The Secret War Against the United States

The Top Threat to National Security and the American Dream

Cyber and Asymmetrical Hybrid Warfare

An Urgent Call to Action

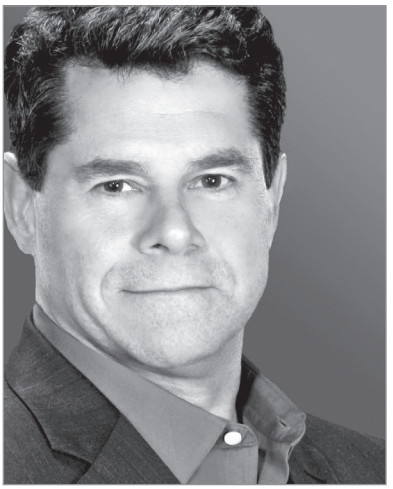
T. Casey Fleming
Eric L. Qualkenbush
Anthony M. Chapa

ABSTRACT

Imagine if Pearl Harbor had been attacked and there had been no response from Washington.

This is the actual case today due to a highly sophisticated, mature, and stealth strategy perpetrated against the United States (US) by advanced military methods leveled at every sector and organization in our society. This includes private sector businesses, all government agencies, the military, and academia—every US organization operating with innovation, intellectual property, or sensitive data. The world is in significant conflict requiring the US government, military, and private sector to deliberately confront this national crisis or become permanently irrelevant. It is no longer "business as usual."

Over the past three decades, as the US military trained in conventional, nuclear, and counterinsurgency warfare, the Chinese Communist Party (CCP) engaged and perfected over forty methods of warfare intended to permanently destabilize and weaken the US both economically and militarily. At the same time, China rapidly grew its economy and military without the required time or investment in innovation. The result is that the US is hemorrhaging its economic strength and relevance at the rate of $5 trillion in lost total value each year, or one-third of the U.S. Gross Domestic Product (GDP). General (Ret.) Keith Alexander, former Director of the National



T. Casey Fleming serves as Chairman and Chief Executive Officer of BLACKOPS Partners Corporation, the leading intelligence, think tank, cybersecurity and asymmetrical hybrid warfare advisors to senior leadership of the world's largest organizations. He regularly advises the private sector, governments, agencies, military, Congress, and academia. Mr. Fleming is widely recognized as a top thought-leader, expert, and speaker in the areas of intelligence, national security, cybersecurity, and asymmetrical hybrid warfare. The Cybersecurity Excellence Awards recently named him *Cybersecurity Professional of the Year.* Mr. Fleming previously led organizations for IBM Corporation, Deloitte Consulting, and Good Technology. He served as the founding managing director of IBM's successful Cyber division, known today as IBM Security. Mr. Fleming earned his Bachelor of Science degree from Texas A&M University and participated in executive programs at Harvard Business School and The Wharton School.

Security Agency (NSA) and Commander of U.S. Cyber Command, referred to China's theft of American innovation and intellectual property as "the greatest transfer of wealth in history." Over time, a weakened US economy directly reduces the strength and effectiveness of the US military. Further, when a country is manipulated by an adversary to lose one-third of the value of its economy each year, it is at war.

ASYMMETRICAL HYBRID WARFARE

Clear and Present Existential Threat

Over the past thirty years, the US government and private sector have advanced their policy of full-cooperation, including substantial financial and technological investment in China, under the belief that they were moving towards a more democratic, free-market society while China played intentional misdirection and deception. In 1986, month number three, the Communist Party of China (CCP) officially declared Asymmetrical Hybrid Warfare (AHW) against the US and its western allies in its nation-state *Program 863.* This strategy commits all of China with its strict Communist military rule to engage in any and all methods to become on par with, surpass, and dominate the West at any and all cost. China's ultimate objective is to harvest and perpetuate the *Chinese Dream* through the extraction and extinguishing of the *American Dream,* the American way of life and ending Western dominance. The Chinese strategy is that after 200 years of Western global dominance, it is their destiny to reverse roles with the US and to relegate it to a forced supplier with a much lower quality of life. To underscore this strategy, China refers to the last century as "the century of great humiliation." It must also be emphasized that AHW strategy is rooted in Unrestricted Warfare or "war without rules."

Eric L. Qualkenbush is a member of the Board of Directors of BLACKOPS Partners Corporation. Mr. Qualkenbush is a former intelligence community senior executive with extensive experience leading large multicultural organizations through transformational change. He is an innovator who has created organization and programs that deal with the worldwide proliferation of weapons of mass destruction, insider threat, espionage mitigation, and competitive intelligence. During his CIA career, he led the CIA's principal training organization and the office that created and managed cover arrangements for all CIA personnel and others in the US government. Mr. Qualkenbush also managed undercover CIA operations in five overseas offices in the Middle East, and in Western and Eastern Europe. He also led pioneering work on mitigating insider threats in both private and public organizations.

DEATH BY A THOUSAND CUTS

The Modern Battlefield is Everywhere

AHW has been established as the future of modern warfare and business strategy across the globe. It is ultimate warfare that has many forms: economic warfare, transaction warfare, industrial warfare, drug warfare, and propaganda warfare, to name only a few. Each method is characterized by the non-utilization of military or conventional warfare that is typical of aircraft, ships, troops, and weapons. While China continues to aggressively develop and expand its military, it does so with the belief that if it must resort to the use of conventional or nuclear warfare, it has ultimately failed at achieving the enemy's capitulation through the combined methods of AHW. In the business sector, AHW has become the *"New Global Competitive Model"* where the "winner takes all." Soon, China will dictate transactions and pricing based on its market dominance. As businesses rush to move to "digital transformation" and "Big Data," each must perform a 180° cybersecurity transformation based on sensitive data protection and adversarial motives as a means to survive. Currently, AHW is the primary focus of our adversaries: China is, by far, the most successful at methodically executing all AHW methods, while Russia, North Korea, Iran, and India engage in relatively few methods at present. The strategy is to continuously inflict damage or cuts to every facet of American society just below the pain threshold where we choose not to act. We believe that China has achieved an estimated 750 cuts towards "death by a thousand cuts." *(Sun Tzu)*

Definition

AHW is characterized as unconventional, non-military, multi-method strategic warfare that is based

Anthony M. Chapa is a member of the Board of Directors of BLACKOPS Partners Corporation. Mr. Chapa is the CEO of Chapa Concepts, which provides threat and technology assessment for leading advanced technology and public sector organizations. Chapa Concepts also provides strategy and operational support to biometric access, security technology, and communications firms. Mr. Chapa retired from the United States Secret Service (USSS), Department of Homeland Security after a highly successful career, including Assistant Director and Chief Technology Officer responsible for the Technical Security Division. Mr. Chapa also served as Special Agent in Charge of the Los Angeles field office including leadership over the nation's premier USSS Electronic Crimes Task Force (ECTF). Mr. Chapa earned his Bachelor of Arts and Master of Arts in Political Science from St. Mary's University.

on deception and void of any rules between countries where economic and military power, strategy and tactics differ significantly. The attacking country exploits inherent weaknesses through numerous uneven and seemingly unrelated AHW methods that are designed to destabilize the unwitting target country for ultimate and complete economic and military submission. Extensive use of misinformation and plausible deniability are used to deceive and deflect suspicion of the strategy or its methodical advancement. Hybrid warfare is a military strategy that blends conventional warfare, asymmetric warfare, irregular warfare, offset warfare, non-linear warfare, and cyber warfare. AHW is rooted in unrestricted warfare (war without rules where "everything is fair play") which is also described as "anything warfare." *Source: BLACKOPS Partners Corporation–See Figure 1.*

Culture Disparity as a Strategic Weapon

It is important to note the striking contrast between the two cultures of the US and Communist China. It is this great divide that has contributed to China's manipulation and acceleration of AHW against the US. The CCP believes its "legalism" philosophy of supreme law and people are superior to America's constitutional democracy underpinned by justice, religion, a Creator, and "all men are created equal." Since 1949, the CCP have controlled all aspects of China's commerce, military, and daily life where intellectual property is state-owned, all data is controlled, and it is the national duty of all citizens to support the regime, including all aspects of espionage. The Communist culture is further defined not by "winning vs. losing"; rather, *"living vs. dying."* It is this extreme belief that underscores China's support for AHW in its conflict with the US. Another distinction is that the CCP controls every business transaction with US companies. In many

cases, the CCP resembles a powerful organized crime faction, through its shell business partnerships and facades. There is no distinction between China's organized crime, military, or government. This places every US business partnership or transaction with China at extreme risk.

Critical Role of Intelligence

China's uncompromising commitment to AHW demonstrates a national objective to destroy the US and its Western allies. The critical nucleus that drives the AHW strategy is the complete dependence on stolen innovation, intellectual property (IP), sensitive data, and military secrets—namely intelligence. For over thirty years, China has orchestrated the most impressive and sophisticated strategy with an intricate global network of espionage and industrial theft to fuel AHW. In recent years, an emboldened China has demanded the complete surrender of all intellectual property during the process of contracting current international business transactions. Conversely, intelligence plays a critical role for the US to gauge the executional success of AHW, changes in strategy, and individual and cumulative damages.

Cyber Warfare as the Key Accelerator

China has successfully intertwined Cyber warfare as the key AHW accelerator due to its relatively minimal investment and the difficulty of attributing actions to a specific actor. At the same time, cybersecurity remains fundamentally broken in the US and the West due to failed cyber strategies, lack of awareness of AHW, lack of accountability, overconfidence, and overdependence on inherently fallible cybersecurity products. This is made clear by the "new normal" of the increased trend in number, frequency, and resulting total damages from cyberattacks.

Current estimates place global cyber losses at $6 trillion by 2021, with expectations that this will increase further in the future, according to Cybersecurity Ventures. Cyber warfare and cybersecurity have become a "whole of society" challenge that requires a unified, elevated strategy and 180° approach to combat the morphing threat. As we examine today's cybersecurity environment, we are looking through the wrong end of the telescope. It is only in the context of AHW that we can begin to fully understand cybersecurity's critical role for successful defense, protection, and resolution. We have learned to treat cybersecurity first and foremost as a human problem and a senior leadership challenge, not solely an IT issue.

Call to Action

The US must immediately increase awareness, positive action, and accountability in all sectors and at all levels through creating a unified and aggressive approach in responding to the advancement and threat of AHW. The following recommendations are put forth:

- Immediately establish the Asymmetrical Hybrid Warfare Center (AHWC)

- Public-Private Partnership Center (P3C) coalition, U.S. university-based with Department of Defense (DoD) participation
- Independent leadership and reporting structure as a resource-focused, support entity charged with maximum efficiency (reporting to the U.S. Executive Branch or U.S. Senate Select Committee on Intelligence)
- Constituents: USG, Pentagon, Congress, private sector, academia, and US Allies
- Mission: strategy, intelligence, counterintelligence, research, tracking, analysis, awareness, training, AHW-countering recommendations to constituents (e.g., foreign acquisition of assets determined to be harmful to US economy or military, false shell companies, espionage reporting database, misinformation generation, spyware)
- Cybersecurity consortium clearinghouse with anonymity scrub: intelligence at a level higher than today with a focus on advanced attack methods for early warning and resolution
- DarkNet research and triangulation, active surveillance as adversaries increasingly exploit this platform
- Regular release of evolving cybersecurity attack methods and best practices
- No organization or entity today is positioned for this center or mission

- Transformational culture change to protect innovation, IP, and cybersecurity sensitive data
- AHW executive briefing and exercise for key US and Allied organizations (government, military, private sector, and academia) to train in AHW strategy, methods, and countering techniques

Summary

The persistent engagement of Asymmetrical Hybrid Warfare (AHW) will continue to grow as the preeminent threat to US national security and will characterize the future focus of each of our adversaries. Asymmetrical/Conventional/Nuclear is the new continuum of modern warfare. The Russian hacking of the 2016 U.S. Presidential election clearly demonstrates the shift of AHW to the forefront and the relative effectiveness of a single act and method. All sectors of US society: private sector economy, the government—especially Congress, military, and academia must increase its awareness of highly advanced AHW, provide accountability, and routinely engage in effective countermeasures to secure and protect the future of the United States.

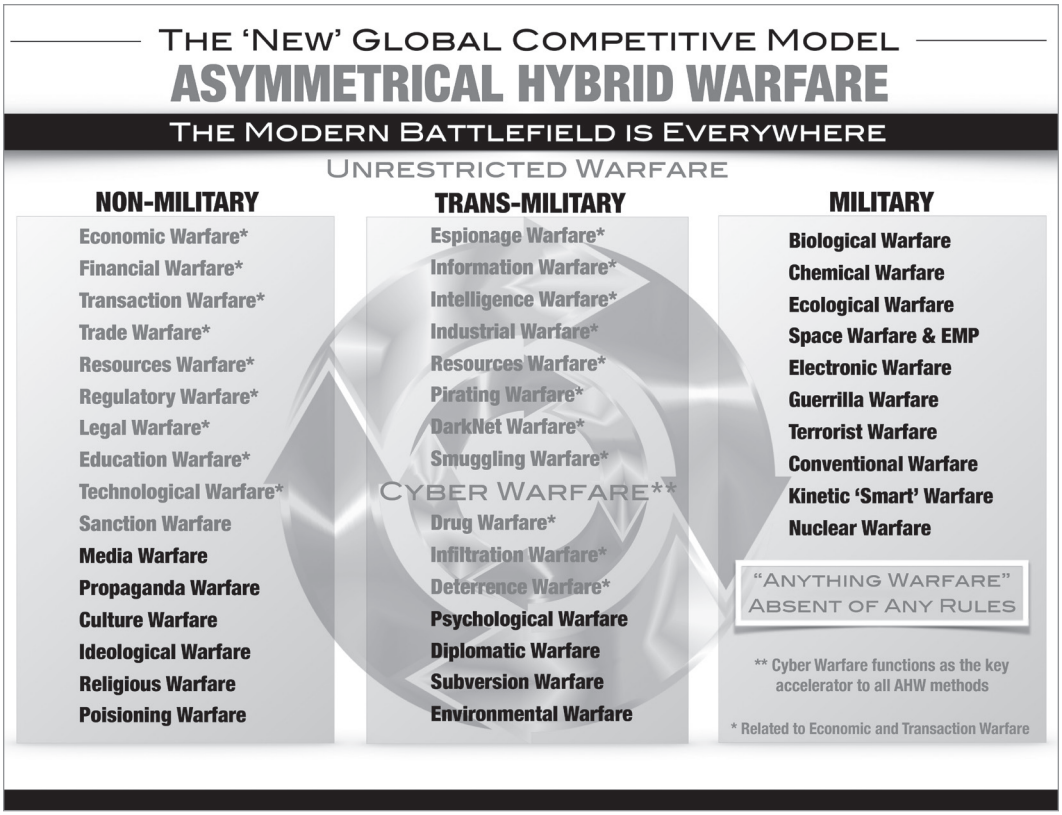


Figure 1. The 'New' Global Competitive Model

The views and opinions expressed in this paper are those of the author(s) alone and do not necessarily reflect the official policy or position of the U.S. Department of Defense (DoD) or any agency of the U.S. Government.