National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

WAR, PEACE, AND THE EVAPORATING GREY ZONE: LOSING THE WAR WE AREN'T FIGHTING

Major Kevin Wong

JCSP 46

Solo Flight

Disclaimer

PCEMI 46

Solo Flight

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SOLO FLIGHT

WAR, PEACE, AND THE EVAPORATING GREY ZONE: LOSING THE WAR WE AREN'T FIGHTING

By Major Kevin Wong

Word Count: 5,191

Nombre de mots : 5.191

WAR, PEACE, AND THE EVAPORATING GREY ZONE: LOSING THE WAR WE AREN'T FIGHTING

War vs Peace

War, in a Western sense of the word, was the opposite of peace. War was composed of formal armed conflicts, to which two or more parties made violence against each other. These parties may be divided into combatants and non-combatants, which explained their role in the conflict.[1] Much of the recent Western, or "conventional", way of war was centred on these principles. They guide our efforts in terms of what is (or is not) a lawful target, who can be killed, and what can be destroyed. The coherence, predictability, and principles that we used to determine and apply the rules of war were key in the Western application of violence for many years.[2] Unfortunately for us, the rest of the world has moved on. They, our principle adversaries being Russia, China, and Iran, fight in new ways. These new methods ignored the established Western principles and often focused on proxy wars, mercenaries, insurgencies, and terrorists to use violence in achieving their aims. Other methods have included non-violent means such as economic coercion, information and propaganda campaigns, espionage, and non-attributable actions.[3] In many ways, this is the way the world used to fight wars prior to the 19th century, when despots, kings, and emperors ruled the world. The problem, for the West, with war today is that both sides are using different definitions of war, making it hard to see that the West is already in a war with our principle adversaries. This paper proposes that the United States (and it's Western allies) are already in a war with China, Russia, and Iran; a war that it does not even know it is fighting, and doesn't realize it is losing. The irony of this thesis is that the Grey Zone methods of war are not unknown in the West, they are simply forgotten. For most of European and early American

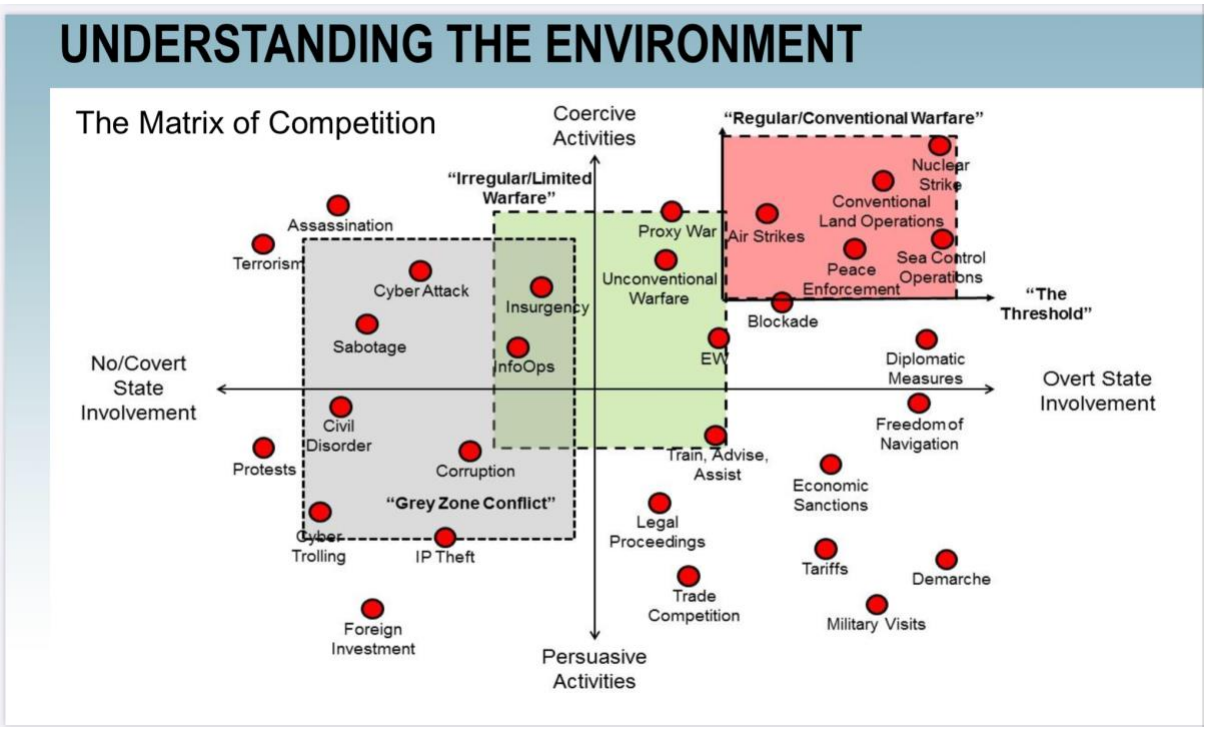
[1] Rosa Brooks, "Rule of Law in the Grey Zone", *Modern War Institute at West Point*, 2 July 2018, accessed 24 March 2020, https://mwi.usma.edu/rule-law-grey-zone/
[2] Ibid.
[3] Ibid.

history, the methods described as modern Grey Zone conflict was in fact the way of the world. Feudal lords in Europe were the richest and largest landowners (for the most part), and they waged war using mercenaries, economic measures, and violence in the extreme (what most would consider war crimes today). The American West was won through similarly savage methods. The idea of large standing armies, which were and remain enormously expensive is a relatively recent idea in comparison to human history. While most countries today have a standing military, many are finding that it is not necessarily the most effective way to achieve national aims. Many, including our principal adversaries have reached back into old play books and are rejuvenating old methods.

The Grey Zone

In his book, "The New Rules of War", Sean McFate argues that, "There is no such thing as war or peace - both coexist, always".[4] This statement captures the essence of Grey Zone conflict in a single, terrifying thought. The very idea of a space between, or perhaps encapsulating both, war and peace is a concept that is not well understood or fully embraced by US and Western leaders. Yet McFate is not alone in his acceptance of it. The Canadian Armed Forces (CAF) has established a small team to develop concepts into how the CAF will operate in this environment and has captured what fighting in the Grey Zone really means. The CAF has adopted a model called the Matrix of Competition, which outlines which activities are expected to be conducted in either "conventional warfare", "irregular warfare", and the "grey zone".[5]

[4] Sean McFate, *The New Rules of War; How America Can Win - Against, Russia, China, and Other Threats*, William Morrow/Harper Collins Publishers, 2019, p 59.
[5] Brigadier-General David Anderson, "How We Fight", 20 February 2020, presented to the Joint Command and Staff Programme serial 46 at the Canadian Force College, slide 14.



As you can see, the actions depicted in the Grey Zone are modernized actions that have occurred throughout human history. Most, such as sabotage, information operations, and civil disorder, have not changed at all, though the methods to encourage or discourage them have. The CAF is not alone in its assessment that a Grey Zone future is already here. McFate, who lectures at the National Defence University of the US Military, describes what he calls "durable disorder", the permanence of the uncertainty that faces the world today. This is best illustrated when comparing two of human histories most well known writers on the art of war; Clausewitz and Sun Tzu. McFate, who quotes John Boyd, another well known military theorist states that Clausewitz worked to lift the fog of war, allowing militaries to fight more effectively with clear information while Sun Tzu preached the opposite. Sun Tzu stated that the fog of war should be encouraged and used to one's advantage.[6]

[6] R. Jordan Prescott, "Goodbye Conventional War. It's Been Fun", *Modern War Institute at West Point*, accessed 25 March 2020, https://mwi.usma.edu/goodbye-conventional-war-fun/

The Last "Real" War

The last time the US won a conventional war was perhaps the brief 1991 Gulf War or the 1982 Falklands War, but more likely it was World War II (WWII). This was the last time the US participated in massive land, air, sea, and special operations battles that were largely clear cut and definable. There were clearly two major participants, the Allies and the Axis powers, their soldiers (for the most part) were clearly identifiable, and although war crimes certainly occurred, they were generally attributable to one side or the other. However, this was by and large the last time a conventional, large scale war was won by the US or the West in general. Korea was a bloody standstill, Vietnam was an outright loss, and the Balkan and African wars/peacekeeping efforts of the 1990s mainly a stalemate or failure. The Falklands was a small glimmer of hope that conventional wars were still possible, but the relatively small scale of the conflict made it an exception, not the rule. Even modern day conflicts in Africa are largely against tribal or ideological militias; poorly run African militaries have had little success and former world powers such as France are struggling to achieve their aims. The major conflicts of the post 911 era have been mostly unconventional at the start; both Afghanistan and Iraq started with small special operations teams, local militias, and overwhelming US air power. Both eventually turned into conventional efforts to tackle unconventional problems and the results are plain to see. Syria was, and largely remains for the US, a special operations fight, though the rationale for this seems to be one of avoiding the decisive, and generally long term, engagement of its conventional forces versus a genuine desire to make good. The 2010 US, then North Atlantic Treaty Organization (NATO), adventure to Libya tried to avoid the use of conventional land forces altogether, resulting in a country that is arguably worse off now than under its previous dictator government. Whatever one calls the quagmires of Afghanistan, Libya, Syria, and Iraq, it is clear the methods used against the US in these theatres were largely in the Grey Zone spectrum of conflict.

Our Principal Adversaries and Conventional Arms

Despite this return to Grey Zone methods of war, many of our principle adversaries today are continuing to prepare for a conventional fight. But is this merely hedging their bets in case of a conventional conflict? This point is well highlighted in China's latest Defence White Paper of 2019 which clearly points out that China sees itself competing with the US as co-global superpowers. This White Paper portrayed the Chinese position as a counter balance to the US, which was characterized by American unilateral policies that threatened open conflict and increased defence and economic competition, possibly leading to global war.[7] This White Paper further described the Chinese military buildup as wholly defensive, designed purely to counter the threats posed by the US and its allies in Asia (Taiwan, South Korea, Japan, Taiwan to name a few). The White Paper placed significant emphasis on the South China Sea, which China saw as its own, and actions such as Freedom of Navigation and reconnaissance flights in international waters and airspace (but right on the Chinese border) as escalating threats from the US and its allies. The White Paper also highlighted the expansion of Chinese joint forces (air, sea, land, rocket/nuclear, cyber, information, and space) to both protect the homeland, in the South and East China Seas as well as land and air borders, but also project power, primarily through naval assets into the Western Pacific and East Africa/Middle East through their new base in Djibouti.[8]

Similarly, Russia has conducted a massive rebuild of its military capabilities and capacities starting in the mid 2000s during the Second Chechen War. This brutal, and likely criminal from an Law of Armed Conflict perspective, campaign nonetheless brought stability to the region and was a key turning point in revitalizing Russian military pride.[9] This victory,

[7] Anthony H. Cordesman, "China's New 2019 Defence White Paper: An Open Strategic Challenge to the United States, But One Which Does Not Have to Lead to Conflict", *Center for Strategic and International Studies,* accessed 26 March 2020, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190724_China_2019_Defense.pdf
[8] Ibid.
[9] Rene De La Padraja, *The Russian Military Resurgence: Post-Soviet Decline and Rebuilding, 1992-2018*, McFarland & Company Incorporated Publishers, North Carolina, 2018, p 167.

grudgingly acknowledged by the West and much touted within Russia, proved to be a springboard for a widespread revival of Russian Military Institutions. Dale R. Herspring stated, "Problems are everywhere - personnel, weapons, equipment, Chechnya - the list goes on and on. Nevertheless by 2006 the situation in the armed forces was more structured and stable than it had been under Yeltsin" as improvements across the military began within one year.[10] The Georgian invasion of South Ossetia in 2007 and the Russian removal of them proved even more vital a turning point for the Russian military, despite a near loss at the Second Battle of Tskhinvali, as victories started to accumulate. One of the initial and most effective institution changes was the reduction of Russian Military districts from 16 in the Soviet days, to eight in 1991, to six in 2001, and then finally to four in 2010; this reduction in headquarters, combined with the creation of true joint commands within the four remaining districts, allowed the Russian military to streamline and at the same time increased their ability to coordinate across services to a level never seen before.[11] The Russian military also made significant efforts to professionalize their force; conscripts now compose not more than 30% of the total force, a professional non-commissioned officer (NCO) corps has been created, and a swath of modern combat platforms, for all services, has slowly come to fruition.[12] Overall, it seems both Russia and China are hedging their bets on a future conventional conflict and preparing accordingly.

The World Has Moved On

Despite these conventional force buildups, Russia and China today continue to be some of the most prolific users of Grey Zone methodologies around the world to achieve national aims. In stark contrast, the US (and West in general) appear to have either forgotten, or is unwilling to use these methods to fight back. In the 75 years since the end of WWII, the

[10] Ibid, p 171.
[11] Ibid, p 222.
[12] Ibid, p 225-227.

rest of the world has clearly moved on from conventional warfare, while the West seems fixated on its usage of large standing militaries despite wildly successful small and secretive special operations missions of its own that have resulted in the elimination of some of the terrorist threats around the globe; actions which could be considered in the Grey Zone or very close to it.

The remainder of this paper is focussed on the use of Grey Zone methodologies by our principal adversaries to include the use of ambiguous and non-attributable forces, the use of information as a weapon, and widespread forms of economic coercion to achieve what used to be purely military objectives. This will ultimately serve to highlight how the principal adversaries of the US and the West believe they are already in war, and how they are winning.

Ambiguous and Non-Attributable Forces

The use of ambiguous or non-attributable forces to conduct operations are not a new concept. In modern war, these operations have generally been the realm of special operations forces or civilian agencies such as the US Central Intelligence Agency or the Soviet era KGB. However, Russia has expanded this concept and used ambiguous forces (based to a great extent on conventional Russian Army troops and various units of the Russian Special Forces) to great success in its illegal annexation of the Crimea and the Donbas Region from Ukraine.[13] This event saw these non-attributable forces, assisting local insurgents and pro-Russian militias inside Ukraine, stage a rapid and effective takeover of Crimea and the Donbas within weeks. All the while, Russia claimed to have no knowledge of these "little green men", so called because they wore green uniforms with no identification markings, though they would eventually be discovered to be Russian military troops.[14] These weeks of

[13] Tor Bukkvoll, "Russian Special Forces in Crimea and Donbas", *Parameters*, vol. 6, iss. 2, 2016.
[14] Mehmet Seyfettin Erol and Safak Oguz, "Hybrid Warfare Studies and Russia's Example in Crimea", *Gazi Akademik Bakis Dergisi*, vol. 9, no. 17, 2015.

denials on the nationality of these "little green men" provided critical time for Russian troops and Russian backed insurgents to completely occupy Eastern Ukraine. By the time identifiable Russian conventional forces became involved in the conflict, it was truly *fait accompli*; Russian conventional forces merely followed the "non-linear warfare" strategy put forward by then Chief of the General Staff, Valeriy Gerasimov, and delivered the death blow to Crimea and Donbas.[15] In this example, Russia radically changed the understanding of "hybrid warfare"; they effectively used ambiguous (insurgents and militias) and initially non-attributable forces ("little green men") against a weaker opponent to avoid a larger conventional fight, expressly with the purpose of isolating that opponent (Ukraine) and preventing the participation of a larger, stronger one (US and NATO). Overall, this has proven to be a successful operation for Russia, giving it greater control of the Black Sea as well military bases in the Eastern Ukraine. Most importantly, it has showcased to the world, and the US in particular, that it is once again a competitor in the global arena.

However, the Russian use of non-attributable forces in Ukraine is only one of the most recent examples of this type of warfare. For centuries the Middle East has been a hotbed of violence, often based on religious ideology, and non-attributable forces have run rampant there. The group Hizballah and its Iranian backers is one of the best examples of non-attributable proxies at work. Based on Shi'a Islam, Hizballah consistently and effectively stirs disorder and discontent in the surrounding area which are either Jewish or prodominantly Sunni Muslim.[16] Although Hezbollah is not believed to be operating at the behest or direction of the Iranian government, the financial aid and weapons shipments from Iran certainly help and strongly influence the actions of this Lebanon based terror group.[17] This loose affiliation had allowed the Iranian government to, at times, deny successfully any knowledge of

[15] Ibid.
[16] Graham E. Fuller, "The Hizballah-Iran Connection: Model for Sunni Resistance", *The Washington Quarterly*, vol. 30, iss. 1, 2007, p 139
[17] Ibid, p 142.

Hezbollah actions, even if they promote the interests of Shi'a Muslims which is Iran's ultimate goal. These plausibly deniable Hezbollah actions further cause chaos and confusion throughout the Middle East, allowing Iran to further its own goal of challenging the US agenda for the region while simultaneously attempting to destabilize Saudi Arabia as the current regional powerhouse.[18] In the last decade, these actions have expanded greatly and Hezbollah is now deeply involved in the conflicts in Iraq, Syria, and even Yemen.[19] Despite not being under direct Iranian control, Hezbollah as an ambiguous force, often not directly traceable to Iranian leadership, and continues to create havoc in the region and serves as a way for Iran to discreetly wage a shadow war on Israel, the US, and Sunni Muslims in the region.

The use of ambiguous or non-attributable forces is no longer limited to the physical domain. The last several decades have seen the increasing use of non-attributable cyber attacks as a means of gaining advantage over others and this is now commonplace. A perfect example of this was the US-Israeli 2010 Stuxnet cyber worm that had struck an Iranian nuclear facility, infecting over 60,000 computers, and retarding the Iranian nuclear program for some time.[20] Other recent examples include Chinese orchestrated Ghostnet and Shadow cyber attacks against Tibetan exiles living abroad and Russian cyber shutdowns against Georgian official websites and media outlets.[21] Though in all three cases, the perpetrators were eventually discovered, all countries deny their involvement officially and repeatedly, making proof beyond any doubt very difficult. This proved to be a cornerstone of the Chinese military revolution in their concept of joint operations. Cyber and Information were acknowledged to be just as vital as land, sea, air, and nuclear forces and the "jointness" of all

[18] Ibid, p 247-148.
[19] Margaret Besheer, *UN Ambassador to UN Takes Aim at Iran, Hezbollah*, Washington: Federal Information and News Dispatch Inc, 2017. Accessed 27 March 2020 https://search-proquest-com.cfc.idm.oclc.org/docview/1889865390?accountid=9867
[20] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, vol. 53, iss. 1, 2011.
[21] Ibid.

future conflicts is not part of the Chinese military doctrine.[22] The frequency of attacks conducted by our principal adversaries also demonstrate that they are increasing using this form of Grey Zone warfare to achieve their national aims; it is generally non-attributable (at least initially and always officially), it is cheaper than conventional military methods to achieve the same aim, and has so far proven to avoid conventional conflict altogether.

Information War

Hand in hand with the expansive use of cyber warfare is the widespread importance placed on information warfare and controlling the narrative. Russia in particular has proven itself capable and willing to lie on an industrial scale. During the height of the Russian campaign to annex Crimea and the Donbas, their manipulation of information to suit their needs and their control of what information was released was described by General Phillip Breedlove, then Supreme Allied Commander Europe, as, "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare".[23] This ability to wage a campaign to essentially steal part of another sovereign country can be described, in Russian nomenclature, as "non-linear" warfare. The integration of the use of "little green men" combined with exquisite control of information is what allowed Russia to win in Crimea and Donbas.[24]

But what exactly has changed in the Russian military? For years, Russian forces have placed emphasis on quantity and overwhelming use of firepower and brute force to achieve its aims. The changes really began in the early 2000s, when Vladimir Putin introduced significant reforms in the Russian military, aimed at challenging and defeating technologically superior adversaries such as the US and NATO. One of these many reforms was the idea that information was now the primary driver of military operations while

---

[22] Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations,* Praeger Publishing, California and Colorado, 2017, p 33-36.
[23] John Vandiver, "SACEUR: Allies Must Prepare for "Hybrid War" ", *Stars and Stripes*, 4 September 2014. Accessed 30 March 2020. https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464
[24] Rod Thornton, "The Changing Nature of Modern Warfare", *The RUSI Journal,* vol. 160, iss. 4, 2015.

moving conventional application of force into a supporting role.[25] Analyst Janis Berzins describes this new Russian perspective as aiming to create multiple versions of reality, through television, internet websites, social media and any other available means, that suit the political and military purposes of the Russian military and government to achieve its aims.[26] This was certainly the case during the early days of the Crimea/Donbas annexation, as Russian misinformation, manipulation of narrative, and outright denials not only sowed confusion in the West, but led to fear and confusion in the populace of Eastern Ukraine while driving patriotism at home to new highs.

Though the near-term goals may have been the annexation of new territories, Russia also managed to prevent large scale conflict with the US and NATO through this method of non-linear warfare. This idea of a "contactless war" allows Russia to achieve its national aims while avoiding conventional fights with the US and NATO. The genius of this strategy is to turn US/NATO strengths, primarily its technological advantage, into a weakness, by denying the US and NATO the information required to legally and justifiably apply that force.[27] Given the success of the Russian annexation of Crimea and Donbas, it is likely that this new method of war will be Russia's primary methodology for the foreseeable future.

Another of the West's principal adversaries that is no stranger to information warfare is China. For decades, the Chinese Communist Party (CCP) has controlled Chinese media, both government owned and China based, in an effort to write its own narrative. In fact, few subjects in the Chinese military receive as much focus as Information Warfare. Though the first Chinese book on information warfare was written in 1985, it was not until the 1991 Gulf War that the People's Liberation Army (PLA), essentially the Chinese military at large, gave it serious thought. In the years since, the PLA has focused its information warfare efforts at

---

[25] Ibid.
[26] Janis Berzins, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy*, 2014. Accessed 30 March 2020. https://www.semanticscholar.org/paper/Russia's-New-Generation-Warfare-in-Ukraine%3A-for-Bērziņš/20509c9769cfc7920908f7b7e959ecdfd43ca2f4#paper-header
[27] Rod Thornton, "The Changing Nature of Modern Warfare"...

the enemy's ability to obtain reliable information, process that information correctly, and then use that information to make timely decisions.[28] This has proven to be in lockstep with wider Chinese governmental efforts to control the narrative.

This Chinese whole of government effort can be described as "anti-head" and "anti-neck" operations; terms meaning attacks to target either leadership or subordinates by dislocating them from the flow of proper of accurate and timely information.[29] In the case of China, they are not averse to using malware methods to collect and disseminate information, against their adversaries or their own populace. This has proven to be a key tool in both industrial and political espionage efforts against the US and the West, and in their monitoring of their own population for purposes of information collection.[30] This has been particularly easy for the Chinese to conduct for two reasons; first, computer networks, cell phone systems, and both traditional and social media platforms in China are controlled by the government. Second, in the US and the West, these same systems are largely vulnerable as they are in the care and control of private companies.Though this concern from the US side was evident as early 1999 in then Deputy Secretary of Defence John Hamre's testimony before the Senate Armed Services Committee, very little was done to change it.[31] This lack of protection would come home to roost on multiple occasions over the next decades as Chinese hackers exploited one of the strengths of the West, open access to information, and conducted repeated attempts to either industrial, political, and economic espionage or attempted to outright change public opinion in the West and the US. A perfect example would be the Chinese attempt to unduly influence the 2016 US Presidential election through an information warfare campaign. Though largely acknowledged as part of great power

[28] Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare*, US Army War College, Pennsylvania, March 2014, p 3.
[29] Dennis F Poindexter, *The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interest, 2nd Ed,* McFarland and Company Incorporated Publishers, 2018, p 21.
[30] M.E. Kabay, "Chinese Information Warfare Capabilities: Analysis of China's Information Warfare Capabilities and Techniques", *Network World (Online)*, 7 April 2009.
[31] Vincent Wei-Cheng Wang and Gwendolyn Stamper, "Asymmetric War? Implications for China's Information Warfare Strategies", *American Asian Review,* vol. 20, iss. 4, 2002.

"competition", the US failed to grasp the seriousness of the issue. As early as 2006, Chinese President Hu Jintao declared that China must, "strengthen the construction of foreign-related media and networks" that "promote China" and called for innovation in "foreign propaganda methods" with the goal of allowing China to influence foreign populations.[32] The Chinese take the use of information warfare a step future by complementing it with other forms of coercion through both attributable and non-attributable agents.

Economic Coercion

Of all the Grey Zone methods described in this paper, economic coercion may well be the oldest and most effective. The Chinese in particular have continued its use and is today one of the prolific lenders of money to other states. China's huge population means it is, at the same time, a global powerhouse in terms of production and exportation of goods, but also a major importer and consumer of goods produced in other countries. China has used these realities to its advantage continuously and repeatedly.

The December 2018 arrest of Huawei executive Mung Wanzhou by Canada, at the request of the US, caused a significant disruption in Canada-China relations. China reacted angrily and then moved to slap either large tariffs or outright bans on several key Canadian products such as canola, soy beans, and pork from entering China. These economic actions form what can be called economic coercion in a Chinese attempt to change Canadian behaviour.[33] In fact, these actions led to not only concerns from within the Canadian farming and cattle raising communities, it required changes by the Canadian federal government to assist these producers and brought up friction points between Canadian and US authorities who had called for Meng's arrest and then failed to provide adequate reasons for it. This

[32] Rush Doshi and Robert D. Williams, "Is China Interfering in American Politics", *Brookings Institute*, accessed 30 March 2020. https://www.brookings.edu/blog/order-from-chaos/2018/10/02/is-china-interfering-in-american-politics/
[33] Chen Duanjie, "Countering China's Economic Coercion: No Fear But Resolve, No Illusion but Diversification", *MacDonal-Laurier Institute for Public Policy,* Ottawa, 2019.

confusion was needless to say beneficial for China as it used the resulting fog of confusion and frustration to expand its influence into the Canadian and US populace.

However, Chinese economic coercion has gone much further than state to state trade policies and China has been well known to coerce other non-state actors for geopolitical and economic gain.[34] US analyst Dan Blumenthal stated, "China is back to being run by state-owned enterprises that are related to the Party. The private sector is diminishing. That provides the Chinese state with a lot more control of economic coercive policies".[35] Another analyst, Ely Ratner, speaking at the same Senate Foreign Relations Committee hearing as Blumenthal, stated that China has been using economic coercion tactics against the US and others for over 20 years with the expressed goal of isolating and dividing American allies against each other to increase China's own geopolitical clout.[36] The two analysts, Blumenthal and Ratner both argue that China has been eating the West's lunch for years, because we have allowed them to. China has been engaged directly with Western business leaders to adopt pro-China, or at least China friendly, policies as a precondition of doing business with 1.4 billion people living in China.[37] This has led directly to increased profits for these large multinationals, but has also resulted in a pool of influential businesses with leaders hesitant to disrupt that arrangement by speaking against the official Chinese position on a variety of subjects.

Even more disturbing than influencing multinational companies is the Chinese use of its Belt and Road Initiative (BRI) as a means to coerce entire states in areas beyond trade and commerce. Called an "economic pie that brings real benefits to all parties" by the Chinese Foreign Minister Wang Yi, the BRI is nothing more than an economic debt trap designed to

[34] Huong Le Thu, "China's Dual Strategy of Coercion and Inducement Towards ASEAN", *The Pacific Review*, vol. 32, iss. 1, 2019.
[35] Bonnie Girard, "The US Senate Considers China's Economic Coercion" *The Diplomat*, 30 July 2018.
[36] Ibid.
[37] Ibid.

influence smaller, poorer states.[38] Examples such as the built by, and subsequent lease to, China of the Sri Lankan port of Hambantota, the China-Pakistan Economic Corridor, a system of road, rail, and pipelines, and the establishment of China's first overseas military base in Djibouti. All were the result of debt repayment failures under the BRI. However, the BRI is expanding and Western Allies such as Greece, Poland, Hungary, Portugal, and Italy have now signed on to receive Chinese monies to develop needed infrastructure. If recent history regarding the BRI holds true, then these projects will likely be beneficial to both the host nation, and more importantly to China, once finished. These projects will also provide leverage for China to use over these host nations.[39]

The West Must Change, Adopt, or Perish

Relative to the history of the human race, the world appears to be in a state of unparalleled peace. However, we should not take that at face value. Advancements in technology have not only shrunk our world, it has made it interconnected at near instantaneous speeds. This has led directly to a war between the globally recognized hegemon, the US (and her Allies) and the principal adversaries that would challenge the international rules based order (Russia, China, and Iran). The decline of major wars has led to smaller, regional ones and this has resulted in the rise of ambiguous and non-attributable forces fighting on behalf of governments, organizations and even private citizens. The speed of information travel has become weaponized, and controlling the narrative is now often the primary factor in winning or losing. The global economic commons and interdependencies that it entails has also connected us in ways never before possible. This has led to significant gaps in financial and economic prosperity and the occurrence of economic coercion between states is now evident.

[38] Didi Tand and Tom Kington, "Xi's Ambition Condemned as a 'Predatory Network of Coercion' ", *The Times*, London, UK, 21 March 2019.
[39] Ibid.

The rise of smaller regional wars has also not removed the need for global superpowers, and those aspiring to become superpowers, from conducting their own "contactless wars" but are actually enabling it.[40] These phenomena are the true future of large scale global conflict as the Grey Zone tactics used by our principal adversaries reap outsized returns from relatively small conflicts. The world over, Russian, China, and Iran are using below the threshold of war methods to achieve their national aims, winning the war that the US and the West doesn't realize it is already fighting. The Grey Zone is truly a rapidly evaporating space that encompasses peace, war, competition, and the entire spectrum in between.

None of these methods are new and most harken back to the medieval era, or even earlier. What is different today is that only our principal adversaries seem to be playing by these new rules. The US and her Allies seem intent on the use of conventional methods for these unconventional threats; by the time we realize what is happening, it may already be too late.

[40] Vincent Wei-Cheng Wang and Gwendolyn Stamper, "Asymmetric War"...

BIBLIOGRAPHY

Anderson, Brigadier-General David, "How We Fight", 20 February 2020, presented to the Joint Command and Staff Programme serial 46 at the Canadian Force College, slide 14.

Berzins, Janis, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy* (2014). Accessed 30 March 2020. https://www.semanticscholar.org/paper/Russia's-New-Generation-Warfare-in-Ukraine%3A-for-Bērziņš/20509c9769cfc7920908f7b7e959ecdfd43ca2f4#paper-header

Besheer, Margaret, *UN Ambassador to UN Takes Aim at Iran, Hezbollah*, Washington: Federal Information and News Dispatch Inc (2017). Accessed 27 March 2020 https://search-proquest-com.cfc.idm.oclc.org/docview/1889865390?accountid=9867

Brooks, Rosa, "Rule of Law in the Grey Zone", *Modern War Institute at West Point* (2 July 2018). Accessed 24 March 2020, https://mwi.usma.edu/rule-law-grey-zone/

Bukkvoll, Tor, "Russian Special Forces in Crimea and Donbas", *Parameters*, vol. 6, iss. 2 (2016) 13-21.

Cheng, Dean, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger Publishing, California and Colorado (2017).

Cordesman, Anthony H., "China's New 2019 Defence White Paper: An Open Strategic Challenge to the United States, But One Which Does Not Have to Lead to Conflict", *Center for Strategic and International Studies*, accessed 26 March 2020, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190724_China_2019_Defense.pdf

De La Padraja, Rene, *The Russian Military Resurgence: Post-Soviet Decline and Rebuilding, 1992-2018*, McFarland & Company Incorporated Publishers, North Carolina (2018).

Doshi, Rush and Robert D. Williams, "Is China Interfering in American Politics", *Brookings Institute*, accessed 30 March 2020. https://www.brookings.edu/blog/order-from-chaos/2018/10/02/is-china-interfering-in-american-politics/

Duanjie, Chen, "Countering China's Economic Coercion: No Fear But Resolve, No Illusion but Diversification", *MacDonal-Laurier Institute for Public Policy*, Ottawa (2019).

Farwell, James P. and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival,* vol. 53, iss. 1 (2011).

Fuller, Graham E., "The Hizballah-Iran Connection: Model for Sunni Resistance", *The Washington Quarterly*, vol. 30, iss. 1, (2007), 139-150.

Girard, Bonnie, "The US Senate Considers China's Economic Coercion" *The Diplomat*, 30 July 2018.

Kabay, M.E., "Chinese Information Warfare Capabilities: Analysis of China's Information Warfare Capabilities and Techniques", *Network World (Online)* (7 April 2009).

McFate, Sean, *The New Rules of War; How America Can Win - Against, Russia, China, and Other Threats*, William Morrow/Harper Collins Publishers (2019).

Poindexter, Dennis F, *The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interest, 2nd Ed,* McFarland and Company Incorporated Publishers (2018).

Prescott, R. Jordan, "Goodbye Conventional War. It's Been Fun", *Modern War Institute at West Point,* accessed 25 March 2020, https://mwi.usma.edu/goodbye-conventional-war-fun/

Seyfettin Erol, Mehmet and Safak Oguz, "Hybrid Warfare Studies and Russia's Example in Crimea", *Gazi Akademik Bakis Dergisi*, vol. 9, no. 17, (2015), 261-277.

Tand, Didi and Tom Kington, "Xi's Ambition Condemned as a 'Predatory Network of Coercion' ", *The Times*, London, UK, 21 March 2019.

Thornton, Rod, "The Changing Nature of Modern Warfare", *The RUSI Journal,* vol. 160, iss. 4 (2015), 40-48.

Thu, Huong Le, "China's Dual Strategy of Coercion and Inducement Towards ASEAN", *The Pacific Review*, vol. 32, iss. 1 (2019), 20-36.

Vandiver, John, "SACEUR: Allies Must Prepare for "Hybrid War"", *Stars and Stripes* (4 September 2014). Accessed 30 March 2020. https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464

Wang, Vincent Wei-Cheng and Gwendolyn Stamper, "Asymmetric War? Implications for China's Information Warfare Strategies", *American Asian Review,* vol. 20, iss. 4 (2002), 167-207.

Wortzel, Larry M., *The Chinese People's Liberation Army and Information Warfare*, US Army War College, Pennsylvania (March 2014).