Great Game' in western Africa," *CBC News*, 2 July 2021, https://www.cbc.ca/news/world/france-western-africa-don-murray-1.6087514, accessed 2 July 2021.

68 Mahshie, "General wields influence."

69 Dinko, "China's 'mask diplomacy'"; and Mohammed Alamin, "Made-by-China Port to Open Sudan's Economy to More Exports," *Bloomberg*, 10 November 2020, https://www.bloomberg.com/news/newsletters/2020-11-10/supply-chains-latest-china-made-port-opens-sudan-to-more-exports, accessed 12 November 2020.

70 Wagner, "'Going Out.' Is China's," 99.

71 Maria Ryan, *Full Spectrum Dominance. Irregular Warfare and the War on Terror* (Stanford, CA: Stanford University Press, 2019), 199.

72 "US Commander: We can no longer afford to underestimate the economic opportunity, strategic consequence Africa embodies, which competitors like China & Russia recognize," *Newz Post*, 22 April 2021, https://newz.ug/us-commander-we-can-no-longer-afford-to-underestimate-the-economic-opportunity-strategic-consequence-africa-embodies-which-competitors-like-china-russia-recognize, accessed 23 April 2021.

73 Dinko, "China's 'mask diplomacy'."

74 Wagner, "'Going Out.' Is China's," 101.

75 John Xie, "China's Rise Complicates Biden's Mideast Policy Plans," *VOA news*, 4 February 2021, https://www.voanews.com/usa/chinas-rise-complicates-bidens-mideast-policy-plans, accessed 5 February.

76 Ibid.

77 Scholl, "The Use of US Special Operation Forces."

78 Jevans Nyabiage, "China likely to take bigger role in peacekeeping missions in West Africa," *South China Morning Post*, 22 November 2020, https://www.scmp.com/news/china/diplomacy/article/3110553/china-likely-take-bigger-role-peacekeeping-missions-west, accessed 21 October 2021; and "China ready to help bring long-term peace to Sahel region: envoy," *Xinhuanet*, 18 November 2020, http://www.xinhuanet.com/english/2020-11/17/c_139521842.htm, accessed 18 November 2020.

79 Gilsinan, "China's Bargain." China provided more than 165 million Chinese-made vaccine doses to Latin America and the Caribbean, accompanied by a concerted public relations campaign highlighting Beijing's role. "From a public relations standpoint, China has sought to shift the narrative from China being at the center of the Covid problem to China being at the center of the Covid solution." Additionally, they provided vaccines to more than 40 African countries. Ken Moriyasu and Tsukasa Hadano, "China floats 'Africa Quad' with Germany and France," *Nikkei Asia*, 7 July 2021, https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/China-floats-Africa-Quad-with-Germany-and-France, accessed 16 July 2021.

80 Douglas MacKinnon, "China is already winning WWIII, via money," 29 May 2021, https://www.msn.com/en-ca/news/newspolitics/china-is-already-winning-world-war-iii-via-money/ar-AAKvU1g, accessed 1 June 2021.

81 Paskal, "The world doesn't realize."

82 Matthew Impelli, "Over 500 U.S. Scientists Under Investigation for Being Compromised by China," *Newsweek*, 23 April 2021, https://www.newsweek.com/over-500-us-scientists-under-investigation-being-compromised-china-1586074, accessed 24 April 2021.

83 Michael Brodka, "Arctic Competition, Climate Migration, and Rare Earths: Strategic Implications for the United States Amidst Climate Change," *The Strategy Bridge*, 1 September 2021, https://thestrategybridge.org/the-bridge/2021/9/1/arctic-competition-climate-migration-and-rare-earths-strategic-implications-for-the-united-states-amidst-climate-change, accessed 5 September 2021.

84 Kilcullen, *The Dragons and the Snakes*, 171-172. There has also been discussion about China redeveloping an old WWII U.S. military airstrip on Canton Island in the Republic of Kiribati for "tourism." This would give the Chinese a "base" in relative close proximity to Hawaii. "China's Agreement with Solomon Islands & Implications for Security in the Pacific," CDA Expert Series. An Interview with Cleo Paskal," ND, https;//cdainstitute.ca/cleo-paskal-chinas-agreement-with-solomon-islands-implications-for-security-in-the-pacific/, accessed 28 April 2022.

85 Kilcullen, *The Dragons and the Snakes*, 171-172.

86 Another example of China's expanding military basing is the new military base that China is building in Tajikistan. It is financing the new base, but in return will take full control of another military base in Tajikistan near the Afghan border that it has already been operating. Anath Krishnan, "Eye on Afghanistan, China to build military

base in Tajikistan," *The Hindu*, 28 October 2021, https://www.thehindu.com/news/international/eye-on-afghanistan-china-to-build-military-base-in-tajikistan/article37221418.ece, accessed 1 November 2021.

87 Christopher Paul, "How China plays by different rules — at everyone else's expense," *The Hill*, 6 February 2022, https://www.msn.com/en-ca/news/other/how-china-plays-by-different-rules-at-everyone-else-s-expense/ar-AATwTHH?ocid=msedgntp, accessed 6 February 2022. CCP officials serve on the boards of the companies, or the owners of companies are CCP officials. All Chinese firms are to some extent state-run, or at least state-influenced or state-subservient in a way that is incomprehensible in the U.S. The FCC does monitor foreign ownership of radio stations, but China's CRI complicates these reviews through obfuscation: by making purchases through shell companies, or through owning a partial stake (or several partial stakes) in a nominally American media group, camouflaging the extent of their influence or control while making it appear to the FCC that Chinese interest is less than 25 percent. While China takes full advantage of the opportunities of the free market, and Chinese firms buy up U.S. media, foreign firms are denied similar access in China. Chinese state-controlled media has a lock on the Chinese domestic market, with virtually no opportunity for foreign ownership, input, or influence.

88 Stew Magnuson, "SOFIC NEWS: Special Operations Command Turns Attention to Indo-Pacific," *National Defense*, 17 May 2022, https://www.nationaldefensemagazine.org/articles/2022/5/17/special-operations-command-turns-attention-to-indo-pacific, accessed 18 May 2022.

89 Charles L. Carter, "Reading the Tea Leaves. Understanding Chinese Deterrence Signaling," *Joint Forces Quarterly 103*, 2021, 39; and Jones, *Three Dangerous Men*, 141.

90 Carter, "Reading the Tea Leaves," 39.

91 Ibid., 40.

92 Alex Vershinin, "The Challenge of Dis-Integrating A2/AD Zone," *JFQ 97*, (2020), 13.

93 David Martin, "Top military official discloses new details about China's hypersonic test," *CBS News*, 17 November 2021, https://www.msn.com/en-ca/news/world/top-military-official-discloses-new-details-about-chinas-hypersonic-test/ar-AAQMQoG?ocid=sapphireappshare, accessed 18 November 2021; and Associated Press, "China's hypersonic missile test 'close to Sputnik moment', says US general Gen Mark Milley says reports about breakthrough missile have 'all our attention', and says US working on same weapons," *The Guardian*, 28 October 2021, https://www.theguardian.com/us-news/2021/oct/28/chinas-hypersonic-missile-test-close-to-sputnik-moment-says-us-general, accessed 28 October 2021.

94 Kelley M. Sayler, *Emerging Military Technologies: Background and Issues for Congress* (Washington D.C.: Congressional Research Service, 2020), 16.

95 Ibid., 16.

96 David Lague, "Special Report: U.S. rearms to nullify China's missile supremacy," *Reuters Aerospace and Defense*, 6 May 2020, https://www.reuters.com/article/us-usa-china-missiles-specialreport-us-idUSKBN22I1EQ, accessed 3 June 2021. Making the issue more difficult for the U.S. and its allies is the fact that formerly the Chinese Achilles

heel was its command-and-control (C2) nodes. The Americans, which formed a plan to use precision-guided technology to quickly decapitate these C2 nodes in time of conflict. The destruction of the command network would thus destroy the integration of enemy defenses allowing for penetration. With the more robust Chinese C2, the ability to fight a short, inexpensive, decapitation campaign, is less likely which means the U.S. would be faced with a more prolonged attrition campaign. Alex Vershinin, "The Challenge of Dis-Integrating A2/AD Zone," *JFQ 97*, 2020, 13-14.

97 O'Rourke, *Renewed Great Power Competition,* 4.

98 "China could have 1,000 nuclear warheads by 2030: Pentagon," *ABC News*, 4 November 2021, https://www.msn.com/en-ca/news/world/china-could-have--nuclear-warheads-by--pentagon/ar-AAQi6WE?ocid=sapphireappshare, accessed 4 November 2021.

99 DNI, *Annual Threat Assessment,* 7.

100 Tara Copp, "DIA Warns China's Space Tech Seeks to Block U.S. Radars, Jam Munitions," *Defense One*, 12 April 2022, https://www.defenseone.com/threats/2022/04/dia-warns-chinas-space-tech-seeks-block-us-radars-jam-munitions/365549/, accessed 20 April 2022.

101 DNI, *Annual Threat Assessment,* 8.

102 Knoll et al, "China's Irregular Approach."

103 Ibid. The researchers note as an example China's current campaign against Taiwan. They reveal that China is already waging a war of public opinion against Taiwan "to generate confusion and undermine faith in government and political institutions." They postulate that in the run-up to, and during, a conflict, Chinese forces would ramp up these efforts, especially against nations hosting U.S. forces. As an example, they believe China could promote narratives about U.S. military abuses of a local population, some exaggerated and some imagined, to turn the population against its government's support to the U.S.

104 UW is defined as "a broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery." DoD, JP 1-02, 383. See also Knoll et al, "China's Irregular Approach."

105 Knoll et al, "China's Irregular Approach."

106 Richard Walker, "Germany warns: AI arms race already underway," *DW*, 7 June 2021, https://www.dw.com/en/artificial-intelligence-cyber-warfare-drones-future/a-57769444, accessed 10 June 2021.

107 Ibid.

108 Elsa Kania, "How Should the U.S. Respond to China's Military-Civil Fusion Strategy?" *ChinaFile*, 22 May 2021, https://www.chinafile.com/conversation/how-should-us-respond-chinas-military-civil-fusion-strategy, accessed 3 June 2021.

109 Ibid.

110 Ibid.

111 Mishra, "China's Growing Security."

112 Ibid. In the fall of 2020, the PRC released "The Blue Defensive Line," a documentary film that showcased a PLA peacekeeping infantry battalion tasked with protecting local refugee camps in South Sudan. The film presented a compelling story of how Chinese peacekeepers are selflessly safeguarding peace and stability, as well as advancing development.

113 Ibid. Nigeria reportedly purchased eight armed UAVs from China. "Nigeria Takes Delivery of Chinese Drones to Combat Insurgency, Armed Banditry," *The Defense Post*, 10 November 2020, https://www.thedefensepost.com/2020/11/10/nigeria-wing-loong-drones/, 12 November 2020.

114 Mishra, "China's Growing Security"; and Mahshie, "General wields influence."

115 Mahshie, "General wields influence."

116 Celine Castronuovo, "US general warns China is actively seeking to set up an Atlantic naval base," *The Hill*, 7 May 2021, https://thehill.com/policy/defense/552331-us-general-warns-china-is-actively-seeking-to-set-up-an-atlantic-naval-base, accessed 10 May 2021. Townsend explained, "Depending on what forces and what systems they're putting in place, it puts our assets, including merchant fleet and shipping lanes and the ability for us to move our naval forces across the globe, it puts those at risk." He concluded, "This is the most significant threat, I think, from China, would be to gain a militarily useful naval facility on the Atlantic coast of Africa." Mahshie, "General wields influence."

117 Mahshie, "General wields influence."

118 In late 2012, the PRC invested heavily in the modernization of its marine fishing fleet. China implemented as series of policies that allowed fishers to replace their small, old wooden boats with larger, steel-hulled vessels. These programs provided subsidies to large segments of the Chinese fishing industry, particularly for those licensed to operate in the "Spratly waters," the 820,000 square kilometers of territory that is claimed by China. These efforts were coordinated with, and became a component of, the existing Maritime Militia. Ryan Martinson, "No Ordinary Boats: Cracking The Code On China's Spratly Maritime Militias," *Center for International Maritime Security*, 17 May 2021, https://cimsec.org/no-ordinary-boats-cracking-the-code-on-chinas-spratly-maritime-militias/, accessed 3 June 2021.

119 Since early March 2021, up to 220 boats from the PRC's Maritime Militia have been moored near Whitsun Reef in the South China Sea. The Philippine government has asked the Chinese government to direct the ships to leave its exclusive economic zone, but Beijing has denied that the ships are part of the militia, saying they are merely "fishing boats" sheltering from sea conditions. As such, China is able to underpin its claims of sovereignty by increasing pressure without the need to involve its conventional forces. See Knoll et al, "China's Irregular Approach"; and Jones, "The Future of Competition."

120 Alessandro Ford, "GameChangers 2021: How IUU Fishing Plundered Latin America's Oceans," *Insight Crime*, 23 December 2021, https://insightcrime.org/news/gamechangers-2021-iuu-fishing-plundered-latin-americas-oceans/, accessed 21 January 2022.

121 Knoll et al, "China's Irregular Approach."

122 "Taiwan expelled thousands of Chinese dredgers from its waters," *AFP*, 25 January 2025, https://a.msn.com/r/2/BB1d4dnj?m=en-ca&referrerID=InAppShare, accessed 25 January 2021.

123 Ibid.

124 "Taiwanese jets scramble as Chinese planes enter air defence zone," *The Globe & Mail*, 21 June 2022, https://www.theglobeandmail.com/world/article-taiwanese-jets-scramble-as-chinese-planes-enter-air-defence-zone/, accessed 22 June 2022; "Taiwan expelled thousands of Chinese dredgers from its waters," *AFP*, 25 January 2025, https://a.msn.com/r/2/BB1d4dnj?m=en-ca&referrerID=InAppShare, accessed 25 January 2021; and Eric Cheung and Brad Lendon, "China air force sends 77 warplanes into Taiwan defense zone over two days, Taipei says," *CNN*, 3 October 2021, https://www.msn.com/en-ca/news/world/china-air-force-sends--warplanes-into-taiwan-defense-zone-over-two-days-taipei-says/ar-AAP57ZO?ocid=sapphireappshare, accessed 4 October 2021.

125 "Three Rounds of Coercion in Philippine Waters," *Center for Strategic and International Studies*, 26 May 2022, https://amti.csis.org/three-rounds-of-coercion-in-philippine-waters/, accessed 21 June 2022.

126 "Trudeau calls China's actions toward Canadian planes 'provocative and irresponsible'," *CBC*, 6 June 2022, https://www.cbc.ca/news/world/china-canada-harass-warplanes-1.6478645, accessed 10 June 2022. Chinese jets frequently flew as close as 20 to 100 feet from Canadian aircraft. The Canadian CP-140 Aurora airplanes were taking part in Operation Neon, a UN effort to monitor sanctions against North Korea in the Asia-Pacific region and prevent the rogue nation's development of weapons of mass destruction. There have been approximately 60 of these types of intercepts with Chinese fighter jets in a six-month period, over two dozen of which have been deemed dangerous. Mercedes Stephenson and Sean Boynton, "Canada alarmed as Chinese fighter pilots 'buzz' Canadian planes over international waters," *Global News*, 1 June 2022, https://www.msn.com/en-ca/news/canada/canada-alarmed-as-chinese-fighter-pilots-buzz-canadian-planes-over-international-waters/ar-AAXYybG?ocid=sapphireappshare, 3 June 2022.

127 Adam Ramzy, "Chinese Pilots Sent a Message. American Allies Said They Went Too Far," *The New York Times*, 9 June 2022, https://www.nytimes.com/2022/06/09/world/asia/china-military-united-states-australia-canada.html, accessed 10 June 2022.

128 Knoll et al,

129 Monique Beals, "FBI chief says espionage threat posed by China 'unprecedented in history'," *The Hill*, 24 April 2022, https://www.msn.com/en-ca/news/politics/fbi-chief-says-espionage-threat-posed-by-china-unprecedented-in-history/ar-AAWxwSE?ocid=sapphireappshare, accessed 25 April 2022; and Pete Williams, "FBI Director Wray says scale of Chinese spying in the U.S. 'blew me away'," *NBC News*,

1 February 2022, https:// www.nbcnews.com/politics/politics-news/fbi-director-wray-says-scale-chinese-spying-us-blew-away-rcna14369, accessed 3 February 2020.

130 Eftimiades, *Chinese Espionage,* 38.

131 Ibid., 5.

132 Cited in Jones, *Three Dangerous Men*, 147.

133 Harding, "The Intelligence Community."

134 RAND, "Cyber Warfare," https://www.rand.org/topics/cyber-warfare.html, accessed 14 February 2022.

135 Katie Terrell Hanna, Kevin Ferguson and Linda Rosencrance, "Cyberwarfare," https://www.techtarget.com/searchsecurity/definition/cyberwarfare, accessed 14 February 2022.

136 Paskal, "The world doesn't realize."

137 DNI, *Annual Threat Assessment,* 8. The CIA thinks that China has been identifying CIA agents when they arrived in foreign countries. CIA officials believed the answer was likely data-driven—and related to a Chinese cyberespionage campaign devoted to stealing vast troves of sensitive personal private information, like travel and health data, as well as U.S. government personnel records. U.S. officials believed Chinese intelligence operatives had likely combed through and synthesized information from these massive, stolen caches to identify the undercover U.S. intelligence officials. It was very likely a "suave and professional utilization" of these datasets. Zach Dorfman, "China Used Stolen Data to Expose Cia Operatives in Africa and Europe," *Foreign Policy*, 21 December 2020.

138 Kevin Collier, "China behind another hack as U.S. cybersecurity issues mount," *NBC News*, 21 April 2021, htpps:// www.nbcnews.com/tech/security/china-another-hack-us-cybersecurity-issues-mount-rcna744, accessed 22 April 2021.

139 Dorfman, "China Used Stolen Data."

140 Ibid.

141 Aria-body, which was housed in a WORD document sent as an attachment, basically acted as an invisible cyberattack tool that had never been detected before. Hackers could use it to remotely seize control of a computer and copy, delete or create files, as well as undertake extensive searches of the targeted device's data. Notably, the software had new ways of covering its tracks to avoid detection. Ronen Bergman and Steve Lee Myers, "China's Military Is Tied to Debilitating New Cyberattack Tool," *The New York Times*, 7 May 2020, https://www.nytimes.com/2020/05/07/world/asia/china-hacking-military-aria.html, accessed 10 May 2020.

142 Ibid.

143 Evgeny Pashentsev, "Coronavirus Pandemics, Huawei 5G Technologies, Artificial Intelligence and Psychological Operations," *Eurocontinent*, 20 April 2020, https://www.

eurocontinent.eu/2020/04/coronavirus-pandemics-huawei-5g-technologies-artificial-intelligence-and-psychological-operations-evgeny-pashentsev/, accessed 19 April 2021.

144 Jones, *Three Dangerous Men*, 162.

145 Ibid., 146.

146 Guttieri, "Accelerate Change or Lose," 98.

147 "China's spies are not always as good as advertised," *The Economist*, 1 June 2022, https://www.economist.com/china/2022/06/01/chinas-spies-are-not-always-as-good-as-advertised, accessed 3 June 2022.

148 Nicole Perlroth, "How China Transformed Into a Prime Cyber Threat to the U.S." *The New York Times*, 19 July 2021, https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html, accessed 20 July 2021.

149 Cited in Elsa B. Kania, "Minds at War. China's Pursuit of Military Advantage through Cognitive Science and Biotechnology," *Prism*, Vol 8, No. 3, (2019), 85.

150 Cited Jones, *Three Dangerous Men,* 142.

151 Disinformation is defined as "the deliberate creation and sharing of false and / or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain," is one example of how society has been ill-served by the new information driven world. Niels Nagelhus Shia and Lars Gjesvik, "Hacking democracy: managing influence campaigns and disinformation in the digital age," *Journal of Cyber Policy*, 2020, https://doi.org/10.1080/23738871.2020.1820060, accessed 18 February 2021. There are numerous definitions for disinformation. For example, Joohn Choe, believes "Disinformation is the propagation of narratives that create a strategic psychological effect in a target population." Joohn Choe, "The Resistance Endgame, Part I: Assumptions," 12 November 2018, https://joohnchoe.medium.com/the-resistance-endgame-part-i-assumptions-f00fa452efa7, accessed 15 February 2021. Researchers for the US Advisory Commission on Public Diplomacy assert "disinformation, or the manipulation and dissemination of information is designed to adversely influence public perceptions and behaviors." Vivian S. Walker and Ryan E. Walsh, *Public Diplomacy and The New "Old" War: Countering State-Sponsored Disinformation* (Washington D.C.: US Advisory Commission on Public Diplomacy, 2020), 4. Finally, the Oxford English Dictionary defines disinformation as "false information which is intended to mislead, especially propaganda issued by a government organization to a rival power or the media," https://www.lexico.com/definition/disinformation, accessed 23 February 2021.

152 Mazarr et al, *Understanding Influence,* 1.

153 Scott W. Harold, Nathan Beauchamp-Mustafaga, Jeffrey W. Hornung, *Chinese Disinformation Efforts on Social Media* (Santa Monica, CA: RAND, 2021).

154 David Klepper and Amanda Seitz, "Facebook: Fake scientist used to spread anti-US propaganda," *The Canadian Press*, 2 December 2021, https://www.msn.com/en-ca/news/science/facebook-fake-scientist-used-to-spread-antius-propaganda/ar-AARm9jt?ocid=sapphireappshare, accessed 4 December 2021.

155 Flora Carmichael, "How a fake network pushes pro-China propaganda," *BBC News*, 5 August 2021, https://www.bbc.com/news/world-asia-china-58062630, accessed 6 August 2021. See also Christian Johnson and William Marcellino, *Truth Decay. Bad Actors in News Reporting* (Santa Monica: RAND, 2017).

156 Joseph Choi, "Documents show Chinese government collects droves of data from Western social media: report," *The Hill*, 31 December 2021, https://www.msn.com/en-ca/newspolitics/documents-show-chinese-government-collects-droves-of-data-from-western-social-media-report/ar-AASjNfg?ocid=sapphireappshare, accessed 1 January 2022.

CHAPTER 3

1 Kilcullen, *The Dragons and the Snakes*, 241.

2 NATO Reflection Group, *NATO 2030: United for a New Era* (Brussels: NATO, 25 November 2020), 16.

3 "Former Navy SEAL commander says Putin has outplayed the US and Russia is the greatest external security threat," *Business Insider*, 8 February 2021, http://www.wearethemighty.com/intel/seal-says-putin-played-us/, accessed 8 February 2021.

4 Biden, *Interim National Security Strategic Guidance*, 8.

5 Harding, "The Intelligence Community's."

6 Ibid.

7 Kilcullen, *The Dragons and the Snakes*, 123.

8 DNI, *Annual Threat Assessment*, 12.

9 TRADOC, *The U.S. Army in Multi-Domain,* vi, 6–7.

10 Farwell, *Adversarial Tactics*, 6. Researchers note that success requires satisfaction of four conditions:

1. Russia has weak neighboring state that lacks robust civil society and has local ethnic or language divisions that can be exploited;
2. weak neighbor has ethnic or linguistic ties to Russia;
3. Russia has local escalation dominance; and
4. Russia seeks to revise the status quo.

11 Putten et al, *Hybrid Conflict*, 5.

12 Elliot Smith, "Russia is building its military influence in Africa, challenging U.S. and French dominance," *CNBC*, 13 Sep 2021, https://www.cnbc.com/2021/09/13/russia-is-building-military-influence-in-africa-challenging-us-france.html, accessed 13 September 2021.

13 Benjamin Arbitter and Kurt Carlson, "The Changing Face of Russian Counter-Irregular Warfare," *War On The Rocks*, 21 December 2021, https://Warontherocks.

Com/2021/12/The-Changing-Face-Of-Russian-Counter-Irregular-Warfare/, accessed 21 December 2021.

14 Anna Cooban, "Why Russia isn't hurting even as it cuts off Europe's gas," *CNN*, 1 June 2022, https://www.cnn.com/2022/06/01/energy/eu-russia-gas-cut-off-value/index.html, accessed 17 June 2021; and "Poland and Bulgaria say they will not succumb to Russia's 'gas blackmail'," *Associated Press*, 27 April 2022, https:// www.cbc.ca/news/world/russia-war-ukraine-gas-europe-1.6432270, accessed 27 April 2022.

15 Jonathan Hackenbroich, "Chinese and Russian economic pressure games – what policy for Sweden and Europe?" *European Council on Foreign Relations*, 2 December 2021, https://ecfr.eu/event/chinese-and-russian-economic-pressure-games-what-policy-for-sweden-and-europe/, accessed 21 February 2021; and Agata Wierzbowska-Miazga and Arkadiusz Sarna, "Russian economic pressure on Ukraine," Centre for Eastern Studies, 26 March 2014, https://www.osw.waw.pl/en/publikacje/analyses/2014-03-26/russian-economic-pressure-ukraine, accessed 21 February 2022.

16 Stephen Dayspring, "Countering Russian Hybrid Warfare: Acknowledging the Character of Modern Conflict," *CTX*, Vol 6, No. 4, 25.

17 Kilcullen, *The Dragons and the Snakes*, 241.

18 Barbara Starr, "Classified US military war game set to take place as concerns about threats posed by China and Russia increase, *CNN*, 27 March 2021, https://a.msn.com/r/2/BB1f1xi6?m=en-ca&referrerID=InAppShare, accessed 27 March 2021.

19 Paul Kirby, "Russia claims first use of hypersonic Kinzhal missile in Ukraine," *BBC News*, 19 March 2022, https://www.bbc.com/news/world-europe-60806151#:~:text=Russia%27s%20military%20has%20fired%20a,ministry%20in%20Moscow%20has%20said, accessed 21 March 2022.

20 Ellen Mitchell, "Outcry grows over Russian missile test that hit satellite," *The Hill*, 17 November 2021, https://www.msn.com/en-ca/news/politics/outcry-grows-over-russian-missile-test-that-hit-satellite/ar-AAQO4K0?ocid=sapphireappshare, accessed 18 November 2021.

21 Thomas Kingsley, "Russia showcases new generation of laser weapons that can blind satellites '1,500km above earth'," *The Independent*, 18 May 2022, https://www.msn.com/en-gb/news/world/ukraine-news-–-live-war-crime-trial-against-russia-begins-as-mariupol-fighters-reach-prison/ar-AAXpn2u?li=AAnZ9Ug, accessed 18 May 2022.

22 Raymond McConoly, "Russian Navy Ships Get More Powerful with Kamikaze drones," *Naval Post*, 30 October 2021, https://navalpost.com/russian-navy-kamikaze-drones/?fbclid=IwAR3MBQilWkpfao4VvgHBecPMuMxanYNA-_Pnvm478n-DiIqT2lDuc-6LWqo, accessed 2 November 2021.

23 Vladimir Isachenkov, "Russia to form 20 new military units in west to counter NATO," *Globe & Mail*, 31 May 2021, https://www.theglobeandmail.com/world/article-russia-to-form-20-new-military-units-in-west-to-counter-nato-2/, accessed 1 June 2021.

24 Dr. Vira Ratsiborynska, Daivis Petraitis and Valeriy Akimenko, *Russia's Strategic Exercises: Messages and Implications* (Riga: NATO Strategic Communications Centre of Excellence, 2020), 5-7.

25 Dr. Jānis Bērziņš, "The Evolution of the Concept of Russian New Generation Warfare: Implications for European Security," *National Defence Academy of Latvia*, Latvia, 2015, https://www.doria.fi/bitstream/handle/10024/117647/BERZINS%20Janis_WG10_Abstract_The%20Evolution%20of%20the%20Concept%20of%20Russian%20New%20Generation%20Warfare-Implications%20for%20European%20Security.pdf?sequence=2, accessed 19 April 2021.

26 Abdullah Atay, "The Strategic Utility of the Russian Spetsnaz in Crimea," *CTX*, Vol. 6, No. 4, 48.

27 Vladimir Isachenkov, "Russia orders troop pullback, but keeps weapons near Ukraine," *CTV News*, 22 April 2021, https://www.ctvnews.ca/world/russia-orders-troop-pullback-but-keeps-weapons-near-ukraine-1.5397601, accessed 22 April 2021; and "Russia to pull troops back from near Ukraine," *BBC*, 23 April 2021, https://www.bbc.com/news/world-europe-56842763, accessed 22 April 2021.

28 Russia has up to 190,000 troops near Ukraine border - US envoy," *BBC,* 18 February 2022, https://www.bbc.com/news/live/world-europe-60428211, accessed 18 February 2022.

29 Julian E. Barnes, "U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion," *The New York Times*, 3 February 2022, https://www.nytimes.com/2022/02/03/us/politics/russia-ukraine-invasion-pretext.html, accessed 3 February 2022; "Russia-Ukraine: US warns of 'false-flag' operation," *BBC News*, 14 January 2022. https://www.bbc.com/news/world-europe-59998988, accessed 14 January 2022; and Katherine Lawlor with Kateryna Stepanenko, "Warning Update: Russia May Conduct a Chemical or Radiological False-Flag Attack as a Pretext for Greater Aggression against Ukraine," *Institute for the Study of War*, 9 March 2022, https://understandingwar.org/backgrounder/warning-update-russia-may-conduct-chemical-or-radiological-false-flag-attack-pretext, accessed 12 June 2022.

30 Patrick Wintour, Luke Harding and Shaun Walker, "West plans to arm resistance if Russian forces occupy Ukraine," *The Guardian*, 20 February 2022, https://www.theguardian.com/world/2022/feb/19/west-plans-to-arm-resistance-if-russian-forces-occupy-ukraine, accessed 21 February 2022; Aya Al-Hakim, "Biden says U.S. believes Russia will attack Ukraine in 'coming days'," *Global News*, 18 February 2022, https://www.msn.com/en-ca/news/world/ukraine-says-russian-special-forces-planted-explosives-at-donetsk-facilities/ar-AAU2Tts?ocid=sapphireappshare, accessed 19 February 2022; and Haley Ott, "Russian-backed separatist leaders declare full military mobilization," *CBS News*, 19 February 2022, https://www.msn.com/en-ca/news/world/russianbacked-separatist-leaders-declare-full-military-mobilization/ar-AAU3XRz?ocid=sapphireappshare, accessed 19 February 2022.

31 "Moscow Orders Troops to Ukraine's Breakaway Regions After Putin Recognizes Them," *The New York Times*, 22 February 2022, https://www.nytimes.com/live/2022/02/21/world/ukraine-russia-putin-biden, accessed 22 February 2022.

32 Kari Paul and Dan Milmo, "Russia-backed hackers behind powerful new malware, UK and US say," *The Guardian,* 24 February 2022, https://www.theguardian.com/world/2022/feb/23/russia-hacking-malware-cyberattack-virus-ukraine, accessed 24 February 2022; "IntelBrief: The Role of the Wagner Group in Russia's Full-Scale War with Ukraine," *The Soufan Center*, 24 February 2022, https://thesoufancenter.org/intelbrief-2022-february-24/, accessed 24 February 2022; and "IntelBrief: Russian Disinformation Forms Key Part of the Kremlin's Approach to Conflict with Ukraine," *The Soufan Center*, 23 February 2022, https://thesoufancenter.org/intelbrief-2022-february-23/, accessed 24 February.

33 Saba Aziz, "Putin puts nuclear forces on high alert as Ukraine agrees to talks with Russia," *Global News*, 27 February 2022, https://www.msn.com/en-ca/news/world/putin-puts-nuclear-forces-on-high-alert-as-ukraine-agrees-to-talks-with-russia/ar-AAUni8u?ocid=msedgntp, accessed 27 February 2022; and Mark Gollom, "Putin implies nuclear attack if West interferes in Ukraine. Why it's not just an empty threat," *CBC News*, 25 February 2022, https://ici.radio-canada.ca/rci/en/news/1864840/putin-implies-nuclear-attack-if-west-interferes-in-ukraine-why-its-not-just-an-empty-threat?presentid=webnews&ocid=msedgdhp, accessed 25 February 2022.

34 Declan Walsh, "U.N. says Russian mercenaries in Central African Republic are driving war crimes," *The Globe & Mail*, 27 June 2021, https://www.theglobeandmail.com/world/article-un-says-russian-mercenaries-in-central-african-republic-are-driving/, accessed 28 June 2021; and Sebastian Shukla, "Russian mercenaries get the big-screen treatment. The reality behind the film is as murky as the plot," *CNN*, 28 May 2021, https://www.cnn.com/2021/05/28/africa/wagner-mercenaries-tourist-film-car-cmd-intl/index.html, accessed 3 June 2021.

35 Stephen Smith, "Macron's Mess in the Sahel," *Foreign Affairs*, 10 March 2022, https://www.foreignaffairs.com/articles/west-africa/2022-03-10/macrons-mess-sahel, accessed 12 March 2022.

36 Jones, "The Future of Competition."

37 Andrew S. Bowen, *Russian Military Intelligence: Background and Issues Congress* (Washington D.C.: Congressional Research Service, 2020), 13. Reportedly, U.S. intelligence sources believed Unit 29155 was also responsible for numerous incidents across Europe and the Balkans. See also Jones, *Three Dangerous Men,* 26. Unit 29155 is comprised largely of former Spetsnaz unit members with deep experience in Central Asia, Africa, the Middle East, and Europe. It was also responsible for assassination as well as other activities to destabilize political opponents in Russia's "near abroad." Chris Cruden, "Flunking The New York Times Test: Making Sense of Russian 'Covert' Action," *Modern War Institute*, 21 February 2022, https://Mwi.Usma.Edu/Flunking-The-New-York-Times-Test-Making-Sense-Of-Russian-Covert-Action/, accessed 21 February 2022.

38 Seth G. Jones, Catrina Doxsee, Brian Katz, Eric McQueen and Joe Moye, *Russia's Corporate Soldiers* (New York: Centre for Strategic & International Studies, 2021), 1. PMCs also permit Russian leaders and oligarchs a means to expand trade and economic influence in the developing world and increase their wealth. For example, PMCs have allowed them access to oil and gas in Syria; gold, uranium, arms, and diamonds in the CAR; oil, gold, and arms in Venezuela; and arms, infrastructure projects, and hydrocarbons in Libya.

39 The Wagner Group, also called "Putin's Private Army," is an umbrella of private military contractor firms that have been linked to Yevgeny Prigozhin (also known as "Putin's Cook") who is a close ally of Russian President Vladimir Putin. The "mercenaries" in the Wagner Group have taken active part in various conflicts, including operations in the Syrian Civil War on the side of the Syrian Government, as well as in Libya and Mali. In addition, they operated from 2014 until 2015, in the conflict in Donbas in Ukraine aiding the separatist forces of the self-declared Donetsk and Luhansk People's Republics, and more recently in the 2022 invasion of Ukraine in 2022.

40 Julia Fiedrich and Niklas Mashur, "Mercenaries in the Service of Authoitarian States," *CSS Analyses in Security Policy*, No. 274, November 2020, 2, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse274-EN.pdf, accessed 21 April 2021.

41 Ibid., 2.

42 *Russian Private Military Companies* (Fort Meade, MD: Asymmetric Warfare Group, 2020), ix-x. Not surprisingly, companies linked to the Wagner Group have grabbed up a number of oil and gas leases. As such, researchers conclude that Russian PMCs will be a "a permanent fixture on the landscape of the Middle East and African oil and gas development for a time to come. Amy Mackinnon, "Putin's Shadow Warriors Stake Claim to Syria's Oil," *Foreign Policy*, 17 May 2021, https://foreignpolicy.com/2021/05/17/putin-shadow-warriors-stake-claim-syria-oil-energy-wagner-prigozhin-libya-middle-east/, accessed 7 July 2021.

43 Molly Dunigan and Ben Connable, "Russian Mercenaries in Great Power Competition: Strategic Supermen or Weak Link?" The RAND Blog, 9 March 2021, https://www.rand.org/blog/2021/03/russian-mercenaries-in-great-power-competition-strategic.html, accessed 14 June 2021. Dmitry Utkin, a former commander of the GRU's Spetsnaz units, allegedly founded the Wagner Group in 2014.

44 In exchange for services, Wagner Group and its subsidiaries are often granted exclusive privileges and licenses for resource exploitation. Mustapha Dalaa, Halime Afra Aksoy, "Russia's Wagner Group reportedly deployed in Africa," *AA.Com*, 5 March 2021, https://www.aa.com.tr/en/world/russias-wagner-group-reportedly-deployed-in-africa/2165414, accessed 11 March 2021.

45 Bowen, *Russian Military Intelligence*, 13.

46 Department of Homeland Security, "Bulletin: Warning of Potential for Cyber Attacks Targeting the United States in the Event of a Russian Invasion of Ukraine," *CNN*, 24 January 2022, https://www.cnn.com/2022/01/24/politics/russia-cyberattack-warning-homeland-security/index.html, accessed 24 February 2022.

47 For three weeks the Russian cyber-attacks were conducted against political, financial, and diplomatic institutions. Next, Russian state-run media, initiated misinformation and disinformation campaigns and propaganda against the Estonian government. Subsequently, a series of protests followed by ethnic-Russian Estonians with the intent to promote an insurrection. The cyber-attacks defaced public websites. These attacks were also coordinated with distributed denial of service (DDoS) attacks of the Estonian banking system and other governmental servers. Simultaneously, Russia's state-run media,

Russia Today (*RT*) and *Sputnik News* networks broadcast hostile political rhetoric about the regime while playing to ethnic-Russian citizens, attempting to provoke a separatist movement. Guido l. Torres, "Nonlinear Warfare: Is Russia Waging a Silent War in Latin America?" *Small Wars Journal*, 24 January 2022, https://smallwarsjournal.com/jrnl/art/nonlinear-warfare-russia-waging-silent-war-latin-america, accessed 9 February 2022.

48 All hackers were Russian nationals who worked for the Russian government and represented individuals from the State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics, as well as members of a Center 16 operational unit. U.S. Department of Justice, "Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide," *Justice News*, 24 March 2022, https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical, accessed 25 March 2022; and Jones, *Three Dangerous Men*, 68.

49 Russian hackers from the GRU, broke into three different Ukrainian power companies' networks, and waited for the opportune time to launch their attack. Investigators state, "They broke in over the summer, got into position and they started learning how to operate those systems." As a result, "they disconnected over 60 substations across Ukraine and caused blackouts for around 225,000 customers in the dead of winter." A year later, the GRU hackers returned with a more sophisticated attack, an automated piece of malware that could cripple multiple transmission stations with one keystroke. "Russian hacking group compromised U.S. power companies." *CBS News*, 16 April 2022, https://www.msn.com/en-ca/news/politics/russian-hacking-group-compromised-us-power-companies/ar-AAWjqCF?ocid=sapphireappshare, accessed 17 April 2022.

50 The U.S. Government identified Unit 26165 as one of two Russian cyber responsible for hacking the Democratic Congressional Campaign Committee, Democratic National Committee, and the presidential campaign of Hillary Clinton. Media and Western governments also have linked Unit 26165 to cyber operations against numerous political, government, and private sector targets in the United States and Europe. Similarly, Unit 74455 has been linked to some of Russia's most brazen and damaging cyberattacks. The U.S. government identified Unit 74455 as responsible for the coordinated release of stolen emails and documents during the 2016 U.S. presidential election. Andrew S. Bowen, "Russian Cyber Units," (Washington D.C.: Congressional Research Service, February 2022), 1.

51 In the summer of 2017, a DOJ indictment says, Russian hackers launched a cyberattack on the safety system of Saudi Arabia's Petro Rabigh petrochemical and refinery complex. Investigators believe that the hackers could have set off explosions and released toxic chemicals in the Saudi plant with the malware they installed, known as "Triton." They noted, "It's the first time in history we've ever seen a cyberattack explicitly designed to kill people. It targets safety systems. And these safety systems are only there to protect lives. So going after that system explicitly, the only reason to do it is to hurt people." The disaster was only averted because the hackers made a small error in their software. Rather than achieving their goal of causing an explosion, they instead were able to just shut down the plant. Russian hacking group compromised U.S. power companies," *CBS News*, 16 April 2022, https://www.msn.com/en-ca/news/politics/russian-hacking-group-compromised-us-power-companies/ar-AAWjqCF?ocid=sapphireappshare, accessed 17 April 2022.

52 Ukrainian websites were paralyzed by DDoS cyber-attacks prior to Russia's invasion. Ukraine's defense, foreign affairs and interior ministries, among others, were knocked offline on 23 February. Ukrainian agencies and banks had been attacked with DDoS cyber-attacks as early as 15 February. Some websites were crippled already in January. Evidence pointed to the GRU being responsible for the attacks. Colin Demarest, "Ukraine pelted with cyberattacks ahead of Russian assault," *C4ISRnet*, 24 February 2022, https://www.c4isrnet.com/battlefield-tech/it-networks/2022/02/24/ukraine-pelted-with-cyberattacks-ahead-of-russian-assault/, accessed 13 March 2022; David E. Sanger and Nicole Perlroth, "Russia appears to carry out hack through system used by U.S. aid agency," *The New York Times*, 28 May 2021, https://www.theglobeandmail.com/world/article-russia-appears-to-carry-out-hack-through-system-used-by-us-aid-agency/, accessed 28 May 2021; Maggie Miller, "New cyberattacks ramp up tensions with Russia," *The Hill*, 7 July 2021, https://www.msn.com/en-ca/news/newspolitics/new-cyberattacks-ramp-up-tensions-with-russia/ar-AALS2Zc, accessed 7 July 2021; Bowen, *Russian Military Intelligence*, 1; and Alina Polyakova and Spencer P. Boyer, *The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition*, Brookings Institute, March 2018, 13-14, https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf, accessed 20 April 2021. Russian state sponsored hackers that injected malicious code into updates for SolarWinds' Orion software, infiltrated and compromised private-sector companies that included Microsoft, Cisco, Intel and Nvidia. Robert Scammell, "SolarWinds cyber strike: Russia did it, say US and UK," *Verdict*, 16 April 2021, https://www.verdict.co.uk/solarwinds-russia-us-uk/ accessed 19 April 2021; and Jonathan Greig, "Russian government procured powerful botnet to shift social media trending topics," *The Record*, 20 May 2022, https://therecord.media/russia-botnet-fronton-social-media-nisos/, accessed 1 June 2022.

53 Russian hacking group compromised U.S. power companies," *CBS News*, 16 April 2022,https://www.msn.com/en-ca/news/politics/russian-hacking-group-compromised-us-power-companies/ar-AAWjqCF?ocid=sapphireappshare, accessed 17 April 2022.

54 Bowen, *Russian Military Intelligence*, 17-18.

55 Ibid., 17-18.

56 Nomaan Merchant, Eric Tucker, And Frank Bajak, "NSA discloses hacking methods it says are used by Russia," *The Globe & Mail*, 1 July 2021, https://www.theglobeandmail.com/business/international-business/article-nsa-discloses-hacking-methods-it-says-are-used-by-russia/, accessed 2 July 2021.

57 See Miriam Matthews, Alyssa Demus, Elina Treyger, Marek N. Posard, Hilary Reininger and Christopher Paul, *Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe* (Santa Monica, CA: RAND, 2021).

58 Artis Pabriks and Andis Kudors, eds., *The War in Ukraine: Lessons for Europe* (Riga: University of Latvia Press, 2015), 45.

59 Farwell, *Adversarial Tactics*, 5. Reflexive control requires the application of "strong psychological pressure and driving messages that provoke emotional responses and disadvantage the enemy require influence operations that go beyond traditional military deception or military information support operations." The Russian flooding

of social media with reinforcing messages of conspiracies and political disinformation in the U.S. during the 2016 election is one example.

60 Global Engagement Center, *U.S. Department of State, GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem* (Washington D.C.: U.S. Department of State, 2020), 8.

61 Thomas Colson, "Russia is using the power of 'Black PR' to destroy political reputations and spread disinformation in the West," *Business Insider*, 5 June 2021, https://www.businessinsider.com/black-pr-is-powering-russia-disinformation-efforts-in-the-west-2021-6?r=US&IR=T, accessed 8 June 2021. Russia utilizes "Dark PR" or "Black PR," which "is broadly defined as the practice of ruining reputations through dishonest public relations tactics, court battles, and other highly shady tactics. It first emerged in post-Soviet 1990s Russia as a means for political operators acting on behalf of state actors to destroy their opponents' reputations."

62 "America's adversaries continue to stoke online misinformation, says intel report," *ABC News*, 26 March 2021, https://www.msn.com/en-ca/news/newspolitics/americas-adversaries-continue-to-stoke-online-misinformation-says-intel-report/ar-BB1eZEDq, accessed 26 March 2021.

63 Torres, "Nonlinear Warfare."

64 Putten et al, *Hybrid Conflict*, 8-9.

65 Jones, "The Future of Competition."

66 Jones, *Three Dangerous Men*, 131.

67 "Russian State Media Fueling Canadian Anti-Vaccination and Anti-Mask Movements," *DisinfoWatch*, 16 September 2021, https://disinfowatch.org/russian-state-media-fueling-canadian-anti-vaccination-and-anti-mask-movements/, accessed 17 September 2021.

68 Ibid.

69 Jason Burke, "Facebook struggles as Russia steps up presence in unstable west Africa," *The Guardian*, 17 April 2022, https://www.theguardian.com/world/2022/apr/17/facebook-struggles-as-russia-steps-up-presence-in-unstable-west-africa, accessed 19 April 2022.

70 Edward Malnick, "Inside the secret government unit returning fire on Vladimir Putin's 'weaponised lies'," *The Telegraph*, 19 March 2022, https://news.yahoo.com/inside-secret-government-unit-returning-155455557.html?guccounter=1&guce_referrer=aHR0cHM6Ly93ZWJtYWlsLmJlbGwubmV0Lw&guce_referrer_sig=AQAAABfkE1Rc8MVp6dWNgyXOIpm10D6rWUEVKvbNY9vQxNQedG15rJB81f5b4Extqjrqp8bH_2LyivxWpKyGHmSejR0F99AlAdEQi0OS0kTM7TAT5lULHftF_oSNd8DwAKYGrlw9kOisHUom0KHaWgMK1vJaZ_WaeM0jg_GJ3wL8Q33g, accessed 21 March 2022; and Alex Hern, "TikTok algorithm directs users to fake news about Ukraine war, study says," *The Guardian*, 21 March 2022, https://www.theguardian.com/technology/2022/mar/21/tiktok-algorithm-directs-users-to-fake-news-about-ukraine-war-study-says, accessed 21 March 2022.

71 "IntelBrief: Russia Recycles Disinformation Playbook in Ukraine During Assault on Mariupol," *The Soufan Center*, 25 April 2022, https://thesoufancenter.org/intelbrief-2022-april-25/, accessed 25 April 2022.

72 Noor Ibrahim, "'We are not prepared': Russia uses artificial intelligence, deep fakes in propaganda warfare," *Global News*, 29 March 2021, https://www.msn.com/en-ca/news/world/we-are-not-prepared-russia-uses-artificial-intelligence-deep-fakes-in-propaganda-warfare/ar-AAVFfWz?ocid=sapphireappshare, accessed 1 April 2022; and Geof Nixon, "Zelensky, Putin videos provide glimpse of evolving deepfake threat, experts say," *CBC News*, 20 March 2022, https://www.msn.com/en-ca/news/canada/zelensky-putin-videos-provide-glimpse-of-evolving-deepfake-threat-experts-say/ar-AAVhUqg?ocid=msedgntp, accessed 20 March 2022.

73 Io Dodds, "The West is losing the information war with Russia – and hasn't even noticed," *The Telegraph*, 22 March 2022, https://news.yahoo.com/why-west-losing-information-war-173628620.html, accessed 23 March 2022.

74 Carl Miller and Jeremy Reffin, "#IstandwithRussia – Anatomy of a Pro-Kremlin Influence Operation," *Institute for Strategic Dialogue*, 8 March 2022, https://www.isdglobal.org/digitaldispatches/istandwithrussia-anatomy-of-a-pro-kremlin-influence-operation/, accessed 13 March 2022. Due the large amount of disinformation being spewed out, Britain created a new counter-disinformation unit, the Government Information Cell (GIC), set up specifically to dispel disinformation being spread by Russia. The Cell is responsible for trawling through online and broadcast material to identify disinformation and address it directly. Ministers and officials see the counter-disinformation effort as a vital element of the support Britain is providing to Ukraine. A senior official in the unit told *The Telegraph* that the Kremlin was "weaponising lies" and using untruths "to justify the unjustifiable". The information cell was "exposing those lies by countering Kremlin disinformation." The approach was described as "pre-bunking." Edward Malnick, "Inside the secret government unit returning fire on Vladimir Putin's 'weaponised lies'," *The Telegraph*, 19 March 2022, https://news.yahoo.com/inside-secret-government-unit-returning-155455557.html?guccounter=1&guce_referrer=aHR0cHM6Ly93ZWJtYWlsLmJlbGwubmV0Lw&guce_referrer_sig=AQAAABfkE1Rc8MVp6dWNgyXOIpm10D6rWUEVKvbNY9vQxNQedG15rJB81f5b4Extqjrqp8bH_2LyivxWpKyGHmSejR0F99AlAdEQi0OS0kTM7TAT5lULHftF_oSNd8DwAKYGrlw9kOisHUom0KHaWgMK1vJaZ_WaeM0jg_GJ3wL8Q33g, accessed 21 March 2022.

75 Farwell, *Adversarial Tactics,* 6-7.

76 Ibid., 7-8.

77 Torres, "Nonlinear Warfare."

CHAPTER 4

1 Putten et al, *Hybrid Conflict*, 2, 15-16.

2 Ibid., 16-17.

3 Polyakova and Boyer, *The Future of Political Warfare*.

4 According to a report produced by the Federal Research Division of the Library of Congress, the MOIS has overall responsibility for covert Iranian operations, but since its founding in 1990, the Quds Force has typically carried out extraterritorial operations like assassinations. As a result, MOIS usually executes internal operations itself and the Quds Force normally conducts extraterritorial operations such as sabotage, assassinations, and espionage. Matthew Levitt, "Trends in Iranian External Assassination, Surveillance, and Abduction Plots," *CTC Sentinel*, February 2022, Vol. 15, Issue 2, 1-11.

5 In a 1997 U.S. State Department briefing, Ambassador Philip Wilcox stated that, "since 1990, we estimate and indeed, we have solid information for, that Iran is responsible for over 50 murders of political dissidents and others overseas." Ibid., 1-11.

6 Ibid., 1-11.

7 Ibid., 1-11; and Celine Castronuovo, "Feds say Iran backed plot to kidnap US-based journalist," *The Hill*, 14 July 2021, https://a.msn.com/r/2/AAM7LOr?m=en-ca&referrerID=InAppShare, accessed 16 July 2021.

8 Levitt, "Trends in Iranian," 1-11.

9 Jon Gambrell, "U.S., Iran in tense sea incident as Tehran preps centrifuges," *CTV News*, 21 June 2022, https://www.ctvnews.ca/world/u-s-iran-in-tense-sea-incident-as-tehran-preps-centrifuges-1.5955952, accessed 21 June 2022.

10 Jon Gambrell and Nicholas Paphitis, "Iran seizes 2 Greek tankers in Persian Gulf as tensions rise," *Canadian Press*, 27 May 2022, https://www.msn.com/en-ca/news/world/iran-seizes--greek-tankers-in-persian-gulf-as-tensions-rise/ar-AAXNPEH?ocid=sapphireappshare, accessed 29 May 2022.

11 Liz Sly, "Iran's role in attack on U.S. troops in Syria signals new escalation," *The Washington Post*, 26 October 2021, https://www.washingtonpost.com/world/iran-militias-tanf-us-forces/2021/10/26/8c75ad98-35c1-11ec-9662-399cfa75efee_story.html, accessed 26 October 2021.

12 Farnaz Fassihi, Ronen Bergman and Eric Schmitt, "Iran's Attack Was Response to Secret Israeli prop Attack on Drone Site," *The New York Times*, 16 March 2022, https://www.nytimes.com/2022/03/16/world/middleeast/iran-israel-attack-drone-site.html, accessed 18 March 2022.

13 Joe Truzman, "Al-Nasser Salah al-Din Brigades Praises IRGC and Hezbollah for Arming Group," *Long War Journal*, 14 November 2021, https://www.longwarjournal.org/archives/2021/11/al-nasser-salah-al-din-brigades-praises-irgc-and-hezbollah-for-arming-group.php, 15 November 2021.

14 Ariane M. Tabatabai, Jeffrey Martini, Becca Wasser, *The Iran Threat Network (ITN) Four Models of Iran's Nonstate Client Partnerships* (Santa Monica, CA: RAND, 2021), 2.

15 See Nakissa Jahanbani and Suznne Weedon Levy, *Iran Entangled. Iran and Hezbollah's Support to Proxies Operating in Syria* (West Point: Combating Terrorism Center, 2022); and Seth Jones, Jared Thompson, Danielle Ngo, Brian McSorley and Joseph

Bermudez, *The Iranian and Houthi War Against Saudi Arabia* (New York: Centre for Strategic & International Studies, 2021), 1, https://www.csis.org/analysis/iranian-and-houthi-war-against-saudi-arabia, accessed 3 June 2022.

16 See Jahanbani and Levy, *Iran Entangled*, 2.

17 Jane Arraf and Eric Schmitt, "Iran's Proxies in Iraq Threaten U.S. With More Sophisticated Weapons," *The New York Times*, 4 June 2021, https://www.nytimes.com/2021/06/04/world/middleeast/iran-drones-iraq.html?utm_source=iterable&utm_medium=email&utm_campaign=2430856_, accessed 8 June 2021; and Jones, "The Future of Competition." The drones Iran is supplying to its proxies are increasingly sophisticated being capable of homing in on their targets with pre-set GPS coordinates. American analysts revealed that the Iranian-sponsored militants are now targeting sites, even specific aircraft hangars, where sophisticated armed drones and contractor-operated turboprop surveillance aircraft are stationed in an attempt to disrupt or cripple the U.S. reconnaissance capability critical to monitoring threats in Iraq. American defences against the drones are less than optimal as the armed drones fly too low to be detected by those defenses. Ibid; and "IntelBrief: U.S.- Iran Proxy War in Iraq Escalates," *The Soufan Center*, 7 July 2021, https://thesoufancenter.org/intelbrief-2021-july-7/, accessed 7 July 2021; and "IntelBrief: Yemen War Expands, Impacting U.S. Forces in the Region," *The Soufan Center*, 9 February 2022, https://thesoufancenter.org/intelbrief-2022-february-9/, accessed 10 February 2022.

18 Thomas Juneau, "How Iran Helped Houthis Expand their Reach," *War on the Rocks*, 23 August 2021, https://warontherocks.com/2021/08/how-iran-helped-houthis-expand-their-reach/, accessed 26 August 2021.

19 Tabatabai et al, *The Iran Threat Network,* 4-5.

20 Isabel Debre, "U.S. seizes dozens of Iran-linked websites accused of 'disinformation'," *Global News*, 22 June 2021, https://globalnews.ca/news/7971628/us-iran-websites/, accessed 24 June 2021.

21 Dr. Paul Stott, *Iranian Influence Networks in the United Kingdom: Audit and Analysis* (London: Centre on Radicalisation & Terrorism, 2021), 1, 8.

22 Emanuele Ottolenghi, "How Iran is Making Inroads in South America," *The Foundation for Defense for Democracies*, 10 March 2022, https://www.fdd.org/analysis/2022/03/10/how-iran-is-making-inroads-in-south-america/, accessed 23 March 2022.

23 Pierre Pahlavi, "Iran's Cyber Influence Strategy Poses Formidable Challenges for the West," *The National Interest*, 9 March 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/iran's-cyber-influence-strategy-poses?page=0%2C1, accessed 12 March 2022.

24 Ibid.

25 Jones, "The Future of Competition." and Jones, *Three Dangerous Men*, 16.

26 Jones, *Three Dangerous Men*, 121.

27 Sean Lyngass, "FBI director blames Iran for 'despicable' attempted cyberattack on Boston Children's Hospital," *CNN*, 1 June 2022, https://www.msn.com/en-ca/news/us/fbi-director-blames-iran-for-despicable-attempted-cyberattack-on-boston-childrens-hospital/ar-AAXYc82?ocid=sapphireappshare, 3 June 2022.

28 Levitt, "Trends in Iranian," 1-11.

29 Reyes Cole, "The Myths of Traditional Warfare: How Our Peer and Near-Peer Adversaries Plan to Fight Using Irregular Warfare," *Small War Journal*, https://smallwarsjournal.com/jrnl/art/myths-traditional-warfare-how-our-peer-and-near-peer-adversaries-plan-fight-using, accessed 2 February 2020. This assessment may be a bit optimistic. NATO numbers main battle tanks in European militaries range between one-tenth and one-fifth of the stock held at the end of the Cold War. One recent RAND study observed that the three largest non-U.S. contributors to NATO—the United Kingdom, France, and Germany—would struggle to field a single armored brigade each. Importantly, they would not be able to field a full brigade for at least a month and sustaining them would be problematic. Moreover, in deploying these forces the countries would have little excess capacity. The report concluded, "without significant improvements in forward posture and deployment capabilities, NATO does not currently present a credible conventional deterrent should Russia choose to attack the Baltics." Clint Reach, Edward Geist, Abby Doll, Joe Cheravitch, *Competing with Russia Militarily* (Santa Monica, CA: RAND, 2021), 11.

30 Eric Schmitt, "Terrorism Threat in West Africa Soars as U.S. Weighs Troop Cuts," *New York Times*, 27 February 2020, https://www.nytimes.com/2020/02/27/world/africa/terrorism-west-africa.html, accessed 27 February 2020.

31 Ben Connable, Stephanie Young, Stephanie Pezard, Andrew Radin, Raphael S. Cohen, Katya Migacheva, James Sladden, *Russia's Hostile Measures* (Santa Monica, CA: RAND, 2020), x, 4.

32 John Taft, Liz Gormisky and Joe Mariani, *Special Operations Forces and Great Power Competition, A Report from the Deloitte Center for Government Insights*, ND, 3, https://www2.deloitte.com/content/dam/insights/us/articles/4980_special-operations-forces/DI_special-operations-forces.pdf, accessed 26 April 2021.

CHAPTER 5

1 Jesse Snider, "Majority of Canadians view China as biggest security threat, with global war of attrition already underway: poll," *National Post*, 10 March 2021, https://a.msn.com/r/2/BB1erjNX?m=en-ca&referrerID=InAppShare, accessed 10 March 2021. A survey of Americans revealed that fifty-two per cent of Americans believe "China is the greatest threat to the United States." Only fourteen per cent state Russia is the greatest threat. Ronn Blitzer, "Majority of Americans see China as top threat, concerned about war breaking out: poll," *Fox News*, 30 November 2021, https://www.msn.com/en-ca/news/politics/majority-of-americans-see-china-as-top-threat-concerned-about-war-breaking-out-poll/ar-AARjGG4?ocid=sapphireappshare, accessed 30 November 2021.

2 Snider, "Majority of Canadians."

3 Madelaine Drohan, ed., *A national security strategy for the 2020s. How Canada can adapt to a deteriorating security environment* (Ottawa: University of Ottawa, 2022), 4.

4 Amanda Connolly, "Canada's defence minister says the world is 'growing darker' and 'more chaotic'," *Global News*, 10 May 2022, https://globalnews.ca/news/8824160/anita-anand-world-growing-darker/, accessed 15 May 2022.

5 Canada, *National Security and Intelligence Committee of Parliamentarians Annual Report 2020* (Ottawa: GoC, 2021), 17.

6 Ibid., 20.

7 Sam Cooper, "China, Russia exploiting high-tech in 'Hybrid Warfare' costs up to $100B per year in Canada: report," *Global News*, 24 June 2021, https://globalnews.ca/news/7975330/china-russia-exploiting-high-tech-hybrid-warfare-cost-billions-canada/, accessed 24 June 2021.

8 John Ivison, "Forget the Cold War, this cyber conflict is hot," *The Chronicle Herald*, 7 April 2021, https:// www.thechronicleherald.ca/opinion/national-perspectives/john-ivison-forget-the-cold-war-this-cyber-conflict-is-hot-572984/, accessed 7 April 2021.

9 Robert Fife and Steven Chase, "New report details Beijing's foreign influence operations in Canada," *Globe & Mail*, 31 May 2021, https://www.theglobeandmail.com/politics/article-new-report-details-beijings-foreign-influence-operations-in-canada/, accessed 1 June 2021.

10 "Senator accused of being China's 'mouthpiece' worries about rise of anti-Asian racism," *Canadian Press*, 3 October 2021, https://www.msn.com/en-ca/news/canada/senator-accused-of-being-chinas-mouthpiece-worries-about-rise-of-antiasian-racism/ar-AAP5tdI?ocid=sapphireappshare, accessed 4 October 2021.

11 Stewart Bell, "Canadian government report accuses China of widespread campaign of espionage, manipulation," *Global News*, 26 January 2022, https://globalnews.ca/news/8537707/SOMNIA/, accessed 27 January 2022.

12 Robert Fife and Steven Chase, "Canada's spy agency warns MPs to beware of influence operations from China," *Globe & Mail*, 11 January 2022, https://www.theglobeandmail.com/politics/article-spy-agency-briefing-mps-to-beware-of-influence-operations-from-china/, accessed 11 January 2022.

13 Terry Glavin, "Terry Glavin: As China aims to manipulate Canadian politics, parliamentarians look the other way," *The National Post*, 22 December 2021, https://www.msn.com/en-ca/news/canada/terry-glavin-as-china-aims-to-manipulate-canadian-politics-parliamentarians-look-the-other-way/ar-AAS3Y7p?ocid=sapphireappshare,accessed 6 January 2022.

14 Tom Blackwell, "Federally funded Canadian group used by China to spread propaganda on Uyghurs: report," *National Post*, 5 July 2022, https://www.msn.com/en-ca/news/canada/federally-funded-canadian-group-used-by-china-to-spread-propaganda-on-uyghurs-report/ar-AAZdJgA?ocid=sapphireappshare, accessed 6 July 2022.

15 Twinkle Ghosh and David Lao, "Here are the key events leading to the release of Meng Wanzhou, 'Two Michaels'," *Global News*, 25 September 2021, https://www.msn.com/en-ca/news/politics/here-are-the-key-events-leading-to-the-release-of-meng-wanzhou-two-michaels/ar-AAONEz5?ocid=sapphireappshare, accessed 2 October 2021.

16 Evan Dyer, "China blocks effort to send canola dispute with Canada to WTO panel," *CBC News*, 30 June 2021, https:// www.msn.com/en-ca/news/canada/china-blocks-effort-to-send-canola-dispute-with-canada-to-wto-panel/ar-AALATLS, accessed 2 July 2021.

17 Tom Blackwell, "'Ill-considered' vaccine deal quashed by China cost Canadian taxpayers $250,000 for aborted study," *National Post*, 21 December 2021, https://www.msn.com/en-ca/news/canada/illconsidered-vaccine-deal-quashed-by-china-cost-canadian-taxpayers--for-aborted-study/ar-AAS1IFX?ocid=sapphireappshare, accessed 27 December 2021.

18 Canada, *National Cyber Threat Assessment 2020* (Ottawa: Canadian Centre for Cyber Security, 2021), https://cyber.gc.ca/en/guidance/executive-summary-2, accessed 21 January 2022.

19 Christopher Nardi, "Canada the target of 'thousands' of cyberattacks every day, CSIS reveals," *National Post*, 28 March 2022, https://nationalpost.com/news/politics/canada-the-target-of-thousands-of-cyber-attacks-every-day-csis-reveals, accessed 29 March 2022. For example, DND confirmed that CMC Electronics, a Montreal-based aerospace company, was hit with a "cyber breach related incident" at their company. The firm conducts aerospace engineering and research and development for DND. In addition, Global Affairs Canada suffered a multi-day network disruption due to a cyber-attack. Alex Boutilier and Mercedes Stepenson, "Global Affairs Canada suffers 'cyber attack' amid Russia-Ukraine tensions: sources," *Global News*, 24 January 2022, https://globalnews.ca/news/8533835/global-affairs-hit-with-significant-multi-day-disruption-to-it-networks-sources/, accessed 24 January 2022; and Alex Boutilier and Sam Cooper, "National Defence looking at potential 'impacts' after cyberattack on military contractor," *Global News*, 9 June 2022, https://globalnews.ca/news/8906423/national-defence-potential-impacts-cyberattack-military-contractor/, accessed 10 June 2022.

20 Yadullah Hussain, "Can Canada fend off a Colonial Pipeline-like cyberattack? *Financial Post*, 19 May 2021, https://financialpost.com/commodities/energy/oil-gas/can-canada-fend-off-a-colonial-pipeline-like-cyberattack, accessed 20 May 2021.

21 Snider, "Majority of Canadians."

22 Jesse Snyder, "CSE responded to more than 2,200 cyber attacks last year amid heightened concern over Chinese, Russian hacks," *National Post*, 28 June 2021, https://nationalpost.com/news/federal-spy-agency-responded-to-more-than-2200-cyber-attacks-last-year-amid-heightened-concern-over-chinese-russian-hacks, accessed 29 June 2021.

23 Ibid.

24 Canada, *National Security and Intelligence Committee of Parliamentarians Annual Report 2020*, 24-26.

25 Cooper, "China, Russia exploiting."

26 Government of Canada, "Policy Statement – Securing Canada's Telecommunications System," 19 May 2022, https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html, accessed 20 May 2022; and Jones, "The Future of Competition."

27 Cooper, "China, Russia exploiting."

28 Catharine Tunney, "Spy agency warned Trudeau China's media tactics becoming more 'sophisticated ... insidious'," *CBC News*, 7 December 2021, https://www.cbc.ca/news/politics/csis-trudeau-china-media-1.6270750, accessed 7 December 2021.

29 Tom Blackwell, "Chinese diplomat, party newspaper post cartoon of Trudeau on indigenous skulls, escalating campaign," *National Post*, 8 July 2021, https://a.msn.com/r/2/AALUQqT?m=en-ca&referrerID=InAppShare, accessed 16 July 2021.

30 Nicole Bogart, "Cognitive warfare: Why disinformation is Russia's weapon of choice in the war on Ukraine," *CTV News*, 25 February 2022, https://www.ctvnews.ca/world/cognitive-warfare-why-disinformation-is-russia-s-weapon-of-choice-in-the-war-on-ukraine-1.5797222, accessed 28 March 2022.

31 Marie Woolf, "Calgary study finds Canada has been targeted with Russian disinformation with tweets linked to foreign powers," *Global News*, 8 June 2022, https://globalnews.ca/news/8907166/university-calgary-twitter-disinformation-study/, accessed 10 June 2022.

32 Cooper, "China, Russia exploiting high-tech."

33 Tom Blackwell, "Chinese government agency that works with Canadians involved in espionage, Federal Court affirms," *The National Post*, 23 February 2022, https://www.msn.com/en-ca/news/canada/chinese-government-agency-that-works-with-canadians-is-involved-in-espionage-federal-court-affirms/ar-AAUcnyL?ocid=sapphireappshare, accessed 24 February 2022.

34 Blackwell, "Chinese government agency."

35 Karen Pauls, "'Wake-up call for Canada': Security experts say case of 2 fired scientists could point to espionage," *CBC News*, 10 June 2021, https://www.cbc.ca/news/canada/manitoba/wake-up-call-for-canada-security-experts-say-case-of-2-fired-scientists-cou, accessed 10 June 2021.

36 Catharine Tunney and Nick Boisvert, "CSIS warned space agency about ex-engineer now facing charges: court documents," *CBC News*, 13 March 2022, https://www.msn.com/en-ca/news/canada/csis-warned-space-agency-about-exengineer-now-facing-charges-court-documents/ar-AAUZTL9?ocid=sapphireappshare, 13 March 2022. Zheng was also accused of using his status as an engineer at the CSA to negotiate satellite station installation agreements with Iceland on behalf of a Chinese aerospace. Catharine Tunney, "Ottawa seeks to hide 'sensitive' details of foreign interference case from public view," *CBC News*, 5 March 2022, https://www.msn.com/en-ca/news/canada/ottawa-seeks-to-hide-sensitive-details-of-foreign-interference-case-from-public-view/ar-AAUDPny?ocid=sapphireappshare, accessed 6 March 2022; and "Charge against

a former Canada Space Agency employee," *RCMP News Release*, 8 December 2021, https://www.rcmp-grc.gc.ca/en/news/2021/charges-a-canada-space-agency-employee/re, accessed 9 December 2021.

37 Anthony Furey, "How Communist China drives drugs, violence and inflated housing prices in Canada: Full Comment with Anthony Furey," *National Post*, 29 June 2021, https://www.msn.com/en-ca/news/canada/how-communist-china-drives-drugs-violence-and-inflated-housing-prices-in-canada-full-comment-with-anthony-furey/ar-AALAkNy, accessed 2 July 2021.

38 Ibid.

39 Karen Pauls, "'Wake-up call for Canada': Security experts say case of 2 fired scientists could point to espionage," *CBC News*, 10 June 2021, https://www.cbc.ca/news/canada/manitoba/wake-up-call-for-canada-security-experts-say-case-of-2-fired-scientists-cou, accessed 10 June 2021.

40 Cooper, "China, Russia exploiting."

CHAPTER 6

1 Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (New York: Everyman's Library, Alfred A. Knopf, 1993), 731.

2 Robert Coalson, "The Value of Science is in the Foresight," *Military Review*, January-February 2016, 29.

3 Cited in Jones, *Three Dangerous Men*, 190. A conventional war is defined as "a form of warfare between states that employ direct military confrontation to defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize or retain territory in order to force a change in an adversary's government or policies. The focus of conventional military operations is normally an adversary's armed forces with the objective of influencing the adversary's government. It generally assumes that the indigenous populations within the operational area are non-belligerents and will accept whatever political outcome the belligerent governments impose, arbitrate, or negotiate. A fundamental military objective in conventional military operations is to minimize civilian interference in those operations." U.S. Department of Defense: The Irregular Warfare Joint Operating Concept (IW JOC), Version 1.0, dated 11 September 2007.

4 David Oakley, "The Problems of a Militarized Foreign Policy for America's Premier Intelligence Agency," *War on the Rocks*, 2 May 2019, https://warontherocks.com/2019/05/the-problems-of-a-militarized-foreign-policy-for-americas-premier-intelligence-agency/, 2 May 2019.

5 Although the NATO parliamentary committee continually warns of the lack of ground troops in Eastern Europe to repel a Russian invasion, analysts insist, "While the conventional view is one of Russian advantage, the new figures show that the United States and its European partners far outstrip Moscow." William M. Arkin, "Exclusive: While the Press and Public Focus on Iran, US Military Prepares for the War with Russia," *Newsweek*, 31 January 2020, https://www.newsweek.com/exclusive-cold-war-back-focus-iran-military-prepares-war-russia-1485088, accessed 6 February 2020.

6 Murray Brewster, "NATO tests its ability to reinforce Europe in a crisis with massive trans-Atlantic operation," *CBC News*, 31 May 2021, https://www.cbc.ca/news/politics/nato-atlantic-exercise-1.6047355, accessed 10 June 2021.

7 Alex Marquardt and Jeremy Harlan, "NATO exercises sweep Europe amid Russian escalation, rising tensions between Moscow and US," *CNN*, 12 May 2021, https://www.msn.com/en-ca/news/world/nato-exercises-sweep-europe-amid-russian-escalation-rising-tensions-between-moscow-and-us/ar-BB1gCEOq?fullscreen=true#image=1, accessed 12 May 2021.

8 Cited in Jones, *Three Dangerous Men,* 7.

9 Cited in Ibid., 5.

10 Cited in Ibid., 11.

11 Cited in Ibid., 11.

12 Taft et al, *Special Operations Forces*, 3.

13 Kimberly Kagan, "Military Learning and the Future of War," *Institute for the Study of War*, 16 September 2020. Http://www.understandingwar.org/backgrounder/military-learning-and-future-war, accessed 17 June 2021.

14 Cited in Christina M. Knopf and Eric J. Ziegelmayer, "Fourth Generation Warfare and the US Military's Social Media Strategy Promoting the Academic Conversation," *ASPJ-Africa and Francophonie*, Vol. 3, No. 4, 2012, 3.

15 General Valery Gerasimov, Chief of the General Staff of the Russian Federation, "The Value of Science in Prediction," in "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows. Analysis and Assessment of Russian Crime and Security,* https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/, accessed 6 February 2015.

16 András Rácz, Russia's *Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*. The Finnish Institute of International Affairs, FIIA Report 43, 41. The Americans use a term called "Gray Zone Conflict" to describe Hybrid Warfare. Gray Zone Conflict is defined "as competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality. They are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks." USSOCOM White Paper, *The Gray Zone*, 9 September 2015, 1.

17 United Kingdom, *Strategic Trends Programme. Future Character of Conflict* (London: Ministry of Defence, ND), 2.

18 Seth Jones, "The Future of Warfare is Irregular," *The National Interest*, 26 August 2018, https://nationalinterest.org/feature/future-warfare-irregular-29672, accessed 22 March 2022.

19 Wesley Wark and Aaron Shull, "National security threats are changing, but Canada is mired in conventional thinking," *CBC News*, 30 April 2021, https://www.cbc.ca/news/opinion/opinion-national-security-1.6003674, accessed 30 April 2021.

20 Special Warfare (SW) is defined as "the execution of activities that involve a combination of lethal and non-lethal actions taken by specially trained and educated forces that have a deep understanding of cultures and foreign language, proficiency in small-unit tactics, subversion, sabotage and the ability to build and fight alongside indigenous combat formations in a permissive, uncertain or hostile environment." Its activities range from influence operations and political action to economic sanctions and diplomacy. SW can improve a government's contextual understanding of potential partners and the situation on the ground before it commits to a course of action.

SW strategic advantages:

1. Improved understanding and shaping of the environment;
2. Cost Effective / cost imposing strategy – small footprint for you; opponent needs to spend disproportionate amounts of money;
3. Managed escalation and credibility risk – make no promises of larger commitments;
4. Sustainable solutions – sustainable two parts – fiscal and political.

SW Limits and Risks

1. Divergent partner objectives;
2. Ineffective partner capability;
3. Unacceptable partner behaviour;
4. Policy Fratricide; and
5. Disclosure.

Dan Madden, Dick Hoffman, Michael Johnson, Fred Krawchuk, John Peters, Linda Robinson, Abby Doll, "Special Warfare. The Missing Middle in US Coercive Options," RAND Research Report, 2014, 3.

21 National Intelligence Council, *Global Trends 2040* (Washington D.C.: NIC, March 2021), 9.

22 Ibid., 90. See also Layne, "Coming Storms."

23 Sayler, *Emerging Military Technologies*, 1.

24 HM Government, *Global Britain in a Competitive Age* (London: HM Stationary Office, 2021), 29. The report asserted, "The tech 'superpowers' are investing to maintain their lead. At the same time, many more countries are now able to compete in S&T, while large technology companies are able to grow more powerful by absorbing innovations produced by small companies. Competition is therefore intensifying, shaped in particular by multinational firms with the backing of states, some of which take a 'whole-of-economy' approach to ensure dominance in critical areas. Maintaining a competitive edge will rely on pre-eminence in and access to technology – as well as access to the human and natural resources needed to harness it – and the ability to protect intellectual property."

25 Thomas O. Falk, "How drones have added a new dynamic to conflicts. Drones have become the means of the first choice in modern warfare and are used by state and non-state actors," *Al Jazeera*, 20 February 2021, https://www.aljazeera.com/news/2021/2/20/how-drones-have-added-a-new-dynamic-to-conflicts, accessed 23 February 2021. In 2019, the

UAV market was worth $10.53bn. By 2024, the market is forecast to reach $43bn. Karen Allen, "Drones and Violent Nonstate Actors in Africa," *Africa Center for Strategic Studies*, 6 August 2021, https://africacenter.org/spotlight/drones-and-violent-nonstate-actors-in-africa/, accessed 9 August 2021.

26 Robyn Dixon, "Azerbaijan's drones owned the battlefield in Nagorno-Karabakh — and showed future of warfare," *The Washington Post*, 11 November 2020, https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html, accessed 12 November 2020.

27 Cited in Dixon, "Azerbaijan's drones owned."

28 "IntelBrief: Welcome to the "New Normal": Non-State Actors and the Use of Drones," *The Soufan Center*, 3 June 2021, https://thesoufancenter.org/intelbrief-2021-june-3/, accessed 3 June 2021; and Joby Warrick, Souad Mekhennet and Louisa Loveluck, "In militants' hands, drones emerge as a deadly new wild card in the Middle East," *The Washington Post*, 7 December 2021, https://www.washingtonpost.com/national-security/iran-drones-iraq-militias/2021/12/06/5685e772-5469-11ec-8769-2f4ecdf7a2ad_story.html, accessed 9 December 2021.

29 "Shadowy Drone Program Gives Yemen Rebels Regional Reach," *The Defense Post*, 26 March 2021, https://www.thedefensepost.com/2021/03/26/yemen-houthis-drone-program/, accessed 26 March 2021. In 2019, Iranian drones attacked two massive Saudi oil refineries, which resulted in knocking out five percent of global oil supply overnight. This damage caused the biggest sudden disruption in history. Tom Donilon, "The Drone Threat Comes Home," *Foreign Affairs*, 28 January 2022, https://www.foreignaffairs.com/articles/world/2022-01-28/drone-threat-comes-home, accessed 28 January 2022.

30 The most advanced Houthi drone is the Samad-3 which can be fitted with 18 kg of explosives and has a range of 1,500 kilometers (930 miles) and a top speed of 250 km/hour, according to rebel media sources and analysts. Each drone costs the Houthis just a few hundred dollars. "Shadowy Drone Program Gives Yemen Rebels Regional Reach"; and Tom Donilon, "The Drone Threat Comes Home," *Foreign Affairs*, 28 January 2022, https://www.foreignaffairs.com/articles/world/2022-01-28/drone-threat-comes-home, accessed 28 January 2022.

31 Donilon, "The Drone Threat."

32 "Drones evolving into terrorists' 'weapon of choice' in the region, experts warn," *The Arab Weekly*, 21 February 2022, https://thearabweekly.com/drones-evolving-terrorists-weapon-choice-region-experts-warn, accessed 22 February 2022. Major General Sean A Gainey, the U.S. Army director of the Joint Counter-Small Unmanned Aircraft Systems Office stated, "They're rapidly purchasing this stuff off the shelf, redesign it, taking the great technology that's being developed for good, and then employing it for other purposes."

33 Louisa Loveluck and John Hudson, "Iran-backed militias turn to drone attacks, alarming U.S. forces in Iraq," 29 May 2021, *The Washington Post*, https://www.washingtonpost.com/world/iran-militias-tanf-us-forces/2021/10/26/8c75ad98-35c1-11ec-9662-399cfa75efee_story.html, accessed 31 May 2021.

34 Donilon, "The Drone Threat."

35 "IntelBrief: Welcome to the "New Normal": Non-State Actors and the Use of Drones," *The Soufan Center*, 3 June 2021, https://thesoufancenter.org/intelbrief-2021-june-3/, accessed 3 June 2021.

36 Zachary Kallenborn, "Swarms of Mass Destruction, The case for declaring armed and fully autonomous drone swarms as WMD," *Modern War Institute at West Point*, 28 May 2020, https://mwi.usma.edu/swarms-mass-destruction-case-declaring-armed-fully-autonomous-drone-swarms-wmd/, accessed 3 June 2022.

37 Kilcullen, *The Dragons and the Snakes*, 81; and Jonathan Marcus, "Combat drones: We are in a new era of warfare – here's why," *BBC News*, 5 January 2022, https://www.bbc.com/news/world-60047328, accessed 7 January 2022.

38 The Turkish use of drone swarms to engage Syrian bases and chemical weapon depots in March 2020, as well as the South Korean demonstration of 1,218 autonomous drones equipped with lights collaborating to form intricate images in the night sky over Pyeongchang during the opening ceremonies of the 2018 Olympics provide a preview of what drone swarms are capable of achieving. See Seclan Hacaoglu, "Turkey's Killer Drone Swarm Poses Syria Air Challenge to Putin," *Bloomberg*, 1 March 2020, https://www.bloomberg.com/news/articles/2020-03-01/turkey-s-killer-drone-swarm-poses-syria-air-challenge-to-putin, accessed 2 March 2020; and Brose, "The New Revolution."

39 For example, Ukraine's UAV capability allows them to fly drones to a range of up to three hundred kilometers, last up to twenty-seven hours, and they can carry up to four laser-guided munitions. However, the Russians also used drones as artillery spotters and were able to cause extensive casualties on Ukrainian troops that they were far enough behind the front lines to be safe. Lauren A. Kahn, "How Ukraine Is Using Drones Against Russia," *Council on Foreign Relations*, 2 March 2022, https:// www.cfr.org/in-brief/how-ukraine-using-drones-against-russia, accessed 13 March 2022; and Jeff Schogol, "A shadowy drone force keeps attacking US troops in Iraq have already come under attack by drones three times so far this year," *Task & Purpose*, 10 January 2022, https://askandpurpose.com/news/drones-attack-us-troops-iraq-syria/, accessed 11 January 2022.

40 For example, compare the cost difference between a UAV ($6,000 Switchblade drone) that can destroy a tank (approximately $6 million), or a Neptune missile ($2 million) that can destroy a ship (a U.S. Ford-class aircraft carrier costs $13 billion). Elliot Ackerman, "A Whole Age of Warfare Sank With the Moskva," *The Atlantic*, 22 May 2022, https://www.theatlantic.com/ideas/archive/2022/05/ukraine-russia-moskva-military-marine-corps/629930/, 25 May 2022.

41 Many analysts believe the Russian leadership anticipated a bloodless coup, much like they experienced in 2014.

42 TRADOC, *The U.S. Army in Multi-Domain*,vii.

43 Ominously, as one Western analyst noted, "The type of self-protection missile defence systems that our frigates – or even our new warships being built – have aren't really designed to defend themselves against the flight pattern of a hypersonic missile."

Steven Chase, "Canada's top soldier says the West faces being outmatched in military defence by China," *Reuters*, 19 April 2021. Https://www.theglobeandmail.com/politics/article-canadas-top-soldier-says-the-west-faces-being-outmatched-in-military/, accessed 20 April 2021.

44 Ellen Mitchell, "Outcry grows over Russian missile test that hit satellite," *The Hill*, 17 November 2021. Https://www.msn.com/en-ca/news/politics/outcry-grows-over-russian-missile-test-that-hit-satellite/ar-AAQO4K0?ocid=sapphireappshare, accessed 18 November 2021; and David Sharp, "Ukraine war is backdrop in US push for hypersonic weapons," *Canadian Press*, 20 March 2020, https://www.msn.com/en-ca/news/science/ukraine-war-is-backdrop-in-us-push-for-hypersonic-weapons/ar-AAVhDWW?ocid=msedgntp, accessed 20 March 2021.

45 David Martin, "Top military official discloses new details about China's hypersonic test," *CBS News*, 17 November 2021, https://www.msn.com/en-ca/news/world/top-military-official-discloses-new-details-about-chinas-hypersonic-test/ar-AAQMQoG?ocid=sapphireappshare, accessed 18 November 2021; and *Associated Press*, "China's hypersonic missile test 'close to Sputnik moment', says US general Gen Mark Milley says reports about breakthrough missile have 'all our attention', and says US working on same weapons," *The Guardian*, 28 October 2021, https://www.theguardian.com/us-news/2021/oct/28/chinas-hypersonic-missile-test-close-to-sputnik-moment-says-us-general, accessed 28 October 2021.

46 Martin, "Top military official"; and Teresa Chen, Alana Nance, Han-ah Sumner, "Water Wars: AUKUS Goes Hypersonic," *Lawfare*, 22 April 2022, https://www.lawfareblog.com/water-wars-aukus-goes-hypersonic, accessed 4 May 2022.

47 "China could have 1,000 nuclear warheads by 2030: Pentagon," *ABC News*, 4 November 2021, https://www.msn.com/en-ca/news/world/china-could-have--nuclear-warheads-by--pentagon/ar-AAQi6WE?ocid=sapphireappshare, accessed 4 November 2021.

48 Relatedly, in January 2022, the Air Force Research Laboratory through its Vanguard Program awarded a contract worth $102 million to Space X to create a "point-to-point rocket cargo delivery system." The intent is to rapidly deploy cargo and personnel through space to support contingency operations thereby disrupting the decision-cycle of an adversary. The potential capability "to land a Starship in an austere environment, the challenge of targeting a rocket reentry from space, an expendable payload, and the ability to deploy numerous other capabilities from the cargo bay of a rocket are all factors that allow rocket cargo delivery to revolutionize the nature of warfare. Gabe Arrington and Justin W. Chandler, "How space is changing the nature of war," *The Hill*, 8 February 2022, https://www.msn.com/en-ca/news/politics/how-space-is-changing-the-nature-of-war/ar-AATCYH3?ocid=sapphireappshare, accessed 9 February 2022.

49 Reach et al, *Competing with Russia Militarily*, 15.

50 Dmitri Litovkin, "Russia begins mass production of the Zircon hypersonic missile," *Russia Beyond*, 15 December 2021, https://www.rbth.com/science-and-tech/334520-russia-begins-mass-production-of-hypersonic-missiles?fbclid=IwAR3pK9bI-hzrLvtw2iqTOS2G9WT47mkcSuV6Dem-hGb2sZUQZV2Nb_zlYqY, accessed 23 December 2021.

51 Reach et al, *Competing with Russia*, 15, 21.

52 Layne, "Coming Storms."

53 Ibid.

54 Alex Vershinin, "The Challenge of Dis-Integrating A2/AD Zone," *JFQ 97*, 2020, 14.

55 Brose, "The New Revolution."

56 Directed Energy Weapons is an "umbrella term covering technologies that produce a beam of concentrated electromagnetic energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to disable, damage or destroy adversary equipment, facilities, and personnel." Henry Obering, III, "Directed Energy Weapons Are Real …And Disruptive," *PRISM*, Vol. 8, No. 3, 37. See also, Prakash Nanda "Face-Off: China's Development of Powerful Directed Energy Weapons (DEWs) Triggers A Global 'Laser War'?" *The Eurasian Times*, 23 November 2021, https://eurasiantimes.com/face-off-chinas-development-of-powerful-directed-energy-weapons-dews-triggers-a-global-laser-war/undefined, accessed 22 November 2021; and Abhishek De, "Explained: India has dismissed as 'fake' a report about China's use of 'microwave' weapons," *The Indian Express*, 26 November 2020, https://indianexpress.com/article/explained/microwave-weapons-india-china-7056441/, accessed 22 November 2021.

57 Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations, Joint Publication 3-85*, May 22, 2020, GL-6. See also Alfred Cannin, "Directed-Energy Weapons," *Air & Space Power Journal*, Vol. 35, Issue 3, Fall 2021, 57-65.

58 "China used 'microwave' pulse weapon to force Indian soldiers off Himalayan hilltops: report," *National Post*, 17 November 2020, https://www.msn.com/en-ca/news/world/china-used-microwave-pulse-weapon-to-force-indian-soldiers-off-himalayan-hilltops-report/ar-BB1b5QtW?ocid=msedgdhp, accessed 17 November 2020.

59 Sayler, *Emerging Military Technologies*, 1.

60 Richard Uber, Penetrating Artificial Intelligence enhanced Anti Access / Area Denial," *Journal of Indo-Pacific Affairs*, Winter 2020, 60; and Kareem Fahim, "Turkey's military campaign beyond its borders is powered by homemade armed drones," *The Washington Post*, 29 November 2020, https://www.washingtonpost.com/world/middle_east/turkey-drones-libya-nagorno-karabakh/2020/11/29/d8c98b96-29de-11eb-9c21-3cc501d0981f_story.html, accessed 30 November 2020.

61 Gerrit De Vynck, "The U.S. says humans will always be in control of AI weapons. But the age of autonomous war is already here," *The Washington Post*, 7 July 2021, https://www.washingtonpost.com/technology/2021/07/07/ai-weapons-us-military/, accessed 8 July 2021.

62 Richard Shimooka, "It's an increasingly unstable world out there. Canada's military should be prepared," *National Post*, 23 October 2020, https://www.bnnbloomberg.ca/elite-taliban-unit-ambush-afghan-forces-killing-34-during-talks-1.1511011, accessed 21 October 2020.

63 Joe Hernandez, "A Military Drone With A Mind Of Its Own Was Used In Combat, U.N. Says," *npr*, 1 June 2021, https://www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d, accessed 3 June 2021.

64 Raymond McConoly, "Russian Navy Ships Get More Powerful with Kamikaze drones," *Naval Post*, 30 October 2021, https://navalpost.com/russian-navy-kamikaze-drones/?fbclid=IwAR3MBQilWkpfao4VvgHBecPMuMxanYNA-_Pnvm478n-DiIqT2lDuc-6LWqo, accessed 2 November 2021.

65 Richard Walker, "Germany warns: AI arms race already underway," *DW*, 7 June 2021, https://www.dw.com/en/artificial-intelligence-cyber-warfare-drones-future/a-57769444, accessed 10 June 2021.

66 For example, China has already developed a motor-powered exoskeleton that can carry ammunition boxes weighing 50 kg. The light-weight exoskeleton suit, known as the portable ammunition support assist system for individual soldiers, can provide 20 kg of assisted strength to its user, relieve more than 50 percent of the burden and greatly reduce risks of waist injury. It takes less than 40 seconds to put on the suit and take it off. The suit's motor gives a reacting force to its user every time the user gets up after bending over, so the user can get up faster with less effort. Optional hooks can be used when carrying ammunition boxes, and they can not only help the user with a better grasp, but also give assisted strength. With the help of the exoskeleton suit, one person can carry ammunition boxes weighing 50 kg without much effort, and two people can carry more than 75 kg with ease. "Powered Exoskeleton to Help Chinese Soldiers Carry 50 kg Ammunition," *DefenseWorld.net*, 13 January 2021, https://www.defenseworld.net/news/28751/Powered_Exoskeleton_to_Help_Chinese_Soldiers_Carry_50_kg_Ammunition#.YACNVzmSmUm, accessed 14 January 2021.

67 Dr. Shannon Houck, Colonel John Crisafulli, Lieutenant Colonel Joshua Gramm, Major Brian Branagan, "Changing Hearts and Brains: SOF Must Prepare Now for Neurowarfare," *The Small Wars Journal*, 12 December 2021, https://smallwarsjournal.com/jrnl/art/changing-hearts-and-brains-sof-must-prepare-now-neurowarfare, accessed 13 December 2021.

68 Ibid.

69 Ibid.

70 Reach et al, *Competing with Russia*, 2.

71 Al Boyer and Cole Livieratos, "The Paradoxical Trinity Of Leadership," *Modern War Institute*, 13 June 2022, https://mwi.usma.edu/the-paradoxical-trinity-of-leadership/, accessed 14 June 2022.

72 Chris Dougherty, *More than Half the Battle. Information and Command in a New American Way of War* (Washington D.C.: Centre for a New American Security, 2021), 1.

73 Espen Berg-Knutsen, "From Tactical Champions to Grand Strategy Enablers: The Future of Small-Nation SOF in Counter-Hybrid Warfare," *Combatting Terrorism Exchange*, Vol. 6, No. 4, November 2016, 62.

74 Ibid., 65.

75 This opportunity is not to discount the potential legal issues and necessary authorities required in many instances to access and interfere with the respective platforms and streaming services. In addition, terrorist organizations such as ISIS / Daesh conduct most of their C2 activities in "closed" chat apps and through gaming networks, although platforms such as Twitter are also being used.

76 Anna Reynolds, ed., *Social Media as a Tool of Hybrid Warfare* (Riga: NATO Strategic Communications Centre of Excellence, 2016), 13-17.

77 Alex Hern, "Fitness tracking app Strava gives away location of secret US army bases," *The Guardian*, 28 January 2018. Https:// www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases, accessed, 10 April 2022; and Liz Sly, "U.S. Soldiers are revealing sensitive and dangerous information by jogging," *TheWashington Post*, 29 January 2018, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-baseswww.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html, accessed 10 April 2022.

78 Jeremy Hsu, "The Strava Heat Map and the End of Secrets," *Wired*, 29 January 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/, accessed 10 April 2022. The difficulty in concealing movement and communications will require education, training and TTPs that allow for "hiding in electronic plain sight," namely the ability to hide within gigantic volumes of electronic traffic and adopting low-profile behaviours to avoid attracting attention. Additionally, it will require "hugging," the ability to get close to protected populations or sites or to piggyback onto systems that opponents cannot disable without harming themselves (e.g., GPS, Google Earth, smartphones).

79 https://www.google.ca/search?q=artificial+intelligence+definition&source=hp&ei=gSNTYvbgGdG2tAa9krG4Dg&iflsig=AHkkrS4AAAAAYlMxkRNplzxRjj_hMYd1oWwpScW4WO9g&oq=Artificial+intelligence+&gs_lcp=Cgdnd3Mtd2l6EAEYADIHCAAQsQMQQzIECAAQQzIICC4QgAQQsQMyBQgAEIAEMgUIABCABDIICC4QgAQQ1AIyBQgAEIAEMgUIABCABDIFCAAQgAQyCAgAEIAEEMkDOgUIABCRAjoQCC4QsQMQgwEQxwEQ0QMQQzoHCC4Q1AIQQzoLCAAQgAQQsQMQgwE6DggAEIAEELEDEMcBENEDOgQILhBDOgUILhCRAjoRCC4QgAQQsQMQgwEQxwEQowI6CAgAEIAEELEDOggIABCxAxCDAToNCC4QgAQQxwEQowIQCjoLCC4QgAQQxwEQrwE6EwgAELEDEIMBELEDELEDELEDELEDEAo6CggAELEDEIMBEAo6CggAELEDEIMBEENQAFihJWC6NGgAcAB4AIABtAGIAcwQkgEEMTguNpgBAKABAQ&sclient=gws-wiz, accessed 10 April 2022.

80 USSOCOM, *JSOU Quick Look*. *Artificial Intelligence Factsheet* (Tampa, FL: JSOU, 20221), 1, https://jsou.libguides.com/ld.php?content_id=61173595, accessed 10 April 2021. Subfields such as machine learning (ML), machine vision (MV) and speech-to-text are all ways in which AI can be applied. According to existing research, AI is typically grouped into the following three categories:

1. Artificial Narrow Intelligence (ANI): AI that can execute one particular decision type, such as capably play chess. ANI is also described as Weak AI;
2. Artificial General Intelligence (AGI): AI that can execute multiple functions, such as capably play both chess and checkers. AGI is also known as Strong AI; and
3. Artificial Super Intelligence (ASI): AI that surpasses human intelligence, such as discovers unexplainable ways to play both chess and checkers. ASI is also categorized as Strong AI.

81 Skyler Stokes, "The AI Revolution and Its Implications on Domestic Counterterrorism," *Middlebury Institute of International Studies Center on Terrorism, Extremism, and Counterterrorism Publications*, 27 Jul 2021, https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/ai-revolution-and-its-implications-domestic, accessed 3 August 2021.

82 Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima and Derek Grossman, *Military Applications of Artificial Intelligence* (Santa Monica, CA: RAND, 2020), xiii.

83 Eric Schmidt, Chair, *Final Report* (Washington D.C.: National Security Commission on Artificial Intelligence, 2021), 7, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf, accessed 11 April 2022.

84 Cited in Morgan et al, *Military Applications of Artificial Intelligence*, 8.

85 Harry Lye, "Cyberwarriors as important as pilots, special forces: UKStratCom head," *Army Technology*, 27 May 2021, https://www.army-technology.com/news/cyberwarriors-as-important-as-pilots-special-forces-ukstratcom-head/, accessed 28 May 2021.

86 Ibid.

87 TRADOC, *The U.S. Army in Multi-Domain,* i.

88 Morgan et al, *Military Applications of Artificial Intelligence*, 16-21; and Zachary Davis, "Artificial Intelligence on the Battlefield," *PRISM*, Vol. 8, No. 2, 118-121. The authors of the RAND study emphasize that "Autonomous weapons, or those capable of identifying and destroying targets without human operators in the decision cycle, raise fundamental questions about moral responsibility, the protection of human dignity, and whom to hold accountable for harmful action if the wrong targets are attacked. Forrest et al, *Military Applications of Artificial Intelligence,* xiii-xiv. See also Sayler, *Emerging Military Technologies*, 2; and Elsa B. Kania, Testimony before the U.S.-China Economic and Security Review Commission: Chinese Advances in Unmanned Systems and the Military Applications of Artificial Intelligence—the PLA's Trajectory towards Unmanned, "Intelligentized" Warfare," *The long term strategy group,* 23 February 2017, https://www.uscc.gov/sites/default/files/Kania_Testimony.pdf#:~:text=In%20addition%2C%20recent%20breakthroughs%20in%20swarm%20intelligence%20%28%E9%9B%86,applications%20of%20artificial%20intelligence.%20Looking%20forward%2C%20PLA%20strategists, accessed 2 June 2022.

89 Brandon et al, "Fight Tonight Reenergizing," 84.

90 Dr. Shannon Houck, Colonel John Crisafulli, Lieutenant Colonel Joshua Gramm, Major Brian Branagan, "Changing Hearts and Brains: SOF Must Prepare Now for Neurowarfare," *The Small Wars Journal*, 12 December 2021, https://smallwarsjournal.com/jrnl/art/changing-hearts-and-brains-sof-must-prepare-now-neurowarfare, accessed 13 December 2021.

91 Ibid. According to a 2020 RAND report, "In general, BCI could theoretically be applied to help future warfighters make more informed decisions within a shorter timetable or to more effectively engage with more robotic systems than their current counterparts." Ibid.

92 RAND Corporation, "Cyber Warfare," Blog page, https://www.rand.org/topics/cyber-warfare.html, accessed 11 April 2022.

93 Harry Lye, "Cyberwarriors as important as pilots, special forces: UKStratCom head," *Army Technology*, 27 May 2021, https://www.army-technology.com/news/cyberwarriors-as-important-as-pilots-special-forces-ukstratcom-head/, accessed 28 May 2021.

94 Ralph D. Thiele, "Hybrid Threats – And How to Counter Them," *ISPSW Strategy Series: Focus on Defense and International Security*, Issue No. 448, September 2016, https://www.ispsw.com/wp-content/uploads/2016/09/448_Thiele_Oslo.pdf, accessed 10 March 2021.

95 Chris Dougherty, *More than Half the Battle. Information and Command in a New American Way of War* (Washington D.C.: Centre for a New American Security, 2021), 14.

96 Ibid.,19.

97 Tom O'Connor, "Russia Is Building an Army of Robot Weapons, and China's AI Tech Is Helping," *Newsweek*, 24 May 2021, https://www.newsweek.com/russia-building-army-robot-weapons-chinas-ai-tech-helping-1594362, accessed 25 May 2021.

98 Dougherty, *More than Half,* 19.

99 Guttieri, "Accelerate Change or Lose," 97.

100 Dougherty, *More than Half,* 1.

101 Ibid., 1.

102 Ransomware attacks have targeted banking, utilities, hospitals, universities and commercial organizations. As a result, the U.S. Department of Justice is elevating investigations of ransomware attacks to a similar priority as terrorism in the wake of the Colonial Pipeline hack and mounting damage caused by cyber criminals. See Christopher Bing, "Exclusive: U.S. to give ransomware hacks similar priority as terrorism," *Reuters*, 3 June 2021, https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/, accessed 10 June 2021. Veronica Stracqualursi, Geneva Sands and Arlette Saenz, "Colonial pipeline: Cyberattack forces major US fuel pipeline to shut down," *CNN*, 8 May 2021, https://a.msn.com/r/2/BB1gvmnp?m=en-ca&referrerID=InAppShare, accessed 9 May 2021; and Josh

Margolin, Molly Nagle and Luke Barr, "Ransomware cyberattack shuts down major US pipeline, company says," *ABC News*, 9 May 2021, https://a.msn.com/r/2/BB1gvx5s?m=en-ca&referrerID=InAppShare, accessed 9 May 2021.

103 Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Quantic Thurston, *Effective Influence Operations* (Santa Monica, CA: RAND, 2009), xii, 2.

104 Ibid., 3-4. The researchers explained that the term influence operations was used "as an umbrella term that includes military activities (e.g., Information Operations, Public Affairs, military support to diplomacy and public diplomacy, and parts of Civil Affairs and Civil-Military Operations) and civilian ones (comprising both public and covert—or clandestine—efforts). Importantly, influence operations include non–Department of Defense (DoD) informational activities, such as the diplomatic and public diplomatic activities of the State Department and influence activities conducted by the U.S. intelligence community."

105 Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare* (Santa Monica: RAND, 2019), xiii.

106 Ibid., xv-xvi.

107 Dougherty, *More than Half,* 12. Information confrontation comprises two related lines of effort: information-psychological and information-technical. Information-psych ological, as the name implies, manipulates the perceptions, beliefs, motivations, and cognitive functions of targets. Information-technical targets the systems that contain or transmit information.

108 Guttieri, "Accelerate Change or Lose," 91-92.

109 "Statement of Lieutenant General Francis Beaudette, U.S. Army Commanding General United States Army Special Operations Command Before The Senate Armed Services Committee Emerging Threats And Capabilities Subcommittee April 28, 202," 7, https://www.Armedservices.Senate.Gov/Imo/Media/Doc/20210428_Usasoc_Posture_Statement_Sasc-Etc-Final.pdf, accessed 4 May 2021.

110 NATO Innovation Hub, *Cognition Workshop Innovative Solutions to Improve Cognition* (Brussels: NATO, 2021), 3, https:// www.innovationhub-act.org/sites/default/files/2021-07/210601%20Cognition%20Workshop%20Report-%20v3.pdf, accessed 3 June 2021.

111 François du Cluzel, *Cognitive Warfare* (Brussels: NATO Innovation Hub, 2021), 4.

112 Jones, *Three Dangerous Men,* 148.

113 Tim Hwang, *Deepfakes – Primer and Forecast* (Brussels: NATO STRATCOM COE, 2020), 6.

114 Ibid., 4.

115 Joshua Rhett Miller, "Deepfake video of Zelensky telling Ukrainians to surrender removed from social platforms," *New York Post*, 17 March 2022, https://nypost.com/2022/03/17/deepfake-video-shows-volodymyr-zelensky-telling-ukrainians-to-surrender/, accessed 26 April 2022.

116 Evgeny Pashentsev and Darya Bazarkina, *Malicious Use of Artificial Intelligence and International Psychological Security in Latin America* (Moscow: International Center for Social and Political Studies and Consulting, 2020), 8.

117 Johnson and Marcellino, *Truth Decay*, 1.

118 Dougherty, *More than Half*, 1.

119 Ibid., 1. The Department of Homeland Security (DHS) has begun implementing a strategy to gather and analyze intelligence about security threats from public social media posts. The objective is to build a warning system to detect the sort of posts that appeared to predict an attack on the U.S. Capitol on 6 January 2020. The focus is not on the identity of the posters but rather on gleaning insights about potential security threats based on emerging narratives and grievances. Rather than look at the individuals, DHS is focusing on what narratives are resonating and spreading across platforms. From this information they believe they will be able to determine what potential targets need to be protected. The aim is to "identify emerging narratives as early as possible and assess whether those narratives are likely to influence acts of violence and how fast they're spreading across multiple platforms." Ken Dilanian, "DHS gathering intelligence on extremists, security threats from public social media," *NBC News*, 10 May 2021, https://a.msn.com/r/2/BB1gyOst?m=en-ca&referrerID=InAppShare, accessed 10 May 2021.

120 Richard Kaipo Lum, "A Map with No Edges. Anticipating and Shaping the Future Operating Environments," *Small Wars Journal*, 5 November 2020, https://smallwarsjournal.com/jrnl/art/map-no-edges-anticipating-and-shaping-future-operating-environments, accessed 6 November 2020.

121 Jeff Seldin, "Foreign Disinformation Feeds US Domestic Terrorism, Official Warns, *VOA*, 17 June 2021, https://www.voanews.com/usa/foreign-disinformation-feeds-us-domestic-terrorism-official-warns, accessed 17 June 2021.

122 Mazarr et al, *Understanding Influence,* xii.

123 United Nations, "Climate Action," ND, https://www.un.org/en/climatechange/what-is-climate-change, accessed 26 April 2022.

124 National Intelligence Council, *National Intelligence Estimate. Climate Change and International Responses to National Security Through 2040* (Washington, D.C.: Office of the Director of National Intelligence, 2021), 1.

125 Ibid., 2.

126 See Daniel Quiggin, Kris De Meyer, Lucy Hubble-Rose and Antony Froggatt, *Climate change risk assessment 2021* (London: Chatham House, 2021); Canada, *Canada's Changing Climate Report* (Ottawa: Government of Canada, 2019); and L. John Leggat, Chair,

Canada's Top Climate Change Risks. The Expert Panel on Climate Change Risks and Adaptation Potential (Ottawa: The Council of Canadian Academies, 2019).

127 National Intelligence Council, *National Intelligence Estimate. Climate Change and International Responses to National Security Through 2040* (Washington, D.C.: Office of the Director of National Intelligence, 2021), 1.

128 Mitchell Consky, "Climate change could increase armed conflict in Africa: study," *CTVNews.ca*, 27 June 2022, https://www.ctvnews.ca/climate-and-environment/climate-change-could-increase-armed-conflict-in-africa-study-1.5963379, 27 June 2022.

129 President Donald Trump has long called for an end to "endless wars," particularly in places where he defined conflict to be "tribal" and not directly affecting the United States. Africa was one such location. Karen DeYoung, "French defense minister visits Washington to press for continued U.S. role in West Africa," *The Washington Post*, 28 January 2020, https://www.washingtonpost.com/national-security/french-defense-minister-visits-washington-to-press-for-continued-us-role-in-west-africa/2020/01/28/39905e38-41e5-11ea-b5fc-eefa848cde99_story.html, accessed 30 January 2020.

130 Robbie Gramer, "U.S. Congress Moves to Restrain Pentagon Over Africa Drawdown Plans," *Foreign Policy*, 4 March 2020, https://foreignpolicy.com/2020/03/04/africa-military-trump-esper-pentagon-congress-africom-counterterrorism-sahel-great-power-competition/, accessed 24 March 2020.

131 Lara, Seligman, "In West Africa, U.S. Military Struggles for Scarce Resources as Terrorism Threat Grows," *Foreign Policy*, 24 February 2020, https://foreignpolicy.com/2020/02/24/in-west-africa-u-s-military-struggles-for-scarce-resources-as-terrorism-threat-grows/, accessed 18 March 2020; *Agence France Presse*, "African Union says preparing 3,000-troop deployment to Sahel," 27 February 2020, https://www.capitalfm.co.ke/news/2020/02/african-union-says-preparing-3000-troop-deployment-to-sahel/, accessed 28 February 2020; and Multi-National Joint Task Force (MNJTF) against Boko Haram Fact Sheet, file:///G:/1%20-%20Virtual%20Library/Resource%20Library/Specialty%20Topic%20Areas/Regional%20Focus/Africa/Sahel/apf_factsheet_-_mnjtf.pdf, accessed 17 March 2020.

132 Méryl Demuynck and Julie Coleman, "The Shifting Sands of the Sahel's Terrorism Landscape," *International Council on Counter-Terrorism*, 12 March 2020, https://icct.nl/publication/the-shifting-sands-of-the-sahels-terrorism-landscape/, accessed 13 March 2020.

133 Phillip Carter III and Bisa Williams, "Developments in the Sahel could be worse than Ukraine crisis," *The Hill*, 21 February 2022. Https:// www.msn.com/en-ca/news/politics/developments-in-the-sahel-could-be-worse-than-ukraine-crisis/ar-AAU8dNC?ocid=sapphireappshare, accessed 22 February 2022; Shawn Snow, *Military Times*, 11 February 2020, https://www.militarytimes.com/flashpoints/2020/02/11/with-limited-resources-us-military-shifts-strategy-from-degrading-militants-in-west-africa-to-containment/, accessed 12 February 2020; Laurence-Aïda Ammour, "How Violent Extremist Groups Exploit Intercommunal Conflicts in the Sahel," *AfricaCenter.Org*, 26 February 2020, https://africacenter.org/spotlight/how-violent-extremist-groups-exploit-intercommunal-conflicts-in-the-sahel/, accessed 27 February 2020; Stratfor Worldview, "Why Is Terrorism Rising in West Africa? Can it be Stopped?" *nationalinterest*.

org, 16 March 2020, https://nationalinterest.org/blog/buzz/why-terrorism-rising-west-africa-132612, accessed 17 March 2020. In Burkina Faso the number of people internally displaced rose from 40,000 at the end of 2018 to in excess of 500,000 at the end of 2019, which represents more than two percent of the population. In Mali, the number practically doubled during this time frame. Louise Dewast, "France summit: Sahel crisis in danger of slipping out of control." *BBC News*, 13 January 2020, https://www.bbc.com/news/world-africa-51061229, accessed 13 January 2020.

134 Michael Phillips, "Militants are Edging South Toward West Africa's Most Stable and Prosperous States," *The Wall Street Journal*, 2 March 2022, https://www.wsj.com/articles/sahel-based-militants-edging-south-toward-west-africas-most-stable-and-prosperous-states-11646221800?utm_source=iterable&utm_medium=email&utm_campaign=3810496_, accessed 5 March 2022.

135 Phillips, "Militants are Edging."

136 Danielle Paquette and Joby Warrick, "Al-Qaeda and Islamic State groups are working together in West Africa to grab large swaths of territory," *The Washington Post*, 22 February 2020, https://www.washingtonpost.com/world/africa/al-qaeda-islamic-state-sahel-west-africa/2020/02/21/7218bc50-536f-11ea-80ce-37a8d4266c09_story.html, accessed 24 February 2020.

137 Jake Pemberton, "Explainer: French anti-jihadist force in Africa," *i24news*, 12 April 2022, https://www.i24news.tv/en/news/international/africa/1649766952-explainer-french-anti-jihadist-operation-in-africa?utm_source=iterable&utm_medium=email&utm_campaign=4069938_, accessed 14 April 2022; Bykehinde Giwa, "French Forces in Mali Retreat to Niger Republic," *News Central TV*, 29 March 2022, https://newscentral.africa/2022/03/29/french-forces-in-mali-retreat-to-niger-republic/, accessed 29 March 2022; and Macron to reduce French military troops in Africa's Sahel," *The Canadian Press*, 10 June 2021, https://www.msn.com/en-ca/news/world/macron-to-reduce-french-military-troops-in-africa-s-sahel/ar-AAKUYtv?ocid=msedgdhp&pc=U531, accessed 10 June 2021.

138 Lara Seligman, "In West Africa, U.S. Military Struggles for Scarce Resources as Terrorism Threat Grows," *Foreign Policy*, 24 February 2020, https://foreignpolicy.com/2020/02/24/in-west-africa-u-s-military-struggles-for-scarce-resources-as-terrorism-threat-grows/, accessed 24 February 2020.

139 Michael Horton, "Competition for Access and Influence Heighten Geopolitical Rivalries in the Horn of Africa," *Terrorism Monitor*, Vol. 20, No. 7, https://jamestown.org/program/geopolitical-rivalries-and-competition-for-access-and-influence-in-the-horn-of-africa-increase-instability/, 11 April 2022.

140 "U.S. Officials: Some Troops to Stay In Africa Amid Moves By Russia, China," *Radio Free Europe/Radio Liberty,* https://smallwarsjournal.com/blog/us-officials-some-troops-stay-africa-amid-moves-russia-china, accessed 31 January 2020.

141 Abraham Mahshie, "African military chiefs: US winning war of influence by helping fight terrorism in Africa," *Washington Examiner*, 24 February 2020, https://www.washingtonexaminer.com/policy/defense-national-security/african-military-chiefs-us-winning-war-of-influence-by-helping-fight-terrorism-in-africa, accessed 26 February 2020.

142 James Stavridis, "A more secure Africa is in America's best interests," *Bloomberg*, 18 February 2020, https://www.japantimes.co.jp/opinion/2020/02/18/commentary/world-commentary/secure-africa-americas-best-interests/#.XkwVWWZYaUl, accessed 18 February 2020.

143 Aaron Mehta, "Why the UK is investing in a new ranger regiment," *Defense News*, 25 May 2021, https://www.defensenews.com/global/europe/2021/05/25/why-the-uk-is-investing-in-a-new-ranger-regiment/, accessed 25 May 2021.

144 Barnett S. Koven and Chris Mason, "Back To The Future: Getting Special Forces Ready For Great-Power Competition," *War on the Rocks*, 4 May 2021, https://warontherocks.com/2021/05/back-to-the-future-getting-special-forces-ready-for-great-power-competition/, accessed 4 May 2021.

145 Mohammed Yusuf, "US: Africa Needs Tailored Strategies to Fight ISIS Groups," *VOA News*, 18 May 2022, https://www.voanews.com/a/us-africa-needs-tailored-strategies-to-fight-isis-groups-/6579078.html?utm_source=iterable&utm_medium=email&utm_campaign=4305193_, accessed 20 May 2022. Vladimir Voronkov, the Under-Secretary General of the UN's CT office warned, "An estimated 6,000 to 10,000 militants are fighting for the Islamic State group in Syria and Iraq." He further called on member states to maintain gains made against the group to prevent it from expanding. "UN says 6,000-10,000 IS militants still 'active' in Iraq and Syria," *The New Arab*, 11 February 2022, https://english.alaraby.co.uk/news/un-says-6000-10000-militants-active-iraq-syria, accessed 11 February 2022.

146 Andrew Eversden, "SOCOM Head On Global Terrorism: 'I Think It's Spread'," *Breaking Defense*, 2 November 2021, https://breakingdefense.com/2021/11/socom-head-on-global-terrorism-i-think-its-spread/, accessed 3 November 2021.

147 "Islamic State expanding globally amid setbacks: US official," *France 24*, 17 September 2020, https://www.france24.com/en/20200917-islamic-state-expanding-globally-amid-setbacks-us-official?utm_source=iterable&utm_medium=email&utm_campaign=1536024, accessed 19 September 2020.

148 Mosa'ab Elshamy, "Top US general in Africa: 'Wildfire of terrorism' on march here," *Military Times*, 20 June 2021, https://www.militarytimes.com/news/pentagon-congress/2021/06/19/top-us-general-in-africa-wildfire-of-terrorism-on-march-here/, accessed 21 June 2021.

149 Elliot Smith, "Russia is building its military influence in Africa, challenging U.S. and French dominance," *CNBC*, 13 Sep 2021, https://www.cnbc.com/2021/09/13/russia-is-building-military-influence-in-africa-challenging-us-france.html, accessed 13 September 2021.

CHAPTER 7

1 SFA is defined as "The Department of Defense activities that contribute to unified action by the US Government to support the development of the capacity and capability of foreign security forces and their supporting institutions." DoD, *Department of Defense Dictionary of Military and Associated Terms Joint Publication 1-02* (Washington

D.C.; DoD, 2010 as amended through 31 January 2011), 326 (Henceforth DoD, JP 1-02). SFA building partner nation capacity can serve two purposes – 1. To deny space and sanctuary and to develop partner capability to conduct specialized missions, including DA against key terrorist group leaders but also elite capabilities to respond to a range of contingencies and threats as they emerge. Helping our foreign partners to provide for their own security and contribute to regional stability is an investment that pays immediate and long-term dividends by reducing the need for costlier US interventions in response to turmoil in regions critical to US interests. "Joint Statement For the Record by the Honorable Michael A. Sheehan Assistant Secretary of Defense for Special Operations / Low-Intensity Conflict and The Honorable Derek H. Chollet Assistant Secretary of Defense For International Security Affairs on Emerging counterterrorism threats before the Committee on Armed Services United States Senate Emerging Threats and Capabilities Subcommittee," ND, 5.

2 Jonathan Broder, "Is Africa Lost to Islamist Militants?" *SpyTalk*, 24 May 2021, https://www.spytalk.co/p/is-africa-lost-to-islamist-militants, accessed 26 May 2021.

3 Military historian Max Boot stated, "Twenty years after the 9/11 attacks, the era of counterinsurgency is drawing to a close—and the COIN doctrine is fast losing influence in national security circles. It would be a grave mistake, however, to devalue COIN. There is no strategy better suited to confronting terrorists and guerrillas. If the United States forgets the precepts of COIN, as it did after the Vietnam War, it will pay a fearful price on future battlefields." Max Boot, "America Still Needs Counterinsurgency," *Foreign Affairs*, 2 June 2021, https://www.foreignaffairs.com/articles/afghanistan/2021-06-02/america-still-needs-counterinsurgency, accessed 4 June 2021.

4 Steff Thomas, "Post-Afghanistan, Special Operations to Shift to Conflict Prevention," *National Defense*, http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1220, accessed 1 August 2013.

5 Carlo Muñoz, "Exclusive: Special ops to turn focus from war on terror to China, Russia," *Washington Times*, 24 February 24, 2019, https://www.washingtontimes.com/news/2019/feb/24/special-ops-mission-shifts-terrorism-china-russia/, accessed 27 February 2019.

6 Centre for Army Lessons Learned, Newsletter 11-34, "Irregular Warfare: A SOF Perspective," June 2011, 6, http://cgsc.contentdm.oclc.org/cdm/landingpage/collection/p15040coll4, accessed 24 March 2020.

7 Dr. Jonathan Schroden, panelist at the "Transforming SOF to Meet Future Challenges" SOF Symposium at the Joint Special Operations University, Tampa, Florida, 8 January 2020.

8 FID is defined as "Participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security." DoD, JP1-02, 145.

9 Written Statement of Admiral William H. McRaven, USN Commander, United States Special Operations Command Before the 113th Congress Senate Armed services Committee Emerging Threats and Capabilities Subcommittee, April 9, 2013. He also

noted that "Extremist networks squeezed in one country migrate to others. Terrorist propaganda from a cell in Yemen can incite attacks as far away as Detroit or Delhi. Technology and globalization have made our countries and our communities interdependent and interconnected."

10 Cited in Thomas and Dougherty, *Beyond the Ramparts,* 6.

11 Cited in Ibid., 19. Admiral McRaven also stated, "Our 'new normal' is a persistently engaged, forward-based force to prevent and deter conflict and, when needed, act to disrupt and defeat threats. Long-term engagement is a hedge against crises that require major intervention and engagement positions us to better sense the environment and act decisively when necessary." Ibid., 45.

12 Cited in Stew Magnuson, "Special Operations Missions to Require New Doctrine," *National Defense*, May 2013, 26. McRaven added, "It's hard, slow and methodical work that does not lend itself to a quick win." He noted the indirect approach was key to preventing conflicts. Therefore, "patience, persistence and building trust with our partners – a trust that cannot be achieved through episodic deployments, or chance contacts [is required]."

13 Joe Miller and Monte Erfourth, "SOF in Competition: Establishing the Foundation of Strategy," *Small Wars Journal*, https://smallwarsjournal.com/jrnl/art/sof-competition-establishing-foundation-strategy-v13, accessed 8 March 2020.

14 Cited in Espen Berg-Knutsen, "From Tactical Champions to Grand Strategy Enablers: The Future of Small-Nation SOF in Counter-Hybrid Warfare," *Combatting Terrorism Exchange*, Vol. 6, No. 4, November 2016, 64-65.

15 The U.S. ARSOF commander stated:

> *Special operations are making significant modernization advancements in three major pathways: 1) our human performance advantage enabled by POTFF funding; 2) we are practicing information warfare and pressing the limits of advance; and 3) our hyper-enabled teams approach. Hyper-enabled teams address the toughest problems our operators will face at the most fundamental level: how they shoot, move, communicate, and survive in highly contested environments. Organic capability is what we will need to fight mobile, independently, and disaggregated. We must be able to process a large amount of real-time information and deliver precision organic fires all while staying undetected. We are investing in low-probability of intercept and detection high bandwidth resilient communications networks; a wide array of precision fires capability including everything from hand-held lethal drones to ground-launched large payload loiter munitions; next generation intelligence, surveillance, and reconnaissance (ISR) with multi-sensor, over-the-horizon, autonomously piloted platforms that use AI to identify their targets; assured precision navigation alternatives when global positioning system (GPS) is not an option; and any technology that minimizes our signature or provides "digital camouflage.*

"Statement of Lieutenant General Francis Beaudette, U.S. Army Commanding General United States Army Special Operations Command Before The Senate Armed Services Committee Emerging Threats And Capabilities Subcommittee April 28, 202," 7, https://www.Armedservices.Senate.Gov/Imo/Media/Doc/20210428_Usasoc_Posture_Statement_Sasc-Etc-Final.pdf, accessed 4 May 2021.

16 For example, the U.S. considered the possibility of using special forces to guard their embassy in Kyiv as a replacement or supplement to U.S. Marines. This option held a number of advantages. "First, it would delegate security to highly experienced soldiers at a time when unique threats may exist and an error in judgment could raise already high tensions between Moscow and Washington. Second, special forces may be better positioned to engage in exfiltration and evacuations operations should diplomatic staff, U.S. citizens, or foreign partners need to be removed from Ukraine on short notice." Adam Weinstein, "US special forces in Kyiv: Much ado about nothing?" *Responsible Statecraft*, 27 May 2022, https://responsiblestatecraft.org/2022/05/27/us-special-forces-in-kyiv-much-ado-about-nothing/, accessed 27 May 2022.

17 Admiral Olsen wrote, "These are warriors who can act swiftly with precision and lethality, yet remain simultaneously capable of building long-term relationships and trust with international partners." Admiral Eric T. Olson, *2010 Posture Statement* (Washington D.C.: United States Special Operations Command, 2010).

18 Stephen Watts, Sean M. Zeigler, Kimberly Jackson, Caitlin Mcculloch, Joseph Cheravitch, Marta Kepe, *Countering Russia. The Role of Special Operations Forces in Strategic Competition* (Santa Monica, CA: RAND, 2021), 7.

19 Niccolò Petrelli, "The missing dimension: IDF special operations forces and strategy in the Second Lebanon War", *Small Wars & Insurgencies*, Vol. 23, No. 1, March 2012, 56-73.

20 Chris Hughes, "SAS soldiers dispatched to Kabul as Brit troops leave Afghanistan after 20 years," Mirror, 2 June 2021, https://www.mirror.co.uk/news/uk-news/sas-troops-dispatched-kabul-brit-24237631, accessed 3 June 2021.

21 Will Irwin and Dr. Isaiah Wilson III, *The Fourth Age of SOF: The Use and Utility of Special Operations Forces in a New Age* (Tampa: JSOU, 2022), 83.

22 Tom Hammerle and Mike Pultusker, "Special Operations are Deterrence Operations: How United States Special Operations Forces should be used in Strategic Competition," *Small Wars Journal*, 24 May 2022. For example, due to Russia's aggressive stance in Eastern Europe, the U.S. has established a new special-operations headquarters in Albania. The U.S. Special Operations Command Europe (SOCEUR) announced the new headquarters will assist SOCEUR's mission to "galvanize our relationship with Allies and partners to counter malign influence, build interoperability, rapidly respond to emerging threats and if necessary, defeat aggression." Stavros Atlamazoglou, "US special operators are getting a new outpost in a tense corner of Europe," *Business Insider,* 7 February 2022, https://news.yahoo.com/us-special-operators-getting-outpost-231700866.html, accessed 8 February 2022.

23 Taft et al, *Special Operations Forces*, 10. Analysts have also noted that there is "Not always a military solution - While IW [irregular warfare] in competition still emphasizes identifying and understanding malign networks, the 'finish' will differ. Instead of direct action, DoD's efforts to illuminate networks could enable a panoply of interagency 'finish' options, including diplomatic or financial sanctions, public diplomacy, information operations, or other effects that incorporate all elements of US national power and are applied deliberately to bring about a desired political

outcome. Kevin Bilms, "The Defense Department Just Published A Summary Of The National Defense Strategy's Irregular Warfare Annex. Here's Why It's So Significant," *Modern War Institute*, 2 October 2020, https://mwi.usma.edu/the-defense-department-just-published-a-summary-of-the-national-defense-strategys-irregular-warfare-annex-heres-why-its-so-significant/, accessed 7 October 2020; and https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.pdf, accessed 7 October 2020.

24 Sandor Fabian, "Building and Enabling Urban Resistance Networks in Small Countries - A Crucial Role for U.S. Special Forces In Great Power Competition," *Small Wars Journal*, 11 April 2021, https://smallwarsjournal.com/jrnl/art/building-and-enabling-urban-resistance-networks-small-countries-crucial-role-us-special, accessed 21 April 2021.

25 Ibid.

26 Federico Bosari, "Hunting the Invader: Ukraine's Special Operations Troops," *CEPA*, 15 March 2022, https://cepa.org/hunting-the-invader-ukraines-special-operations-troops/,accessed 17 April 2022; Robert Stevens, "UK special forces are supplying war zone training to Ukraine's troops," World Socialist Web Site, 18 April 2022, https//www.wsws.org/en/articles/2022/04/18/ukuk-a18.html, accessed 19 April 2022; John Vandiver, "US special operations presses on in Ukraine amid threat of Russian invasion," *Stars & Stripes*, 19 January 2022, https://www.stripes.com/theaters/europe/2022-01-19/special-forces-press-on-in-ukraine-amid-threat-of-russian-invasion-4343248.html, accessed 21 January 2022; and D.G. Martin, "One on One: North Carolina, Special Forces, and Ukraine," *Chapelboro.Com*, 28 March 2022, https://chapelboro.com/town-square/one-on-one-north-carolina-special-forces-and-ukraine, accessed 29 March 2022.

27 Eric Schmitt, Julian E. Barnes and Helene Cooper, "Commando Network Coordinates Flow of Weapons in Ukraine, Officials Say," *New York Times*, 25 June 2022, https://www.nytimes.com/2022/06/25/us/politics/commandos-russia-ukraine.html, accessed 27 June 2022; David Pugliese, "Canadian special forces operating in Ukraine, *New York Times* reports," *Ottawa Citizen*, 26 June 2022, https://Canadian special forces operating in Ukraine, New York Times reports | Edmonton Journal, accessed 27 June 2022; Robert Stevens, "UK special forces are supplying war zone training to Ukraine's troops," World Socialist Web Site, 18 April 2022, https//www.wsws.org/en/articles/2022/04/18/ukuk-a18.html, accessed 19 April 2022; and Alex Boutilier, Mercedes Stephenson and David Baxter, "Canada deploys special forces to Ukraine amid rising tensions with Russia," *Global News*, 18 January 2022, https://globalnews.ca/news/8517110/canada-special-forces-ukraine-russia/, accessed 21 January 2022.

28 The importance of the training function is such that the U.S. created in 2018 new Army Security Force Assistance Brigades (SFABs). The SFABs are designed to assist the U.S. military's capacity to advise foreign forces without disrupting existing combat units. There are six SFABs (five active duty and one National Guard). Similar to U.S. SF they are geographically aligned, covering Africa, Europe, the Middle East, the Pacific, and South America. This regionalization allows for the development of area expertise and continuity in their operations. Max Boot, "America Still Needs Counterinsurgency," *Foreign Affairs*, 2 June 2021, https://www.foreignaffairs.com/articles/afghanistan/2021-06-02/america-still-needs-counterinsurgency, accessed 4 June 2021.

29 Watts et al, *Countering Russia*, 70.

30 Walter Pincus, "General James Mattis and the Changing Nature of War," *The Cipher Brief*, 2 February 2021, https://www.thecipherbrief.com/column/fine-print/general-james-mattis-and-the-changing-nature-of-war, accessed 3 February 2021.

31 For example, Ukrainian oligarch Serhiy Taruta confirmed Russian special operations forces most likely had a role in the initiation of the rebellion. Taruta took part in the Ukrainian government's negotiations with the rebels in Donetsk. He revealed that the Ukrainian authorities were able to bribe the rebels, who had taken over the town hall in Donetsk, to leave the building. However, as soon as that agreement was clear, "green men" came to Donetsk from Sloviansk and changed the mind of the Donetsk rebels. After that visit, a compromise was no longer possible. As such, it appears that Russia used its SOF to initiate parts of the anti-Kyiv rebellion in Donbas. Tor Bukkvoll, "Russian Special Operations Forces in Crimea," *Parameters*, Vol. 46, No. 2, Summer 2016, 18.

32 Ibid., 18.

33 Scholl, "The Use of US Special Operation Forces." The researchers also noted: "In addition, the Nigerian security forces in conjunction with SOF discovered an illegal weapons cache traced back to a subsidiary of the construction company. The port construction blueprints were obtained by the Nigerian security team and sent to Defense Intelligence Agency for analysis, who discovered the planned concrete footings were specific to support surface-to-air and shore-to-ship missiles. Armed with this analysis, the U.S. Ambassador explained to their Nigerian counterparts that the port would become a strategic target and potential war zone between great powers; the Nigerians seized the Chinese-purchased land and halted the port construction. SOF's forward presence provided advanced warning of Chinese nefarious activities and, partnering with the US Embassy team, thwarted these activities."

34 An American official explained, "We want the Baltics to present a deterrent to Russia. And part of what we can do in the Army is have our special operations forces work with the Baltic militaries to help them in terms of…developing what I would call resistance capabilities. Nations supported under the ROC [Resistance Operating Concept] are encouraged to establish the legal and organizational framework for a resistance and bring it under the official control of their armed forces. One such example is the Estonian Defence League, a volunteer paramilitary organization whose 16,000 members are organized under Tallinn's defense ministry and receive training from U.S. special operations." David Winkie, "Less door-kicking, more resistance: Inside Army SOF's return to unconventional warfare," *Army Times*, 9 September 2021, https://www.armytimes.com/news/your-army/2021/09/09/less-door-kicking-more-resistance-inside-army-sofs-return-to-unconventional-warfare/, accessed 19 September 2001.

35 Insider, "US Green Berets Who've Trained Taiwanese Troops Explain How They Could Fight China and Why the US Keeps Their Mission Secret," *SOFREP*, 26 October 2021, https://sofrep.com/news/us-green-berets-whove-trained-taiwanese-troops-explain-how-they-could-fight-china-and-why-the-us-keeps-their-mission-secret/, accessed 28 October 2021; and Julian Borger, "Secret group of US military trainers has been in Taiwan for at

least a year," *The Guardian*, 7 October 2021, https://www.theguardian.com/world/2021/oct/07/taiwan-us-military-trainers-china, accessed 14 October 2021.

36 Douglas London, "Could Sabotage Stop Putin From Using the Nuclear Option?" *Foreign Policy*, 12 May 2022, https://foreignpolicy.com/2022/05/12/putin-russia-ukraine-sabotage-stop-putin-nuclear-option/, accessed 15 May 2022.

37 Heiki Jakson, James Brendan Byrne, Emanuele Nicola Cecchetti, Jan Ciampor, Jaroslav Hajek, Maximilian Hausler and Kateryna Dubrova, *Energy in Irregular Warfare* (Brussels: NTO Energy Security Centre of Excellence, 2017), 24.

38 Ibid., 25-26.

39 Ibid., 25-26.

40 Ibid., 25-26.

41 Tor Bukkvoll, "Russian Special Operations Forces in Crimea," *Parameters*, Vol. 46, No. 2, Summer 2016, 17.

42 Ibid., 19-20.

43 Stavros Atlamazoglou, "Navy SEALs and Army Green Berets Are Training For A Frigid Battlefield," 1945, 15 May 2022, https://www.19fortyfive.com/2022/05/navy-seals-and-army-green-berets-are-training-for-a-frigid-battlefield/, accessed 16 May 2022.

44 "US special force troops disguised as airport workers took part in Qassem Suleimani killing, report claims," *The National*, 9 May 2021, https://www.thenationalnews.com/mena/us-special-force-troops-disguised-as-airport-workers-took-part-in-qassem-suleimani-killing-report-claims-1.1219570, accessed 10 May 2021.

45 "Israel told US it carried out assassination of Iranian colonel, report says," *Middle East Eye*, 26 May 2022, https://www.middleeasteye.net/news/israel-behind-killing-iran-colonel-us-told, 26 May 2022; and Joe Truzman, "IRGC Colonel Assassinated in Tehran, Mossad Suspected of Being Behind Hit," *The Long War Journal*, 22 May 2022, https://www.longwarjournal.org/archives/2022/05/irgc-colonel-assassinated-in-tehran-mossad-suspected-of-being-behind-hit.php, accessed 25 May 2022.

46 Eric Schmitt and Ben Hubbard, "U.S. Military Offers New Details on Raid That Led to Death of ISIS Leader," *The New York Times*, 10 February 2022, https://archive.md/R1m7Z#selection-301.0-785.137, accessed 11 February 2022.

47 Cited in Bryce Loidolt, "Were Drone Strikes Effective? Evaluating the Drone Campaign in Pakistan Through Captured al-Qaeda Documents," *Texas National Security Review*, Vol. 5, Issue 2, Spring 2022, https://tnsr.org/2022/01/were-drone-strikes-effective-evaluating-the-drone-campaign-in-pakistan-through-captured-al-qaeda-documents/, accessed 9 February 2022.

48 Cited in Ibid.

CHAPTER 8

1 Globalization is defined as "the process of interaction and integration among people, companies, and governments worldwide. Globalization has accelerated since the 18th century due to advances in transportation and communication technology," https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095855259, accessed 28 October 2021.

2 USSOCOM, *On Competition*, xi.

3 The Turkish use of drone swarms to engage Syrian bases and chemical weapon depots in March 2020, as well as the South Korean demonstration of 1,218 autonomous drones equipped with lights collaborating to form intricate images in the night sky over Pyeongchang during the opening ceremonies of the 2018 Olympics provide a preview of what drone swarms are capable of achieving. See Seclan Hacaoglu, "Turkey's Killer Drone Swarm Poses Syria Air Challenge to Putin," *Bloomberg*, 1 March 2020, https://www.bloomberg.com/news/articles/2020-03-01/turkey-s-killer-drone-swarm-poses-syria-air-challenge-to-putin, accessed 2 March 2020; and Brose, "The New Revolution."

4 See Nick Allen, Nataliya Vasilyeva and Joe Barnes, "Russia may invade Ukraine, U.S. warns as Russian forces gather near border," *The Telegraph*, 11 November 2021, https://nationalpost.com/news/world/russia-may-invade-ukraine-u-s-warns-as-russian-forces-gather-near-border, accessed 13 November 2021; Sam Fleming and Valentina Pop, "NATO calls on Moscow to ease tension over military build-up near Ukraine," *Financial* Times, 16 November 2021, https://archive.md/HODrs#selection-1503.0-1503.72, accessed 16 November 2021; and Eric Cheung and Brad Lendon, "China air force sends 77 warplanes into Taiwan defense zone over two days, Taipei says," *CNN*, 3 October 2021, https://www.msn.com/en-ca/news/world/china-air-force-sends--warplanes-into-taiwan-defense-zone-over-two-days-taipei-says/ar-AAP57ZO?ocid=sapphireappshare, accessed 4 October 2021.

5 Alan Bell, "On A Wing and A Prayer: Task Force 317 And The Recapture Of South Georgia Island," in Colonel (retired) Bernd Horn, ed., *Risk: SOF Case Studies* (Kingston: ERC Press, 2020), 125. See Bell's chapter, as well as Lieutenant General Sir Cedric Delves, *Across an Angry Sea. The SAS in the Falklands War* (London: Hurst & Company, 2018), 41-107, for an "operator's account" of the entire mission.

6 Ken Connor, *Ghost Force. The Secret History of the SAS* (London: Orion), 368-371; and John Strawson, *A History of the SAS Regiment* (London: Secker &Warburg, 1985), 236-238.

7 Delves, *Across an Angry Sea*, xvii, 131-174.

8 De La Billiere's plan was not met with enthusiasm. One former SAS operator recalled, "the Director [De La Billiere] wished us all good luck, said he would have our backs and that we would have his full support throughout the [Falklands] campaign. Unfortunately, at that time, little did we realize what he meant, but we were to learn later in the conflict that we were being signed on to execute 'mission impossible' tasks, without the benefit of discussion or first refusal." Alan Bell, "On a Wing and a Prayer – Task Force 317 and the Recapture of South Georgia Island," unpublished paper, 2014.

The Officer Commanding SAS "B" Squadron also disagreed. He was not convinced of the plan's viability. While staging on Ascension Island he voiced his concern. Director Special Forces was not impressed. De La Billiere lamented, "I was dismayed to find that the attitude of this unit [B Squadron] remained lukewarm. The trouble, I found, lay in the squadron commander, who himself did not believe in the proposed operation." The squadron commander was duly sacked. General Sir Peter De La Billiere, *Looking for Trouble. SAS to Gulf War* (London: Harper Collins Publishers, 1995), 346-347. Cedric Delves, then a squadron commander in the SAS later explained, "The EXOCET menace eventually grew acute. But an operation employing us to reduce the threat would have been pregnant with disproportionate risk, probably requiring a sizeable carrier task group to take forward the Squadron and its supporting helicopters, closing the Argentine mainland, bringing us all well within range of hundreds of enemy aircraft. And there could be no guarantee of nailing the objective, aircraft having a habit of moving. Nobody in his right mind would contemplate such a gamble. It was the sort of thing that could end in catastrophe and lose us the war." Delves, *Across an Angry Sea*, 115.

9 In advance of the raid, a Sea King helicopter was to drop off eight SAS operators (Operation Plum Duff) to observe the Argentinian Base and report. Due to weather conditions the helicopter was forced to abort. The helicopter pilot flew to Chile, ditched and destroyed the aircraft and all eight SAS operators and three aircrew were eventually picked up by Chilean forces and later returned to Britain. The aborted mission no compromised the element of surprise. Moreover, British intelligence discovered that Argentina's radar system was better than had originally been thought. As a result, Operation Mikado was cancelled. Peter Jackson, "Falklands War: SAS role in the conflict," *BBC*, 4 May 2021, https:// www.bbc.com/news/uk-17203398, accessed 4 November 2021; and Connor, *Ghost Force*, 373-378.

10 The first US SOF teams began searching for mobile Transporter-Erector-Launchers on 7 February 2001. U.S. SOF and the SAS divided the responsibility for searching for the SCUD TEL launchers. The Americans operated in a several thousand square mile area northwest of the main Baghdad to Amman route up to the Syrian border (known as "Scud Boulevard") and the SAS was given the same size area known as "SCUD Alley." William Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets. Lesson from Vietnam and the Persian Gulf War* (Santa Monica, CA: RAND, 2001), 30-39. See also DoD, *USSOCOM History,*34-42*;* Douglas C. Waller, *Commando. The Inside Story of America's Secret Soldiers* (New York: Simon & Shuster, 1994), 225-352; Susan Maquis, *Unconventional Warfare* (Washington D.C.: Brookings Institute Press, 1997), 227-249; Thomas K. Adams, *US Special Operations Forces in Action. The Challenge of Unconventional Warfare* (London: Frank Cass, 1998), 231-244; T. Carney and Benjamin F. Schemmer, *No Room for Error* (New York: Ballantine Books, 2003), 224-236; Connor, *Ghost Force*, 456-501; and Robin Neillands, *In the Combat Zone. Special Forces Since 1945* (London: Weidenfeld and Nicolson, 1997), 287-297.

11 There is no firm number of how many TELs were destroyed, however, the Iraqi launch rate dramatically decreased. Overall, the Iraqis fired 88 missiles against Israel and Saudi Arabia and Bahrain. They fired 33 in the opening week of Desert Storm at a daily rate of 4.7 launches. During remaining 36 days, they fired 55 missiles at a daily rate of 1.5 launches. Rosenau, *Special Operations Forces, 42*. See also DoD, *USSOCOM History,* 42-44; B.J. Schemmer, "Special Ops Teams Found 29 Scuds Ready to Barrage

Israel 24 Hours Before Ceasefire," *Armed Forces Journal International,* July 1991, 36; Mark Thompson, Azadeh Moaveni, Matt Rees, and Aharon Klein, "The Great Scud Hunt," *Time*, 23 December 2002, Vol. 160, no. 26, 34; and Cameron Spence, *Sabre Squadron* (London: Michael Joseph, 1997).

12 R. Jeffrey Smith, "U.S. Special Forces Carried Out Sabotage, Rescues Deep in Iraq," *The Washington Post*, 4 March 1991, https://www.washingtonpost.com/archive/politics/1991/03/04/us-special-forces-carried-out-sabotage-rescues-deep-in-iraq/5b3738be-100c-40b2-b550-27be373cb88d/, accessed 5 November 2021.

13 Leigh Neville, *Special Operations Forces in Iraq* (Oxford: Osprey Publishing, 2008), 26-27.

14 In late 2002, CIA and 10 SFG infiltrated into Kurdistan, into the Harir Valley to develop intelligence and organize and train Peshmerga guerrillas. These teams paved the way for SOF teams when the war started.

15 "The battle for Kyiv: In Ukraine's capital, citizens head for shelter and take up arms," *National Post*, 25 February 2022, https;//www.msn.com/en-ca/news/world/the-battle-for-kyiv-in-ukraines-capital-citizens-head-for-shelter-and-take-up-arms/ar-AAUk4Rb?ocid=sapphireappshare, accessed 26 February 2022. Even prior to the invasion, American intelligence officials warned that Russian forces were being issued with "kill lists" of prominent Ukrainian politicians, officials and campaigners to be hunted down as part of Vladimir Putin's chilling vow to subject the country to "denazification." Cahal Milmo, "Russian special forces have entered Kyiv to hunt down Ukraine's leaders, says Volodymyr Zelensky," *inews.com.uk*, 25 February 2022, https://inews.co.uk/news/russia-special-forces-kyiv-ukraine-leaders-mercanaries-behind-lines-1483303, accessed 17 April 2022. See also https://www.msn.com/en-ca/news/world/assassination-plot-against-zelensky-was-foiled-and-unit-sent-to-kill-him-was-destroyed-ukraine-says/ar-AAUwfr5?ocid=sapphireappshare, accessed 4 March 2022; and Assassination plot against Zelensky was foiled and unit sent to kill him was 'destroyed,' Ukraine says," *National Post*, 2 March 2022, https://www.msn.com/en-ca/news/world/assassination-plot-against-zelensky-was-foiled-and-unit-sent-to-kill-him-was-destroyed-ukraine-says/ar-AAUwfr5?ocid=sapphireappshare, accessed 4 March 2022.

16 Follow-on forces eventually secured the airport for the Russians. However, they abandoned it on 2 April 2022 as part of their operational realignment of forces to eastern Ukraine. Chris Brown, "Just beyond Ukraine's battlefields, NATO's elite forces prepare for what could come next," *CBC News*, 14 May 2022, https://www.cbc.ca/news/world/ukraine-nato-special-operations-1.6452144, accessed 16 May 2022.

17 "Ukraine's partisans are hitting Russian soldiers behind their own lines," *The Economist*, 5 June 2022, https://www.economist.com/europe/2022/06/05/ukraines-partisans-are-hitting-russian-soldiers-behind-their-own-lines, accessed 10 June 2022; Andrew E. Kramer, "Ukrainian Official Outlines Intentional Ambiguity on Strikes Inside Russia," *The New York Times*, 30 April 2022, https://www.nytimes.com/2022/04/30/world/europe/ukraine-russia-attack-denials.html, accessed 2 May 2022; Laurence Peter, "Transnistria and Ukraine conflict: Is war spreading?" *BBC News*, 27 April 2022, https://www.bbc.com/news/world-europe-61233095, accessed 27 April 2022; and "Russian Missile Launchers Targeted in Donetsk Oblast, Ukrainian Special Forces Say,"

NT News, 6 July 2022, https://www.ntnews.com.au/news/national/russian-missile-launchers-targeted-in-donetsk-oblast-ukrainian-special-forces-say/video/3ee446fc1b0fd14e17342762fe67376e, accessed 6 July 2022.

18 "Ukraine's partisans are hitting Russian soldiers behind their own lines," *The Economist*, 5 June 2022, https://www.economist.com/europe/2022/06/05/ukraines-partisans-are-hitting-russian-soldiers-behind-their-own-lines, accessed 10 June 2022.

19 Ibid.

20 See Eric V. Larson, Derek Eaton, Brian Nichiporuk and Thomas S. Szayna, *Assessing Irregular Warfare* (Santa Monica, CA: RAND, 2008).

21 For example, British SOF are currently conducting OPs to monitor Russian activity in the Ukraine. Marco Giannangeli, "British SAS soldiers in Ukraine report spike in ceasefire violations," *Express*, 11 April 2021, https://www.express.co.uk/news/uk/1421624/russia-ceasefire-ukraine-british-soldiers-violations accessed 12 April 2021.

22 If reporting is accurate, Ukrainian Special Forces were utilized to attack Russian lines of communication, which aggravated the Russian logistical problem. In addition, Russia deployed SOF elements to infiltrate Kyiv to shape operations for follow-on conventional forces, as well as tasking them with assassinating top Ukrainian political leaders. See Federico Bosari, "Hunting the Invader: Ukraine's Special Operations Troops," CEPA, 15 March 2022, https://cepa.org/hunting-the-invader-ukraines-special-operations-troops/, accessed 17 April 2022; and Milmo, "Russian special forces."

23 Niccolò Petrelli, "The missing dimension: IDF special operations forces and strategy in the Second Lebanon War", *Small Wars & Insurgencies*, Vol. 23, No. 1, March 2012, 56-73.

24 Department of Defense (DoD), *SOF Interagency Reference Guide, Fourth Edition* (Tampa: JSOU, April 2020), c6.

25 See Insider, "US Green Berets"; and Dr. Sandor Fabian, "Building and Enabling Urban Resistance Networks in Small Countries - A Crucial Role For U.S. Special Forces In Great Power Competition," *Small Wars Journal*, 11 April 2021, https://smallwarsjournal.com/jrnl/art/building-and-enabling-urban-resistance-networks-small-countries-crucial-role-us-special accessed, 12 April 2021.

26 Arbitter and Carlson, "The Changing Face."

27 Stavros Atlamazoglou, "North Korea has the world's largest special-operations force. A defected spy offers hints about how they'd be used in a war," *Business Insider*, 27 October 2021, https://www.businessinsider.com/how-north-korea-might-use-special-operations-troops-in-war-2021-10, accessed 30 October 2021. On 31 January 1969, a North Korean SOF team infiltrated into South Korea with the objective of assassinating South Korean President Park Chung-hee. The North Korean commandos managed to reach Park's residence in Seoul, however, not knowing the code to access the residence they were eventually discovered and a raging firefight with South Korean troops ensued.

28 For example, see Tyler Rogoway, "Special Ops Train to Defend Strategic Aleutian Islands Radar Outpost During All-Out War." *The War Zone*, 18 October 20021, https://www.thedrive.com/the-war-zone/42783/special-ops-train-to-defend-strategic-radar-outpost-in-the-aleutian-islands-during-all-out-war, accessed 26 October 2021.

29 Ibid.

30 Ellen Mitchell, "Outcry grows over Russian missile test that hit satellite," *The Hill*, 17 November 2021, https://www.msn.com/en-ca/news/politics/outcry-grows-over-russian-missile-test-that-hit-satellite/ar-AAQO4K0?ocid=sapphireappshare, accessed 18 November 2021. This test was in addition to Russian tests of a "non-destructive space-based anti-satellite weapon" in July 2020. At the time, General John Raymond, the head of U.S. Space Command, asserted that the test was "further evidence of Russia's continuing efforts to develop and test space-based systems" and an "example that the threats to U.S. and Allied space systems are real, serious and increasing." Ibid.

31 The British have already addressed this issue to some degree by creating a new "Ranger" Regiment and tasking the Royal Marine Commandos to undertake tasks normally given to the SAS and SBS (e.g., COIN, FID) so that the SOF entities can focus on countering "big state adversaries." Larisa Brown, "Military chief reveals secret new role for special forces against China and Russia," *The Times*, 17 July 2021, https://www.thetimes.co.uk/article/military-chief-reveals-secret-new-role-for-special-forces-against-china-and-russia-hgbdwcsg7, accessed 25 July 2021; and Oliver Trapnell, "UK special forces to take on Russia and China in new covert role - 'Ready to react'," *Express*, 19 July 2021, https://www.express.co.uk/news/world/1464392/uk-special-forces-russia-china-secret-roel-mission-brigadier-mark-totten-ont, accessed 19 July 2021.

32 David Martin, "Top military official discloses new details about China's hypersonic test," *CBS News*, 17 November 2021, https://www.msn.com/en-ca/news/world/top-military-official-discloses-new-details-about-chinas-hypersonic-test/ar-AAQMQoG?ocid=sapphireappshare, accessed 18 November 2021.

33 Most major actors have developed autonomous systems capable of reconnaissance and offensive operations. For instance, the Russians possess "Kamikaze drones," also known as "loitering munitions" that are totally autonomous that can "find, decide to engage, and engage targets on their own" without the need for human intervention" that can be launched from land or ships. Raymond McConoly, "Russian Navy Ships Get More Powerful with Kamikaze drones," *Naval Post*, 30 October 2021, https://navalpost.com/russian-navy-kamikaze-drones/?fbclid=IwAR3MBQilWkpfao4VvgHBecPMuMxanYNA-_Pnvm478n-DiIqT2lDuc-6LWqo, accessed 2 November 2021. Similarly, the U.S. Air Force Research Lab (AFRL) is flying autonomous drones that are capable of navigating uneven, harsh terrain and independently finding and transmitting target specifics, performing manned-unmanned teaming missions and operating a large number of functions without needing pilot control. These autonomous drones are designed to work in swarms and blanket an area with surveillance, test enemy defences, find targets over high-threat areas and potentially function as munitions to attack specific targets. See Kris Osborn, "Next-Level Autonomy Achieved: Meet the Air Force Avenger Drone. This will allow military personnel to expand the scope of their mission," *The National Interest*, 20 July 2021,

https://nationalinterest.org/blog/buzz/next-level-autonomy-achieved-meet-air-force-avenger-drone-189945, accessed 20 July 2021; and Paul McLeary, "Navy, Marines Push Plans to Transform How they Fight," *Breaking Defense*, 16 April 2021, https://breakingdefense.com/2021/04/navy-and-marine-corps-push-plans-to-transform-how-they-fight/, accessed 20 April 2021. A final example is Britain that has tested operating swarms of drones underwater, on the sea and in the air. They have tested drones to conduct tactical re-supply as well as for reconnaissance and acquiring enemy targets. Ben Mitchell, Shane Jarvis and Max Channon, "Royal Marines Commandos operate 'drone swarms' in a first for Britain's armed forces," *WalesOnLine*, 17 July 2021, https://www.walesonline.co.uk/news/uk-news/royal-marines-commandos-operate-drone-21076315, accessed 19 July 2021.

34 Jack Watling, "Old Habits Die Hard: Special Operations Forces, Twenty Years Of Counterterrorism, And The New Era Of Great Power Competition," *The Modern War Institute*, 21 June 2021, https://mwi.usma.edu/old-habits-die-hard-special-operations-forces-twenty-years-of-counterterrorism-and-the-new-era-of-great-power-competition/, accessed 6 January 2022.

35 Brose, "The New Revolution." Notably, even Iran's IRGC has long-range ballistic missiles that travel 1,800 km and hit their designated targets. Maziar Motamedi, "Iran's Revolutionary Guard tests long-range missiles, drones," *Al Jazeera*, 16 January 2021, https://www.aljazeera.com/news/2021/1/16/irans-revolutionary-guards-test-long-range-missiles-drones, accessed 18 January 2021.

36 Watling, "Old Habits Die Hard."

37 Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War. The Coming Age of Post-Truth Geopolitics," *Foreign Affairs*, January/February 2019, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war, accessed 9 February 2021.

38 DoD, *MARSOC 2030* (Washington D.C.: Department of the Navy, 2030), 13.

39 Ibid., 17.

40 Kris Osborn, "Special Forces Can Conduct Undersea Ops Without Making a Sound. You'll never hear them coming," *The National Interest*, 8 July 2021, https://nationalinterest.org/blog/buzz/special-forces-can-conduct-undersea-ops-without-making-sound-189314, accessed 8 July 2021.

41 Watling, "Old Habits Die Hard."

42 Ibid.

43 DoD, *MARSOC 2030*, 9.

44 United Kingdom. *Strategic Trends Programme. Future Character of Conflict* (London: MoD, ND), 2.

CONCLUSION

1 Taft et al, *Special Operations Forces*, 8. It is also why some analysts and practitioners describe the current era as "Fourth-Age SOF." They believe that SOF needs to be better balanced to serve national interest by:

1. Serving as strategic shapers by performing a global special warfare function that provides the Joint Force geostrategic positional and informational advantage over competitors and adversaries;
2. Accommodating a strategy of campaigning for influence by serving as an exceptional and versatile agent of influence;
3. Contributing in unique ways to a strategy of integrated deterrence;
4. Improving America's ability to pursue the fight against extremists, as well as proliferators and potential users of WMD; and
5. Preparing for a traditional warfare special operations role or extraordinary crisis-response contingencies.

Will Irwin and Dr. Isaiah Wilson III, *The Fourth Age of SOF: The Use and Utility of Special Operations Forces in a New Age* (Tampa: JSOU, 2022), 63.

2 Written Statement of Admiral William H. McRaven, USN Commander, United States Special Operations Command Before the 113th Congress Senate Armed services Committee Emerging Threats and Capabilities Subcommittee, April 9, 2013. He also noted that "Extremist networks squeezed in one country migrate to others. Terrorist propaganda from a cell in Yemen can incite attacks as far away as Detroit or Delhi. Technology and globalization have made our countries and our communities interdependent and interconnected."

3 Cited in Ibid., 19. Admiral McRaven also stated, "Our 'new normal' is a persistently engaged, forward-based force to prevent and deter conflict and, when needed, act to disrupt and defeat threats. Long-term engagement is a hedge against crises that require major intervention and engagement positions us to better sense the environment and act decisively when necessary." Ibid., 45.

4 See Larson et al, *Assessing Irregular Warfare*.

5 Colin Gray, *Explorations in Strategy* (Westport, CT: Praeger, 1996), 149.

INDEX

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.

A Perilous Future: High Intensity Conflict and the Implications for SOF
Lieutenant-Colonel Andrew L. Brown, PhD, ed., 2022.

The U.S. Government's public release of their 2018 National Defense Strategy heralded a significant change in the American view of the world. It marked a "pivot" from a two decade focus on counter-terrorism and counter-insurgency, to a new focus on strategic competition, commonly referred to as Great Power Competition (GPC). The new U.S. strategy emphasized the importance of countering an emergent China and a resurgent Russia, as well as a number of rogue international actors. The American strategic pivot impacted Canada, as well as NATO and other Western partners. Notably, while strategic competition is not new, with the end of the Cold War, the U.S. and its Western partners failed to realize that their perception of peace, competition and conflict was not in consonance with that of their adversaries. Consequently, by 2018, they believed they were at a disadvantage in the new world order. Their concern was underscored by the fact that the impact of globalization, the proliferation of cheap and accessible technology, the explosion in the access and dissemination of information, as well as a number of other factors such as climate change and pandemics, has made the current era of strategic competition so much more complex and challenging than those that preceded it. While the role of Special Operations Forces remains key to a nation's military capability, they must fully understand the nature of competition and their role in the GPC in order to be truly effective. Strategic Competition: Impacts for SOF unpacks these interrelated and complex issues in order to help decision-makers be well situated to effectively employ a central asset in their arsenal and to enable SOF operators to more fully appreciate their role in the current defence environment.