NEWSBYTES

April 10, 2024 No. 1148 Since 2001
A ministry of Calvary Chapel of Appleton

"Let us be alert to the season in which we are living. It is the season of the Blessed Hope, calling for us to cut our ties with the world and build ourselves on this One who will soon appear. He is our hope—a Blessed Hope enabling us to rise above our times and fix our gaze upon Him." Tozer

China's 'Unrestricted Warfare': Is It Here Already?

by Pete Hoekstra

- China-linked hackers appear to be looking to attack U.S. infrastructure, especially key components such as the electrical grid, water reservoirs and treatment plants, pipelines, and transportation and communications systems, among other targets.
- The goal is seemingly to disrupt the U.S. everything critical to life – if you have no electricity, your cellphone will not work; no water will come out of the tap; gas pumps will not pump gas; flights and trains will stop, and disease from disabled sewage treatment plants will spread. There will be havoc and panic. The government and military will be unable to protect the nation. That is what is meant by "unrestricted warfare." Not a bullet was fired. It did not have to be. According to Sun Tzu's *The Art of War*, it is perfect.
- What are some of the steps that should be taken?
- The West has correctly identified the CCP as the malign threat that it is; now we have a responsibility to put into place the measures and deterrents to prevent it from attacking us through cyberspace or any other way. Let us not wait until we experience a 9/11-scale cyberattack that could be far more damaging to the U.S. than what took place on that dark day more than 20 years ago.

The West has correctly identified the Chinese Communist Party as the malign threat that it is; now we have a responsibility to put into place the measures and deterrents to prevent it from attacking us through cyberspace or any other way. Let us not wait until we experience a 9/11-scale cyberattack that could be far more damaging to the U.S. than what took place on that dark day more than 20 years ago.

(Image source: iStock)

If there is one thing FBI Director Christopher Wray has been consistent on, it is the threat of Communist China across a wide range of fronts. At an unprecedented event on July 6, 2022,

Wray and his British counterpart, MI5 Director General Ken McCallum, held a joint public appearance – the first ever -- to discuss the growing security challenge posed by China. Evidently, they saw the matter as urgent.

In this joint appearance, the two men highlighted the threats posed by the Chinese Communist Party (CCP) and the CCP's civil-military fusion state -- specifically, that the CCP is intent on acquiring and stealing technology and business secrets from the West. Targeted areas include advanced materials, data and artificial intelligence (AI). China's President Xi Jinping has made it clear that he intends China to not only catch-up to, but surpass, the West.

More recently, Wray highlighted how the CCP and those affiliated with it apparently plan to use its technological capabilities to target the West.

China-linked hackers appear to be looking to attack U.S. infrastructure, especially key components such as the electrical grid, water reservoirs and treatment plants, pipelines, and transportation and communications systems, among other targets.

The goal is seemingly to disrupt the U.S. everything critical to life – if you have no electricity, your cellphone will not work; no water will come out of the tap; gas pumps will not pump gas; flights and trains will stop, and disease from disabled sewage treatment plants will spread. There will be havoc and panic. The government and military will be unable to protect the nation. That is what is meant by "unrestricted warfare." Not a bullet was fired. It did not have to be. According to Sun Tzu's *The Art of War*, it is perfect.

Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA), testified before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party that the threats posed by China are not imaginary: they are real. Her agency already has discovered CCP penetrations into the telecommunications industry, aviation, energy and water infrastructure. As the threat from China continues to grow, the global security environment requires the U.S. and our allies to act now to harden our infrastructure and systems to mitigate the threat.

The problem is one of supreme urgency. No one knows who will win the U.S. presidential election on November 5. If I were head of the Chinese Communist Party, I would probably be saying to myself, "I am stuck with a weak economy, more than a billion people who will not be happy with that, and just more seven months with an American president who calls me a 'competitor,' as if the US-Chinese relationship were about EV car dealerships -- although that, too. What are my choices? a) Use this opportunity, which will soon be closing, to choke off Taiwan and take over the world's supply of semiconductor chips. If the U.S. tries to stop us, we could threaten them with mayhem or simply go ahead and make some. b) *Instead* of Taiwan, why not just go straight for the U.S. while it is bogged down in Ukraine, the Middle East and its election? Or c) We can wait and see who wins (with our help) and if it is the wrong person, we still have two-and-a-half months until the new president is inaugurated."

What are some of the steps that should be taken?

First, stop *all* investments in China and reroute essentials, such as the manufacture of medicines, to other nations. *Any* investment, even in paper cocktail umbrellas, goes toward

strengthening the People's Liberation Army against us. We can hear the screeching of Wall Street and their Augustinian cry: "But not yet!" The threat, however, should be viewed in terms of national security. No one will ring a bell when the lights go out.

The U.S. will also need to impose secondary sanctions, so that any country preferring to do business with China is prohibited from doing business with the U.S.

In addition, China -- for poisoning to death roughly 100,000 Americans each year with fentanyl and other opiates, a mass-murder equivalent to one large plane crash every day -- should be designated as a state sponsor of terrorism. China should also be barred from using the international banking system, or SWIFT, "a secure network that allows more than 10,000 financial institutions in 212 different countries to send and receive information about financial transactions to each other."

Second, companies and universities also need to get serious about their security systems to make the theft of intellectual property more difficult to perpetrate but easier to detect. We cannot allow our enemies to short-circuit the difficult and expensive process of technological innovation by simply walking out the door with the plans.

This precaution, sadly, would do well to include a moratorium, at least for the time being, on students from Communist China attending U.S. universities. Again, there will be more screeching from academic institutions that are fond of holding out their tin cups, but are we really interested in educating our "competitors" to take us over or kill us?

Third, the U.S. needs to cooperate with its allies to protect the intellectual property and technological advances of our countries' respective corporations as a national security priority. One excellent example where this cooperation has been successful is between the U.S. and the Netherlands. The governments of the two countries have worked together closely to protect against technology transfer to the CCP. While each country has the decision as to its own trade policies, sharing intelligence and threat assessments enables both countries to make better decisions regarding joint security concerns.

Fourth, companies must be willing to notify the government if their systems have been attacked or compromised by outside entities. Under current law, publicly-traded companies have four days to report a cyber incident to regulators. Businesses sometimes have been understandably reluctant to acknowledge that their systems have been compromised: there is the risk of reputational damage and unpleasant repercussions. Organizations, however, need to be confident that sharing this information with the government will only be used to help address the specific incident. Tragically, our government has not quite been doing all it can to inspire trust. There might be some extremely unpleasant repercussions from that.

Finally, there must be a coordinated strategy between our national, state and local governments on the CCP threat, including prime examples of where this system has failed, as in the production of EV batteries in the U.S. by CCP firms; the CCP buying up American farmland, especially near military bases, and the government's failure to hold the CCP to account for its lies about COVID's human-to-human transmissibility, which caused the unnecessary deaths of more than a million Americans, and the CCP's mass-poisoning of Americans with fentanyl, which in itself is an act of war.

While the federal government has warned "that Chinese EVs could collect your data and send it back to China," states and local governments are welcoming Chinese EV battery manufacturing plants into their communities, frequently with massive government subsidies. This lack of coordination is a serious vulnerability in our national security posture.

Wray and McCallum were correct in highlighting the threat from the CCP in 2022. Wray has reemphasized the growing threat. The evidence is clear, and the time has come for our elected leaders and public servants — at all levels of government — to respond in a coordinated fashion to this threat. The West has correctly identified the CCP as the malign threat that it is; now we have a responsibility to put into place the measures and deterrents to prevent it from attacking us through cyberspace or any other way. Let us not wait until we experience a 9/11-scale cyberattack that could be far more damaging to the U.S. than what took place on that dark day more than 20 years ago.

Peter Hoekstra is a Distinguished Senior Fellow at Gatestone Institute. He was US Ambassador to the Netherlands during the Trump administration. He also served 18 years in the U.S. House of Representatives representing the Second District of Michigan and served as Chairman and Ranking Member of the House Intelligence Committee.

Hamas is ‘collapsing,’ captured terrorists tell Israel

March 31, 2024

Hamas paying ‘very heavy’ price, Israeli Defense Minister says, citing testimony by captured terrorists.

By World Israel News Staff

The Hamas terror organization is suffering heavy losses and is collapsing in on itself, captured terrorists have told their Israeli interrogators, according to Israel’s defense minister.

Defense Minister Yoav Gallant (Likud) met with IDF soldiers at the 98th Division’s headquarters Sunday, and held an operational assessment.

During his visit, Gallant discussed Israel’s recent gains in its ongoing war against Hamas in the Gaza Strip, saying that testimonials by terrorists captured in the IDF’s massive raid on Shifa Hospital in Gaza City highlighted the decline of Hamas’ operational capabilities.

“The group is collapsing from within,” Gallant said captured terrorists have told Israeli security officials.

“In the last week or two, hundreds of terrorists have been captured and what they say about what happened to them tells the whole story. They say that Hamas is collapsing from within. The prices they pay are very heavy.”

“In the last few days, we have also seen very great progress, both in the terrorists in the field, and with more senior commanders, even very senior ones,” Gallant continued.

Shifa Hospital, the local headquarters for Hamas in the northern Gaza Strip prior to the Israeli invasion of Gaza, was reoccupied by Hamas forces in recent months, Israeli security officials said earlier this month.

On the night of March 18th, the IDF launched a massive, multi-day raid on the hospital, sparking running gun battles with terrorists inside and outside of the facility.

Hundreds of terrorists were killed during the operation, with over 800 others arrested.

IDF chief spokesman Rear Admiral Daniel Hagari told reporters on March 25th that the operation in Shifa Hospital had “a huge effect on Hamas and Islamic Jihad,” adding that it was the most enemy combatants killed and captured in a single raid in the war, which will cause “severe damage” to terror organizations in the northern Gaza Strip.

“Backlash Is Real”: DEI Exodus Gains Steam Across Corporate America

OPINION

DEI concept | Image by skynesher/Getty Images

By **ZeroHedge**

Apr 4, 2024

(ZeroHedge) — *Have we reached peak DEI stupidity?*

Yes, we are well past the peak. As we explained in early March, “Both the DEI and ESG gravy trains on Wall Street are finally coming to an unceremonious end.”

The unraveling of “diversity, equity, and inclusion” initiatives was seen on the state level, as Red states rushed to ban DEI programs in 2023. Google, Facebook, and other tech

companies slashed DEI staff by late last year. Early this year, universities began rolling back diversity programs, while Harvard President Claudine Gay was demoted.
DEI was doomed to fail, and corporations have been quickly scrambling to abandon mindless and profitless diversity programs with Marxist roots. The latest earnings call data shows that “DEI” mentions have collapsed from their peak in 2021, according to **Axios**, citing data from AlphaSense.

In January, Johnny Taylor, president of the Society for Human Resource Management, told Axios that corporate executives are fed up with DEI.

“The backlash is real. And I mean, in ways that I’ve actually never seen it before,” Taylor said, adding, “CEOs are literally putting the brakes on this DE&I work that was running strong” since George Floyd’s murder in early 2020.
Kevin Clayton, senior vice president and head of social impact and equity for the Cleveland Cavaliers, said the chief diversity officer role was all the rage across corporate America after Floyd’s murder. He said companies filled these positions “out of gilt,” and hiring wasn’t the best.

Axios noted, “Some businesses are cutting back funding, trimming DEI staff — and even considering pulling back on things like employee resource groups comprised of workers of various races, ethnicities or interests.”

The pushback on DEI is finding momentum across corporations and universities. Subha Barry, former head of diversity at Merrill Lynch, told Bloomberg last month: **“We’re past the peak.”**

“The seemingly small changes — lawyerly tweaks, executives call them — are starting to add up to something big: the end of a watershed era for diversity in the U.S. workplace, and the start of a new, uncertain one,” per Bloomberg.

If it’s DEI or ESG, the blowback phase is well underway. Companies are running away from these diverse and green programs because, simply, they don’t make money.

(and they COST companies money, as well as being generally racist in a reverse-perverse kind of way….MD)