http://nationalinterest.org/print/blog/the-buzz/how-china-wins-the-south-china-sea-war-without-firing-shot-19006

How China Wins the South China Sea War (Without Firing a Shot)

Bill Gertz
1/10/2017

Is it too late to stop Beijing?

China is engaged in a broad-ranging information warfare campaign as part of a covert effort to take control of the South China Sea — in the words of ancient strategist Sun Tzu, without firing a shot.

The Chinese cyber attacks have been carried out extensively on regional states along with political influence operations designed to falsely convince the international community that the waters of the sea are and have been China's sovereign maritime territory.

James Clapper, the US director of national intelligence, told a Senate hearing last week that aggressive Chinese cyber attacks were continuing. " China continues to succeed in conducting cyber espionage against the US government, our allies, and US companies," he said.

In the South China Sea, the covert effort remained at low levels over the past 10 years as China built up more than 3,000 acres of new islands and in recent months began militarizing the islands in the takeover campaign.

Another goal of the information operation was to play down the significance of Beijing's South China Sea activities in a calculated bid to avoid provoking the United States.

The South China Sea information war program is outlined in my book, *iWar: War and Peace in the Information Age* [3], published Jan. 3.

"The People's Republic of China has studied the US approach to information warfare from the Cold War and has successfully navigated itself into a position of 'respectability' compared to their brothers from Russia and their ham-fisted 'Russia Today' (RT)," said retired US Navy Capt. James Fanell, a former Pacific Fleet intelligence director who specializes in Chinese affairs.

Fanell see Chinese information warfare targeting the United States and the inability to recognize the danger to a frog being slowly boiled alive. "The heat in the pool just keeps going up one degree at a time," he says.

Until the recent UN Permanent Court of Arbitration ruled against China's expansive claims to the sea, China appeared to have succeeded in deceiving the world into believing that the waters were historically theirs and that any other countries' claims to the sea as international waters were false.

Beijing also announced, significantly, that any attempt to counter these claims posed a threat to China's core national interests — language widely regarded as a basis for going to war to defend those interests.

The campaign utilized a sophisticated combination of information warfare and Chinese deception operations that lulled the United States into first ignoring the problem, and later

halfheartedly attempting, through public statements, to prevent military weapons and facilities from being added.

By late last year, however, it was too late. China was finished building a series of military bases in the South China Sea, first on Woody Island in the Paracels, in the northern part of the sea, then on three separate maritime outposts in the Spratly Islands in the southern part.

Behind the scenes China launched an aggressive information and cyber warfare operation against regional states beginning around 2010, using military cyber warfare units located in the Chengdu military region under a code-named Unit 78020. No government was spared in the attacks that involved cyber strikes against computer networks in Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, and Vietnam.

"We assess Unit 78020's focus is the disputed, resource-rich South China Sea, where China's increasingly aggressive assertion of its territorial claims has been accompanied by high-tempo intelligence gathering," states a report by the cyber security firm ThreatConnect. "The strategic implications for the United States include not only military alliances and security partnerships in the region, but also risks to a major artery of international commerce through which trillions of dollars in global trade traverse annually."

The South China Sea is used for international trade to the tune of US$5 trillion annually.

The goal for China in the sea is to impose regional hegemony and drive out the US Navy, which has kept the area free and open to international trade for decades.

The information warfare campaign focused on all the governments of Southeast Asia, including the headquarters of the 10-nation Association of Southeast Asian Nations and private and public energy organizations. The operation included data theft, to gain valuable commercial information and foreign government secrets that could be given to Chinese companies or used in negotiations.

For the longer term, Chinese military hackers gained strategic access to target government computer networks that could be attacked and shut down in a crisis or conflict, or used to spread disinformation internally to confuse and weaken China's enemies.

For the South China Sea campaign, the Chinese used an extensive network of hundreds of Internet Protocol addresses that in some cases were used for only an hour before being abandoned — all in line with a methodology designed to avoid detection by cyber security services, both government and private.

Through these information warfare activities China incrementally gained control over the South China Sea and employed multiple pillars of national power with the larger goal of influencing and ultimately imposing political control over the entire region.

The shadow information war is typical of the kinds of activities China engages in not just in Southeast and Northeast Asia but globally as part of its drive for world acceptance and domination.

China today employs strategic information warfare to defeat its main rival: the United States. China's demands to control social media and the Internet are part of its information warfare against America and must be resisted if free and open societies and the information technology they widely use are to prevail. China remains the most dangerous strategic threat to America — both informationally and militarily.