Hybrid Warfare: Are You Prepared?

By Rex M. Lee
03.31.2020

Warfare as we know it has changed forever as the world becomes more connected. The key driver for this change is the "Re-Rise of Great Power Competition" between nation-states such as the United States, the European Union, United Kingdom, Russia, and China governed by Chinese Communist Party, ("CCP").

Secretary of State (U.S.), Mike Pompeo, recently addressed threats and this existential risk to companies associated with Great Power Competition.

Pompeo's message highlighted economic rivalry and competition for global energy markets between the United States, Russia and China during his keynote address where he had this to say:

"*The more we could spread the United States model of free enterprise, of the rule of law, of diversity, stability, transparency in transactions, the more successful the United States will be, the more successful and secure the American people will be…our model matters now, frankly, more than ever in an era of "Great Power Rivalry and Competition" where some nations are using their energy for maligned purposes…*"- Mike Pompeo, Secretary of State, U.S., CERAWeek 2019, March 12th, 2019, Houston, TX

Today, a year later, we see Russia lowering oil prices during the global Corona Virus ("Covid-19") pandemic outbreak creating a price war between OPEC and Russia sending oil prices plummeting as the demand for oil drops because people are ordered by their governments to shelter-in-place due to the virus.

Russia dropping their oil prices during a global pandemic is a great example of what the Secretary of State, Pompeo, was speaking about, pertaining to Great Power Competition.

It is clear that Russian Prime Minister, Valdemar Putin, is using Russia's oil as a weapon of an *alternative form of warfare known as "Hybrid Warfare"* where the modern battlefield is everywhere rather than centered on a traditional battlefield where two mechanized armies engage in war. (see image [GPC slide]).

Figure 1-Hybrid Warfare Threat Landscape*

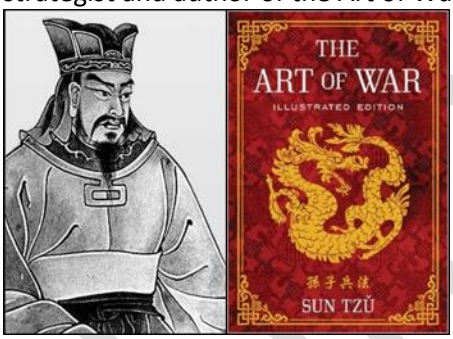
*Source: BlackOps Partners, Washington, DC

We have seen Great Power Competition before regarding competition for resources such as oil which led to the United States entry into World War II when the U.S. embargoed oil keeping Japan from fueling their invasion of China prior to the bombing of Pearl Harbor on Dec 7th, 1941.

"Hybrid Warfare"- The Modern Battlefield is Everywhere

Hybrid Warfare simply means that the modern battlefield is everywhere where and targets include companies, governments, armed forces, and even civilians including adults, teens, children, doctors, lawyers, judges, govt. officials, artists, entertainers and business professionals.

If you never heard of Hybrid Warfare, you may not have read the Art of War by Sun Tzu, Chinese Military strategist and author of the Art of War, 5th century BC.



Hybrid Warfare is not a new concept but a rebranding of the Art of War by Sun Tzu in my opinion, see a quote by Sun Tzu for an example:

- *"The supreme art of war is to subdue the enemy without fighting…The greatest victory is that which requires no battle"*- Sun Tzu, The Art of War

T. Casey Fleming, Chairman and CEO of BlackOps Partners, a think tank, intelligence, and security strategy firm in Washington, DC, gives his definition of Hybrid Warfare as it relates to threats against Western multi-national Corporations who compete against Nation state-controlled corporations from adversarial countries such as China and Russia, regarding Hybrid Warfare:

- *"Achieving military and political objectives through attacking everything short of conventional military methods. Today, companies and their innovation and IP are on the frontlines in the gray zone between peace and war. Adversaries like the Chinese Communist Party are well down the*

> *path of replacing many companies and globally dominating industries and sectors."*- T. Casey Fleming, BLACKOPS Partners, Washington, DC.

Fleming's review of Hybrid Warfare is highly relevant to Secretary of State Mike Pompeo's views on Great Power Competition between U.S. energy producers and energy producers from China and Russia which validates that Russia is currently using their oil as a weapon during a global pandemic today.

Putin's use of oil as a weapon during a global crises such as a pandemic outbreak is a strategy right out of the Art of War.

"Hybrid Warfare"- The Existential Risk to National & Economic Security

Hybrid Warfare presents *a top existential risk* to the national security and the economy of Western allies such as the U.S., U.K., and the E.U. due to the fact that Western countries are reliant on China, an adversary, for the bulk of their supply chains associated with the manufacturing of vital products, medicine, electronics, and technology.

- *"Know your enemy and know yourself and you will always be victorious."*- Sun Tzu, The Art of War

Providing college educations to Chinese nationals while doing business with your adversary, 100% controlled by the Chinese Communist Party ("CCP"), has grave consequences as the United States is finding out during the Covid-19 pandemic.

For example, the fact that the U.S. government, over the years, has made it profitable for U.S. corporations to outsource the manufacturing of many vital goods and services to China gives the President of the People's Republic of China, XI Jinping, leverage over U.S. manufacturers and government when it comes to negotiations.

- *"When you surround an army, leave an outlet free. Do not press a desperate foe too hard."*- Sun Tzu, The Art of War

President, Jinping, and/or the CCP can simply use the Covid-19 pandemic as a means to cut off the supply chain to many vital industries which include pharmaceutical goods such as anti-biotics, tech and telecom infrastructure, electronics, and tech products such as smartphones and PCs in general.

Ultimately, the CCP can intentionally disrupt or cut off these vital supply chains while knowing that companies doing business in China cannot easily repatriate back to their countries of origin while still being able to compete effectively with Chinese corporations.

Consequently, these Chinese companies will have competitive products, at lower prices, to market on a global basis which is a tactic associated with Hybrid Warfare.

At risk are vital goods and services which include necessities such as electronics, appliances, telecom infrastructure, pharmaceuticals, smartphones, tablet PCs and PCs in general.

Even U.S. movie studios are also doing business with China leading to censorship within movies such as any subject matter pertaining to China's appalling human rights record regarding the oppression of civil rights such as free speech.

Professional sports leagues, such as the National Basketball Association ("NBA"), are doing business in China and bowing to censorship enforced by the CCP in their lust for profits.

For example, in the fall of 2019 the NBA and the Houston Rockets organization officially and publically apologized for a tweet supporting Hong Kong protestors sent by Rockets GM, Daryl Morey, out raging many in the United States for the fact that the NBA and the Rockets issued public apologies to China governed by the CCP.

- *"Fight for Freedom. Stand with Hong Kong"*- Daryl Morey, GM, Houston Rockets, Tweet.

America's leading tech giants such as Google, Apple, HP, IBM and Microsoft are also doing business in China at the expense of their civil liberties, innovation and intellectual property ("IP") as a condition, enforced by the CCP, of doing business with the Chinese people who are oppressed by the CCP.

Senior executives for these companies appear to be more focused on profits rather than future economic consequences, civil liberties for the people of China, and even their own employees such as the case with Rocket's GM Daryl Morey who had to delete his tweet forcing the Rockets organization to publically apologize to the Chinese government.

What is also concerning is the fact that these senior executives from these tech giants are willing to give up innovation and IP to the CCP in order to make money in China.

These tech executives may not realize that Chinese companies will use their own innovation and IP to compete against their companies for global market share untimely trying to put these tech giants out of business which is a method of Hybrid Warfare and/or The Art of War.

An example of this is the fact that Chinese social media platforms such as WeChat, developed by Tencent, and TikTok, developed by ByteDance, are taking huge global market share away from American social media giant Facebook who also owns Instagram.

If this sounds outrageous, all these U.S. tech executives, including Mark Zuckerberg (CEO/Chairman-Facebook), need to do is read the article, The Theft That Led to Success: The Story of Nortel and Huawei* which describes how Huawei drove Nortel, out of business after over a century of success within the telecom industry.
*Source: Gadget Advisor- The Theft That Led to Success: The Story of Nortel and Huawei by Beezz Ludlum, Feb 8th, 2019

After reading the article "The Theft That Lead to Success", maybe these tech executives, including Mr. Zuckerberg, will understand who they doing business with and how these nation-state corporations from China compete using Hybrid Warfare techniques which mirror techniques described by Sun Tzu in the Art of War.

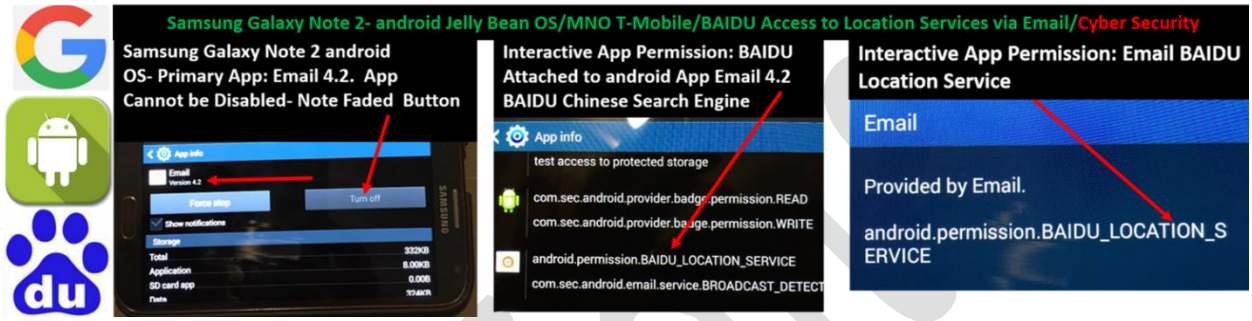
All of these examples of doing business with adversarial countries such as China have consequences such as being leveraged by China, governed by the CCP, in a time of crises such as the Covid-19 Virus pandemic.

Examples of Threats Pertaining to Hybrid Warfare

Below are examples of threats posed by Hybrid Warfare:

- **Intrusive Telecom Infrastructure**- Huawei and ZTE are accused by the U.S. government of manufacturing telecom infrastructure such as 5G networks that are supported by surveillance and data mining technology.

- **Intrusive Telecom Products**(1)- Samsung Galaxy Notes contain uncontrollable preinstalled surveillance and data mining technology developed by Google and Baidu (China) for the android OS (see enclosed example) according to a smartphone report for the Department of Homeland Security (U.S.).



- **Election Interference**- U.S. intelligence agencies accused Russia of using social media platforms such as Facebook to disrupt the 2016 U.S. presidential election.

- **Energy Market Disruption**- Russia intentionally enters into a price war with OPEC during the global Covid-19 pandemic in 2020 causing oil prices to plummet.

- **Election Voter Manipulation**- Cambridge Analytica used personal information collected from 80 million U.S. Facebook users to manipulate the user into voting for then presidential candidate, Donald Trump.

- **Intrusive Social Media Platforms**(2)- in 2019, The Pentagon (U.S.) bans members of the armed forces from using the social media platform TikTok due to predatory surveillance and data mining business practices employed by ByteDance (China) the developer of the platform.

- **Distribution of Intrusive Apps & Platforms**(3)- Google, Apple and Microsoft are inadvertently distributing surveillance and data mining technology in the form of apps & platforms developed by nation-state tech companies from China and Russia that include Tencent, ByteDance and Prisma Labs.

- **Distribution of Nation-state Propaganda via Social Media Networks**(4)- Nation-states such as China and Russia use social media platforms for the distribution of propaganda such with the case regarding China's use of Twitter to distribute favorable propaganda pertaining to the global Covid-19 pandemic outbreak.

- **Apps & Operating Systems Launch Attacks on Networks(5)**- Apps and Operating Systems such as the Windows OS are hijacked by nation-state hackers in order to be used to launch attacks on networks associated with critical infrastructure.

- **Stolen Intellectual Property ("IP")(6)**- according to the U.S. Federal Bureau of Investigation ("FBI"), China has been accused of stealing IP from numerous corporations including medical institutions such as MD Anderson Cancer Center, in Houston, TX. *"China is the 'Most Significant' Threat to the U.S., over 1,000 Open Investigations into Chinese Intellectual Property Theft"- FBI Director, Christopher A. Wray.*

(1) Source: Department of Homeland Security Smartphone Report, by RML Business Consulting, for the Study on Mobile Device Security, April, 2019 **(2)** Source: the NY Times- U.S. Military Branches Block Access to TikTok App Amid Pentagon Warnings by Neil Vigdor, Jan 20th, 2020 **(3)**Source: The Epoch Times- Google, Apple & Microsoft Distribute Chinese Surveillance Technology by Rex M. Lee, Feb 25th, 2019 **(4)**Source: The Hill- Twitter Comes Under Fire Over Chinese Disinformation on Corona Virus by Chris Mills Rodrigo, March 25th, 2020 **(5)**Source: Mission Critical Communications Magazine- The Rise of Foreign Cybersecurity Threats by Rex M. Lee, Aug 2019 **(6)** Source: Houston Chronical- MD Anderson Ousts 3 Scientists Over Concerns About Chinese Conflicts of Interests by Todd Ackermann, April 19th, 2019

All of these threat examples have one thing in common, they are all linked to Hybrid Warfare which poses huge cybersecurity, privacy, safety and civil liberty threats at the strategic and tactical level that need to be addressed by governments, corporations, universities, small businesses and individuals.

Cybersecurity Threats Posed by Hybrid Warfare: Tactical vs. Strategic

For many years' governments, universities and corporations focused on cybersecurity at the tactical level by way of IT departments, software patches and upgrades plus the adoption of cybersecurity software.

Fighting cybersecurity threats at the tactical level is a lesson in futility since the battle is often fought from a reactionary position by way of software upgrades, patches and the deployment of unproven apps/platforms.

These software upgrades, patches and app/platforms are all vulnerable to malware, developed by nation-state hackers, and are often dealt with at the tactical level within IT but the long term problem regarding nation-state sponsored hacking is never dealt with at the strategic level by elected & govt. officials, senior executives and board members including the Board Chairmen.

- *"Our adversaries have been attacking from the strategic layer for decades while we have been defending from the tactical layer. This must change immediately by updating corporate and security strategy based on hybrid warfare - the long-term strategy of your adversary is to replace your company. There will be clear winners and losers in the considerable short term."* -T. Casey Fleming, BlackOps Partners, Washington, DC

Governments, universities, medical institutions and companies need to implement cybersecurity at the strategic level by adopting a strategy at the board, senior executive, and elected & govt. official layer.

- *"Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win"*- Sun Tzu, The Art of War

Every company, medical institution and university with innovation and IP is at immediate risk along with governments looking to protect classified information which in today's connected world can simply be acquired by adversarial nation-state tech companies through intrusive apps and platforms that support telecom products such as smartphones.

An immediate cultural change is required at all levels of government, universities and companies who are trying to protect innovation, IP and classified information.

Due to threats from Great Power Competition and Hybrid Warfare, cultural change must be focused on security overall including security associated with the supply chain and government contractors.

This cultural change must be led by elected and government officials, CEOs, and the Board Chairmen. Information is power making it extremely important that all employees and citizens are aware of threats posed by this new era of Great Power Competition and Hybrid Warfare.

Existential risks and threats need to be identified while strategic level strategies are developed to mitigate plus eliminate these risks and threats.

A few cybersecurity firms, such as BlackOps Partners, have adopted tactical wargames as a means to help companies react to threats associated with Hybrid Warfare at the strategic level.

Through wargaming, companies, universities, medical institutions, and governments can re-position their overall strategy to remain relevant as Hybrid Warfare continues to evolve enabling adversarial nation-state competitors to replace them.

Stay safe and healthy during these trying and unprecedented times.

Author- Rex M. Lee

My next article for the Vision Times will be centered on Digital Authoritarianism and Cyber Oppression.

Rex M. Lee is Freelance Tech Journalist and Cybersecurity & Privacy Advisor. For more information contact Rex at RLee@MySmartPrivacy.com *or go to My Smart Privacy at: www.MySmartPrivacy.com*