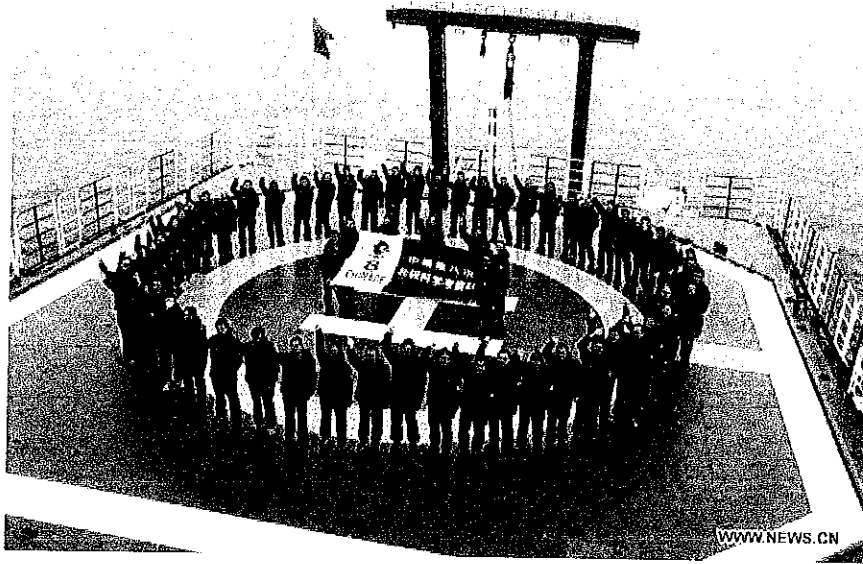


China seeks bigger role in Arctic

By Liz Ruskin, Alaska Public Media - February 6, 2018



Scientists pose for team photo on the Chinese icebreaker Xuelong in 2017. (Photo: Xinhua/Yu Qiongyuan)

At its most northern point, China is hundreds of miles from the Arctic Circle, but its leaders want a say in how the region is governed. Recently, the country issued its first national policy on the Arctic, and it reveals its expansive ambitions in the far North.

Listen **now**

"China is determined to better know the Arctic, protect the Arctic, utilize the Arctic and participate in the governance of the Arctic," Vice Foreign Minister Kong Xuanyou said as the policy was announced, according to China's official state media.

The policy says China will cooperate with others on development in the region, including new shipping routes it calls a "Polar Silk Road," after the ancient trade routes connecting China to Europe.

This is the first white paper China has ever issued for a region outside its own territory, said University of Canterbury (New Zealand) Professor Anne-Marie Brady. She said the document demonstrates the country's growing assertiveness in global affairs.

"China is stepping into the power vacuum of global leadership since the Trump administration came to power, and it's preparing to shape the new world order," Brady said Tuesday, at a forum organized by the Wilson Center, a Washington, D.C. think tank.

Kissinger Institute Director Robert Daly said it's natural for China to play a major role in the Arctic, particularly when it comes to science, trade and financing. But he said the big question is how other countries are going to react. Daly said the Chinese policy repeats certain phrases, like "the shared future of mankind," to portray itself as a benevolent force, interested only in *economic* globalization.

"But note that the last sentence of this important document reads like this: 'China will advance Arctic-related cooperation under the Belt and Road Initiative,'" Daly said. "That's about as important as a preposition can be in this world: 'Under the belt and road initiative.'"

Belt and Road is the banner for how China hopes to increase its influence around the world. It's a global development policy Chinese President Xi Jinping announced in 2013. Daly said extending that China-centric policy to the Arctic isn't a good idea.

"China's participation can be welcomed within existing frameworks," Daly said. "But this notion that China will lead it under Belt and Road has to be resisted, rejected, countered."

China's interest in the region has grown over the past decade. It has had observer status at the Arctic Council since 2013. The country has one polar icebreaker and is building a second. And it's a major investor in Russia's Yamal liquefied natural gas facility.

Liz Ruskin, Alaska Public Media

<http://www.alaskapublic.org>

Liz Ruskin covers Alaska issues in Washington as the network's D.C. correspondent. She was born in Anchorage and is a West High grad. She has degrees from the University of Washington and the University of Missouri School of Journalism in Columbia. She previously worked at the Homer News, the Anchorage Daily News and the Washington bureau of McClatchy Newspapers. She also freelanced for several years from the U.K. and Japan, in print and radio. Liz has been APRN's Washington, D.C. correspondent since October 2013.

She welcomes your news tips at [lruskin \(at\) alaskapublic \(dot\) org](mailto:lruskin@alaskapublic.org) | About Liz



As War Danger Mounts in the Arctic, Peace Hinges on a Revival of the Wallace Doctrine

According to the Department of Defense's dismally short sighted vision for the Arctic, U.S. strategic interests were best maintained not by cooperation with Arctic partners, by rather by belligerent sabre rattling under the guise of "competition" with nations who have continuously professed a desire to work with the west as allies.

In recent weeks, this belligerence has taken the form of a new forward posture of 150 advanced U.S. fighter jets to be housed at the Eielson Airforce Base in Alaska including a mix of F22 Raptors and F35 Lightning II jets only 600 miles away from the Russia border. Each fighter plane carries the ability to launch strikes onto Russia after a brief flight across the 100 mile Bering Strait gap. Considering the entire American air force only has 187 F22s and 250 F35s, the proportions of this absurd build up can best be appreciated.

In the most recent DOD Arctic Strategy Report which has shaped this suicidal battle plan, Russia and China are defined as nothing but existential threats to the world order which must be stopped at all costs with the report's authors stating: *"In different ways, Russia and China are challenging the rules-based order in the Arctic. U.S. interests include limiting the ability of China and Russia to leverage the region as a corridor for competition that advances their strategic objectives through malign or coercive behavior."*

Describing this aggressive display that folds into the renewed threats of attack faced by dangerous NATO maneuvers across Europe in recent months, Russian Major General Vladimir Popov told Sputnik News:

"Alaska is remote from the U.S. mainland, but is an outpost in relation to Russia—we are separated only by a strait, and the border is literally within the line of sight. This is a strategic region for the U.S. Adding 150 more fighters would at least double the combat potential of the existing forces there."

Continuity of Government and NORAD

What makes this dire situation ever more precarious is the fact that President Trump has found himself stuck in a COVID-19 quarantine.

What should be a mere hiccup in governmental procedures is quickly being turned into something much greater as renewed calls for enacting Continuity of Government procedures secretively written into law this past March 2020 arising by various leading figures of the deep state such as House Speaker Nancy Pelosi. When MSNBC asked Pelosi (now second in line to take the mantle of presidency) if anyone reached out to her from the White House regarding Continuity of Government, Pelosi said: *"No, they haven't. But that is an ongoing, not with the White House but with the military, quite frankly, in terms of the — some officials in the government."*

That these calls are occurring amidst a heightened clamor for military coup to unseat the President, the general threat of civil war and the looming danger of economic meltdown, statements like those uttered by Pelosi to CNN and MSNBC this week should not be taken lightly.

In the updated March 2020 Continuity of Government protocols, General Terrance O'Shaunessy (head of both NORAD and NORTHCOM) would take the "temporary" reins of the presidency under crisis conditions of ungovernability which are not too difficult to imagine

As War Danger Mounts in the Arctic, Peace Hinges on a Revival of the Wallace Doctrine — Strategic Culture amidst the storms currently sweeping America. Military staff who would take up a parallel chain of command continue to be stationed 650 meters below Cheyenne Mountain in Colorado where they have been deployed since March 2020 following Mark Espers' orders to NORTHCOM to "prepare to deploy".

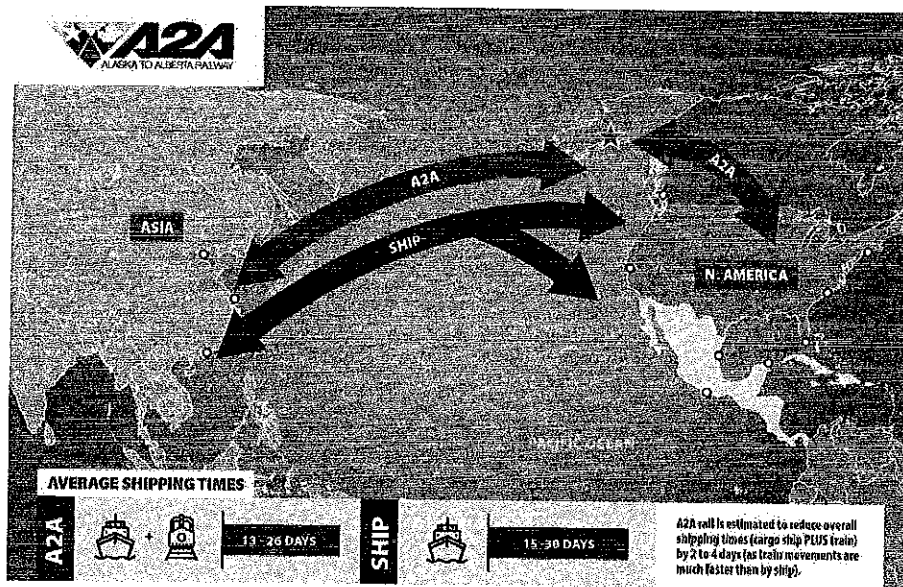
O'Shawnnessy has repeatedly echoed the views of the Washington/NATO establishment that the greatest threats to the world stem from Russia and China directly referencing their supposedly nefarious intentions in the Arctic.

The Polar Silk Road: A Healthier Paradigm for the Arctic

Rather than bring the forces of war to the Arctic, Russia and China have together been demonstrating a far more efficient and moral approach which certain patriotic forces within North America tend to be in alignment with, including the current President.

Since January 2018, the Arctic has increasingly become dominated by the positive extension of the New Silk Road northward in the form of the maritime and land based "Polar Silk Road" which has united brilliantly with President Putin's Far East development program. This program aims to increase arctic shipping five fold by 2024 and begin a bold program of infrastructure, rail, road, pipeline, mining and port building in order to begin accessing the vital raw materials desperately needed for the coming centuries of multipolar development.

On September 26, President Trump working alongside political allies in Alaska, Alberta and the private sector allike streamlined a project which taps into this spirit of genuine economic cooperation and long term thinking unseen in decades in the form of the Alaska-Canada Rail connection. Looking at the business models guiding this emerging project, it is important to note that the destructive thinking of globalization and zero sum logic are not to be found at all as the entire program is vectored on tying North America economic interests into China's Belt and Road and growing Asian markets.



The Wallace Doctrine for the Arctic Must Be Revived

As I wrote in my recent report Trump's A Revival of the Wallace Doctrine for the Post-War World, the last serious pro-development strategy to arise from a leading American politician took the form of President Franklin Roosevelt's ardent anti-imperial Vice President Henry Wallace, who spent years with his Russian counterparts during WWII arranging the conditions of mutual development of both nations during the post-War age with a strong focus on the long awaited Bering Strait Rail connection and obvious Alaska-Canada transport corridors. In his *Two Peoples One Friendship*, Wallace described his discussions with Foreign Minister Molotov in 1942 saying:

"Of all nations, Russia has the most powerful combination of a rapidly increasing population, great natural resources and immediate expansion in technological skills. Siberia and China will furnish the greatest frontier of tomorrow... When Molotov [Russia's Foreign Minister] was in Washington in the spring of 1942 I spoke to him about the combined highway and airway which I hope someday will link Chicago and Moscow via Canada, Alaska and Siberia. Molotov, after observing that no one nation could do this job

As War Danger Mounts in the Arctic, Peace Hinges on a Revival of the Wallace Doctrine — Strategic Culture
by itself, said that he and I would live to see the day of its accomplishment. It would mean much to the peace of the future if there could be some tangible link of this sort between the pioneer spirit of our own West and the frontier spirit of the Russian East."

The Wallace/FDR Vision for the Post-War Era



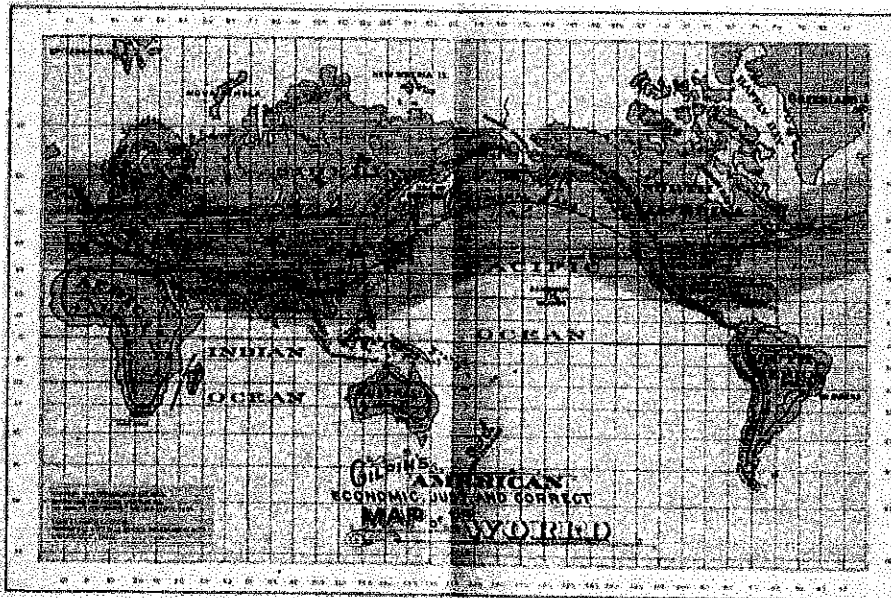
The Molotov/Wallace vision wasn't something entirely new.

Earlier programs for building the Bering Strait rail connection were advanced by Russian Prime Minister Sergei Witte and Czar Nicholas II who in 1906 sponsored teams of American engineers to conduct feasibility studies of the project, then estimated to cost \$200 million.

On the American side of the project, Lincoln's trusted bodyguard William Gilpin (a man who was known as a leading spirit of America's own Trans Continental Railway) and later Governor of Colorado promoted the work throughout his life saying of the Alaska Canada rail connection:

"It is sufficiently apparent that the building of a railroad by way of Alaska, Bering Strait and northeastern Siberia, connecting with the Canadian Pacific in British Columbia and in Siberia with the Russian line now being pushed forward to Vladivostok, is by no means an unpracticable undertaking".

Gilpin's global program was outlined thoroughly in his 1890 book the Cosmopolitan Railway.



Exhibiting the stark raving fear of the renewal of this latent spirit of U.S.-Russian friendship in the build up to the November elections, Thomas Wright (senior Fellow at the Brookings Institute) wrote a panicky op ed in the Atlantic on September 30 called "What a Second Trump Term Would Mean for the World". In this article, Wright echoes the broader fears of the deep state of a revival of the Henry Wallace doctrine which the author laments would have been just terrible had it not fortunately been sabotaged by the "great" figure of Harry Truman in January 1945. Wright says:

"Looking back on U.S. diplomatic history, one of the great counterfactuals is what would have happened if Franklin D. Roosevelt had not replaced his vice president Henry Wallace with Harry Truman in 1944. Wallace was sympathetic to the Soviet Union and became an ardent opponent of the Cold War. If he had become president when FDR died, in April 1945, the next half century could have gone very differently—likely no NATO, no Marshall Plan, no alliance with Japan, no overseas troop presence, and no European Union... The U.S. is now teetering on another historically important moment. With Trump, we would not only be deprived of our Truman. We would be saddled with our Wallace—a leader whose instincts and actions are diametrically opposed to what the moment requires. With few remaining constraints and a vulnerable world, a re-elected Trump could set the trajectory of world affairs for decades to come."

It should be clear to all that the renewal of the Wallace-Gilpin spirit of development into North America's Arctic is not only good business but also serves as a vital precondition to re-establishing a world order founded upon trust, win-win cooperation, and non-zero sum thinking. While it is fairly clear that Trump's political instincts are vectored in this direction (giving rise to such frightful diatribes by emissaries of the Cold War at Brookings and the CFR), it still remains to be seen if sufficient political influence can be exerted to rein in the swamp before a hot war and military coup are unleashed.

The author can be reached at matt.ehret@tutamail.com

© 2010 - 2020 | Strategic Culture Foundation | Republishing is welcomed with reference to Strategic Culture online journal www.strategic-culture.org.

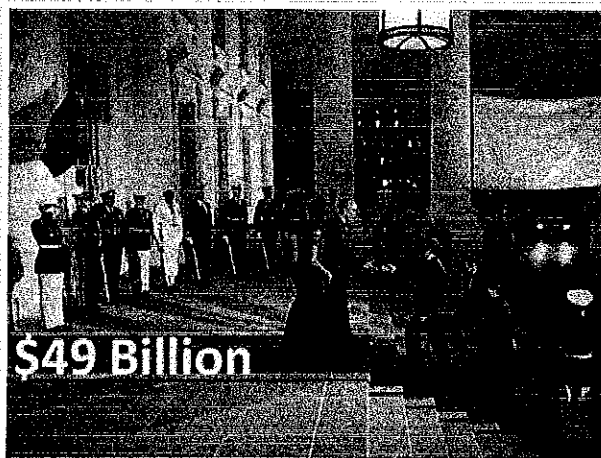
The views of individual contributors do not necessarily represent those of the Strategic Culture Foundation.

More



Sunday, September 27, 2015

Carlyle Co-founder Makes Head Table for Chinese State Dinner



Carlyle Group co-founder David Rubenstein and his wife Alice sat at the prestigious head table at the White House State Dinner for Chinese President Xi Jinping. *Politico* referred to affair as "a glitzy and glamorous good time." *WaPo* reported the wealth at the head table to be \$49 billion. That's from a mere fourteen guests. As four of the guests are couples the \$49 billion comes from ten people, an average of nearly \$5 billion per power person/couple.



The Carlyle Group taught the Chinese about private equity, with its numerous PEU investments in China. Carlyle's Chinese affiliates killed and sickened babies (Yashili) and exposed children to toxic jewelry (Oriental Trading). That's what happens when greed combines with management practices that erode quality.

Carlyle has its sights set on turning Alaska into a Chinese like economy. Mrs. Rubenstein, Alice Rogoff Rubenstein is in a unique position to advance this as owner of the largest newspaper in Alaska. President Obama visited Mrs. Rubenstein's home less than a month ago. Rogoff wants the

Insider Architect of the Implosion

"I had a choice. I could be an insider or I could be an outsider. Outsiders can say whatever they want. But people on the inside don't listen to them. Insiders, however, get lots of access and a chance to push their ideas. People — powerful people — listen to what they have to say. But insiders also understand one unbreakable rule: They don't criticize other insiders." —Larry Summers, Ph.D.

Testimonials

The *PEU Report* is absolutely brilliant and has given me faith that someone out there has noticed what is going on in the world. —Ex-Bloomberg reporter

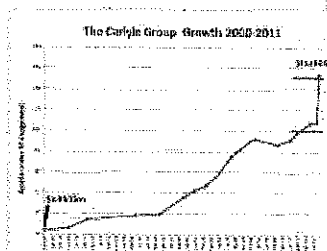
I really can't say enough how much I enjoy your commentary on *PEU*. You manage to dig into the details and sum it up in a way that is so succinct and entertaining. —Ex-Bloomberg reporter

When Tim Geithner, the former Treasury secretary, takes over as president of Warburg Pincus, the private-equity firm, even a high-school dropout can discern a pattern. —Another person who noticed

PEU = Private Equity Underwriter

As income and wealth rises to the top, so does political power.

The Carlyle Group



Broke \$100 Billion Under

government's help to develop deep water ports on the west coast of Alaska.

President Obama hosted the billionaires' head table. He is putting the finishing touches on his legacy and likely future employment.

Posted by PEU Report/State of the Division at 10:38 AM

Newer Post

Home

Older Post

Management (April 2011)
Exceeded \$150 billion (July 2011) now over \$200 billion

About Me





PEU Report/State of the Division

San Angelo, Texas, United States

When something starts to stink, it's good to find out what's rotting. Oftentimes, it's truth decay. Does the world become a dark comedy as you age? Was it always that way and I just noticed?

[View my complete profile](#)

Subscribe To

-  Posts 
-  Comments 

Contact e-mail:

Send your message to
peureport@gmail.com

Blog Archive

- 2020 (79)
- 2019 (66)
- 2018 (58)
- 2017 (154)
- 2016 (152)
- ▼ 2015 (219)
 - December (6)
 - November (16)
 - October (16)
 - ▼ September (23)

Carlyle Group: Employee Owned PA Consulting Goes PEU

Alaska Should Aggressively Pursue Investment Returns

FDA Nominee Served on Portola Pharmaceuticals Board

Carlyle Co-founder Makes Head Table for Chinese St...

Co-founder Quits Carlyle's Claren Road

Carlyle's Investor Meeting Hears from Another Ex-P...

Carlyle Upscales Silicon Valley Home Park

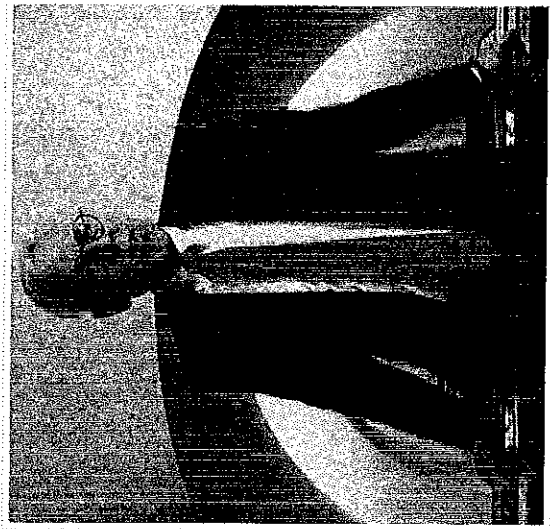
VW vs. GM: The Akerson Effect

Who Will File Iran Notice for NYT Oil & Money Speech?

Carlyle Burned by Energy Prices

Otter Surfaces in Encryption Debate?

Chertoff & Carlyle Group Bet on CyberSecurity: Bu...



That's David Rubenstein, one of the most disgusting people taking up space on the planet Earth.

His wife bankrolls the *Alaska Dispatch*. I understand that she is rather nice. She couldn't possibly be nice enough to counter-balance the insidious creepiness of her husband, though. The guy is perhaps the sleaziest merchant of death since I.G. Farben. He's certainly been responsible for far more deaths of innocents than Union Carbide in Bhopal, but possibly not as many as the people who came up with destroying the Mekong Delta aquifer and ecosystem for 150 years with Agent Orange. If you google **Carlyle Group** and **criminal acts**, there are 17,500 items there.

People die every fucking hour of every fucking day because of the schemes and scams of the family bankrolling the *Alaska Dispatch*.

So, Tony, Mia, Scott, Jill, Rena, Josh, Craig, Stephen, Amanda, Seth (see update two), Scott, Peter, Aaron, Todd, Jacob, Alisa and Lexie - enjoy the Rogoff-Rubenstein blood money. Every sleazy penny.

Update Two: Apparently Seth left when he investigated where the \$\$\$ comes from.

images - John & Heather, Mel's pie chart; Brian & Gov. Howard Dean

Posted by Philip Munger at 2:07 PM

20 comments:

Anonymous said...
I agree, those IM photos of Palin's cellulite were way out of bounds. She's a sociopath, but we don't need to look at her legs to see that...
January 3, 2010 at 5:01 PM

guides, lodges and other pilots due to arrive fo...
4 years ago

Alaska Robotics
A Comic Convention for Juneau -
[Image: Alaska Robotics Mini-Con: Click Here]
4 years ago

The Ester Republic
When Guns Left Campus - "by Carla Helfferich" The recent brouhaha about weaponry on the University of Alaska campuses has been giving me spasms in my old-timer muscles. I've be...
4 years ago

SOL in SOLDotma, Alaska
Miticche's Freedom to Discriminate and Hate Bill - Addendum/Correction: I've left the original post intact, but Miticche's bill might just exclude clergy, which is still unfortunate because they are already...
4 years ago

Henkinaa
Getting wrangled - Back to writing, in collaboration with my Brisbane friend Sian and the assistance of author wrangler Rachel & author wrangler assistant Cuihn Cattledog. An...
5 years ago

Ground Truth Trekking Blog
Bering Sea Coast trip - part 1 - as seen in the ADN - Obviously, I haven't been updating this in awhile. However, I did send an update to the ADN on the first leg of the expedition, and those of you who didn't...
5 years ago

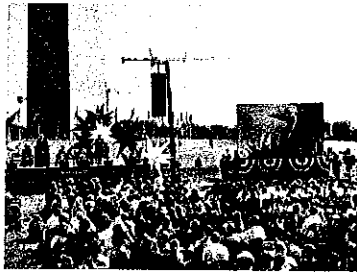
The Rogue Wave
This Afternoon at the RnR Bar, Radio Redux Radioplay Number 1 Narrator: Welcome to Kodiak, greatest fishing port in the world, located on the stormy East...
5 years ago

ALASKA CAFE
A New Direction For The Fisheries - Democracy worked recently in the latest gubernatorial race in Alaska in my opinion. Special interests lost and that's the way Alaskans wanted it. Since my ...
5 years ago

SHANNYN MOORE: JUST A GIRL FROM HOMER
Alaska - Just a Disconnect - Oh, my darling Alaskans. The wringing of

The Billionaire Behind Alice Rogoff

By Liz Ruskin, Alaska Public Media - May 13, 2014



David Rubenstein on the Jumbotron at the Washington Monument Monday. (Liz Ruskin)

The Washington Monument reopened this week for the first time since it was damaged in a 2011 earthquake. A ribbon-cutting ceremony Monday featured military bands, Interior Secretary Sally Jewell, Washington's mayor and TV weatherman Al Roker. But the man of the hour was David Rubenstein, who single-handedly paid half of the \$15 million repair bill.

[Download Audio](#)

"Seven and a half million dollars, which is incredible. Thank you David," Jewell said, one voice in a chorus of gratitude for Rubenstein that morning.

If you've heard anything about Alice Rogoff, the woman who recently bought the Anchorage Daily News, you'll likely know that she's married Rubenstein, the billionaire who co-founded the Carlyle Group, a Washington, D.C.-based private equity firm, and is No. 209 on the Forbes list of wealthiest Americans.

With his white hair and serious glasses, he looks a bit like the actor Steve Martin if he were playing someone wonky. Rubenstein says he may be the only person to have climbed up the Washington Monument in a suit and tie. His public speeches are often laced with witty, self-effacing asides. But when it was his turn at the microphone Monday, Rubenstein spoke only briefly.

"Many Americans have had good fortune," he said, his words undercut by the siren of a passing emergency vehicle. "I have had good fortune. And I really wanted to give back to the country and this is just a down payment on my obligation to pay back the country for what it has done for me and my family."

He's done a lot of what he calls "patriotic philanthropy" lately, and it's giving him a reputation makeover. After 9/11, Rubenstein became known as the mastermind of Carlyle Group. Conspiracy theories swirled around his private equity firm, mostly because it invested money from wealthy Saudis, and also because it hired ex-prime ministers and Pentagon bigshots who opened doors, making the firm rich. A more recent rumor, all over certain YouTube channels, has it that Carlyle Group is behind the disappearance of that Malaysian jet.



Rubenstein talks to news crews at the Washington Monument (Interior Department photo)

"Are we to believe the NSA's private surveillance army run by the Carlyle Group has no information on Flight 370?" the narrator of one video says, with spooky music playing in the background.

The allegation has been discredited by the conspiracy-debunkers at Snopes.com. But if you're inclined to believe in such things, a lack of evidence only proves it further.

Liz Ruskin, Alaska Public Media

<http://www.alaskapublic.org>

Liz Ruskin covers Alaska issues in Washington as the network's D.C. correspondent. She was born in Anchorage and is a West High grad. She has degrees from the University of Washington and the University of Missouri School of Journalism in Columbia. She previously worked at the Homer News, the Anchorage Daily News and the Washington bureau of McClatchy Newspapers. She also freelanced for several years from the U.K. and Japan, in print and radio. Liz has been APRN's Washington, D.C. correspondent since October 2013. She welcomes your news tips at [lruskin \(at\) alaskapublic \(dot\) org](mailto:lruskin@alaskapublic.org) | [About Liz](#)



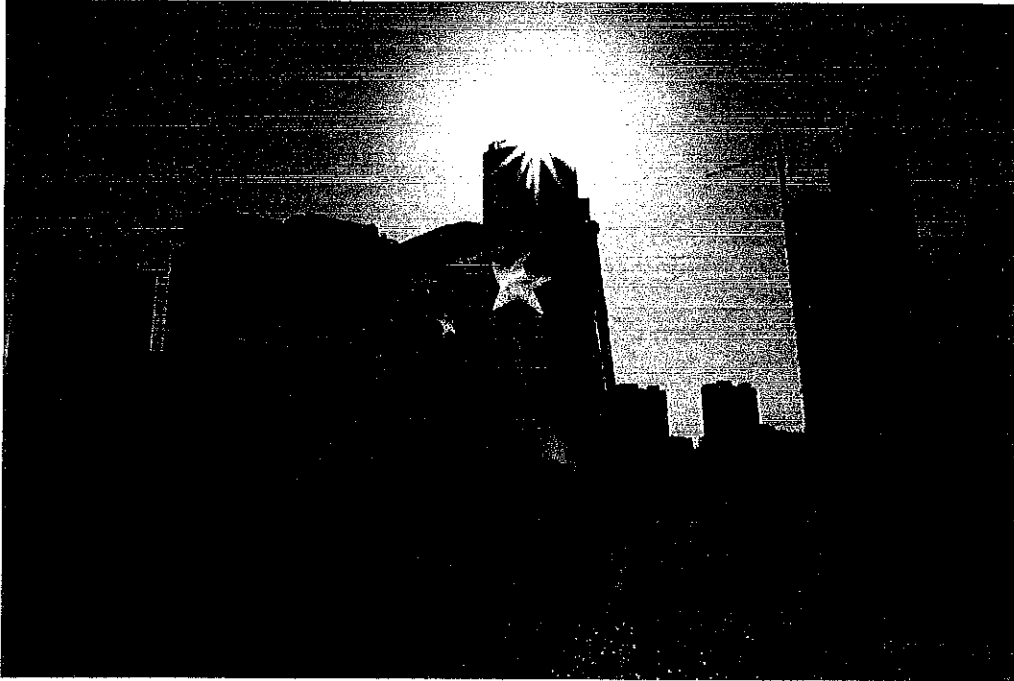
Select Language ▼

SUBSCRIBE TO OUR MORNING BEACON NEWSLETTER

SUBSCRIBE TO OUR BEACON EXTRA NEWSLETTER

Lawmaker Demands Hearing on Spread of Chinese Propaganda in Congress

Rep. Banks seeks to expose China Daily's subversion of U.S. law



Adam Kredo - DECEMBER 23, 2019 1:35 PM

Rep. Jim Banks (R. Ind.), a member of the House Armed Services Committee, is pressing congressional leaders to hold a hearing on the proliferation of Chinese Communist government-funded propaganda across Capitol Hill, according to official communications obtained by the *Washington Free Beacon*.

Following a *Free Beacon* exposé on the routine breach of federal law by *China Daily*, a propaganda organ run by the Chinese government, Banks is calling on his colleagues to investigate how and why Communist propaganda is arriving on the doorsteps of nearly every congressional office each day.

Banks spearheaded a related effort in September, when he petitioned congressional authorities and the Department of Justice to investigate *China Daily's* appearance across Capitol Hill.

The lawmaker's effort to hold the Communist Party paper accountable to federal law comes on the heels of a *Free Beacon* report exposing how *China Daily* has repeatedly violated federal disclosure laws by failing to tell officials how much it spends to publish regime-approved advertising in some of the nation's leading newspapers, including the *New York Times*, the *Washington Post*, and at least 30 others.

China Daily's advertising supplements are designed to look like they are part of a U.S. paper's reporting pages. The ads paint the Communist regime in a glowing light and downplay the nation's routine human rights abuses. The failure by *China Daily* to disclose how much it is spending on this influence campaign appears to violate the Foreign Agents Registration Act, or FARA, a federal statute designed to compel transparency in foreign influence operations.

Banks is continuing his effort to hold *China Daily* accountable and stop its spread across Capitol Hill amid fears the paper is influencing powerful members to take a softer approach to the Communist regime's abuses.

"*China Daily* is owned and bankrolled by the Publicity Department of the Communist Party of China—the agency responsible for monitoring and controlling all media produced in the one-party state," Banks wrote in a letter recently sent to the Committee on House Administration, a body that could provide oversight on the paper.

Banks has turned to the committee after his effort to pressure Chief House Administrator Philip G. Kiko to take action was rebuffed.

"In late September, I sent a letter to Chief House Administrator Philip G. Kiko, requesting he remove *China Daily* from circulation in Congress. He informed me that the 'review of the topical content' of congressional communications is outside of his jurisdiction. So, I've turned to your committee for assistance in combatting this threat," the letter said.

Citing the *Free Beacon's* latest reporting on the matter, Banks noted that "the Chinese Communist Party committed \$6.6 billion dollars to foreign propaganda efforts in 2009 and according to Foreign Agent Registration Act (FARA) receipts, has invested over \$20 million on the *China Daily* since 2017."

Banks is concerned that *China Daily* and its advertising organ, the National News Agency, are "helping an authoritarian dictator influence American democracy."

"Uninformed staffers could easily mistake *China Daily* for a legitimate news source regarding China-U.S. relations and the Chinese regime's policies," Banks wrote. "That's clearly the intention of the Chinese Communist Party."

Congressional hearings on the matter could help pave the way for legislative remedies that would prohibit *China Daily* from making its way to Capitol Hill. One solution could be to enact a ban on FARA-registered publications from being delivered to federal buildings.

"This would include *China Daily* and other state-owned propaganda outlets like *Russia Today*," Banks wrote in his letter. "The committee could also draft a House rule mandating the inclusion of a disclaimer on all state-owned newspapers delivered to congressional offices. Such a disclaimer should identify the newspaper as propaganda and name the foreign government that produces and finances it."

Banks further requested that such efforts be considered immediately.

"There's a lot of rhetoric in Congress about 'combatting Chinese influence' and being 'tough on China,' he wrote. "Americans won't take our claims seriously if we can't prevent China from running a propaganda campaign in our own workplace."

China 'used secret microwave pulse weapon to cook Indian soldiers alive' and force them into retreat in Himalayan border battle

Electromagnetic weapons were allegedly used on disputed Himalayan border
They cleared out Indian troops without violating ban on gunfire, a professor said
It came weeks after soldiers fought with rocks and clubs in a deadly brawl

By TIM STICKINGS FOR MAILONLINE

PUBLISHED: 05:27 EST, 17 November 2020 | UPDATED: 15:46 EST, 17 November 2020

Chinese troops used 'microwave' weapons to force Indian soldiers to retreat by making them violently sick during a Himalayan stand-off, a professor has claimed.

The electromagnetic weapons which cook the human tissue of enemy troops 'turned the mountain tops into a microwave oven' and made the Indian soldiers vomit, international studies expert Jin Canrong told his students in Beijing.

The microwave weapons heat water molecules in the same way as the kitchen appliance, targeting water under the skin and causing increasing amounts of pain to the target from ranges of up to 0.6 miles away.

Jin hailed the Chinese forces for 'beautifully' executing the move which cleared out Indian troops without violating a ban on gunfire along the disputed border.

It is the first known use of microwave weapons on a battlefield.

According to The Times, the weapons were said to have been deployed in late August, weeks after a deadly brawl involving rocks and clubs which killed at least 20 Indian soldiers and brought the two nuclear-armed powers closer to war than they have been in 53 years on one of the world's highest-altitude battlefields.

Jin told his students that within 15 minutes of the weapons being deployed, 'those occupying the hilltops all began to vomit'.

'They couldn't stand up, so they fled. This was how we retook the ground,' he explained.

China's forces decided to use the weapons because the altitude was too high to fight against a team of Tibetan mountaineering specialists, Jin said.

Gunfire is banned under an old agreement, although there were warning shots in September in an exchange of fire which both sides blamed on each other.

While the US has also developed microwave-style weapons, China's alleged use of them may be the first against enemy troops anywhere in the world.

Also envisioned for use in crowd control, the weapon works by heating the water under the skin to painful temperatures which force people out of the area.

The sensation was once described in a medical journal as equivalent to touching a hot lightbulb. Overexposure to radiation can also cause headaches, nausea and vomiting.

China's so-called Poly WB-1 was first put on display at an air show in 2014 and was thought to be supplied to Chinese naval forces.

The tools are known as 'microwave' weapons because they have a similar effect to the type of oven, although technically the radiation is in the form of millimetre waves rather than microwaves.

There is some suspicion that similar weapons were used against US diplomatic personnel who mysteriously fell ill in China and Cuba in a series of incidents beginning in 2016.

America's equivalent 'heat ray', the Active Denial System, was unveiled in 2007 and deployed to Afghanistan but apparently never used against hostile troops.

The Pentagon touted it as 'the first non-lethal, directed-energy, counter-personnel system with an extended range greater than currently fielded non-lethal weapons'.

Fears of a political backlash were thought to have contributed to its withdrawal from Afghanistan, although the US government said it complied with international law.

News of the weapon's alleged use in the Himalayas comes as China and India discuss ways to de-escalate tensions on the rugged mountain frontier.

The nuclear-armed neighbours have deployed tens of thousands of troops since tensions erupted into the deadly medieval-style clash in June.

India said 20 of its soldiers were killed in the night-time brawl which is thought to have involved up to 900 soldiers, while China acknowledged casualties but did not give figures.

Post-mortems showed that the 'primary reason for death is drowning and it looks like they fell from a height into the water because of head injuries,' one Indian official said.

Both sides blamed each other for provoking the conflict, while the US took India's side by offering 'deepest condolences' to the soldiers killed.

The two sides are now discussing a staggered disengagement from the border area where temperatures have dropped to -18C, Indian officials said.

'We have a firm plan for disengagement on the table, it is being internally discussed on both sides,' said one of the officials.

Under the plan that was shared during a meeting of top commanders last Friday, both sides will pull back from the contested Pangong Tso lake area and establish a buffer zone.

Chinese soldiers will dismantle defence structures on several hilly spurs overlooking the lake and pull back, officials briefed on the discussions said.

India, which has occupied heights on the lake's south bank, will also withdraw. Both sides will cease patrolling certain sections.

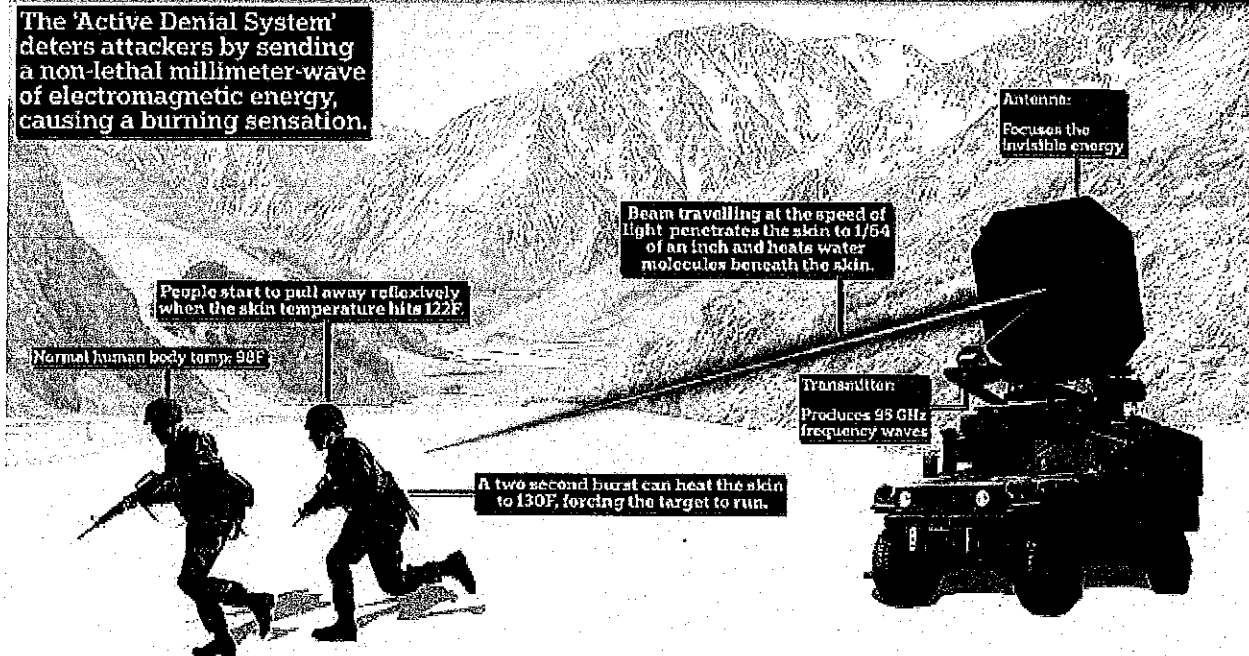
The two countries fought a full-scale war in 1962 and both continue to lay claim to thousands of square miles of territory.

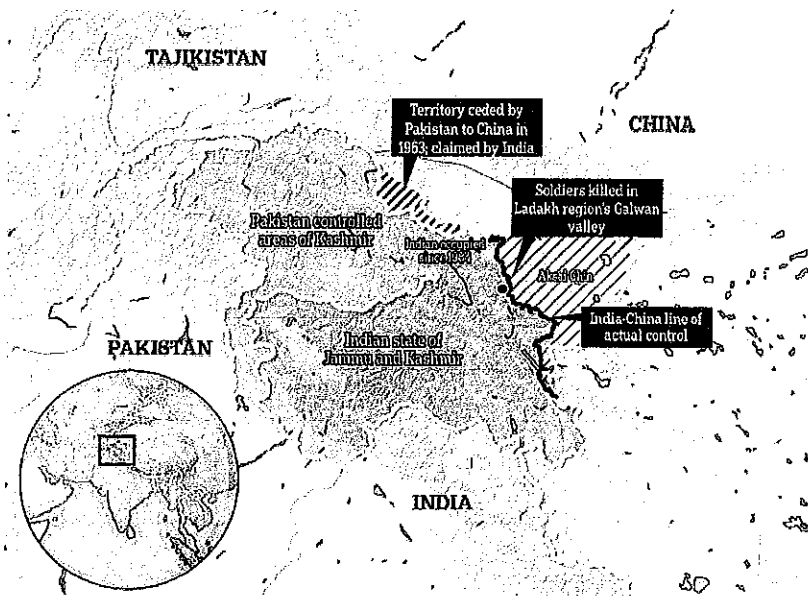




HOW DO MICROWAVE WEAPONS WORK?

The 'Active Denial System' deters attackers by sending a non-lethal millimeter-wave of electromagnetic energy, causing a burning sensation.





DECEMBER 15, 2020AUTHOR: SUZANNE DOWNING

Breaking: State disconnects SolarWinds software, same as attacked by Russians

<https://mustreadalaska.com/state-disconnects-solarwinds-software-same-as-attacked-by-russians/>

The State Security Office has been notified by the Cybersecurity and Infrastructure Security Agency (CISA) that some versions of a system monitoring software the state uses is being exploited by "malicious actors."

Those malicious actors are believed to be Russian spies, or foreign intelligence workers, as they are being called. SolarWinds Orion products have been attacked by Russian hackers all over the United States.

On Monday, all State of Alaska departments that have SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, on their network were instructed to immediately disconnect or power down the products from their networks.

The State Security Office said that until it gets the Windows operating system rebuilt and reinstalls the patched SolarWinds software, departments are prohibited from rejoining the Windows host operating system to the "enterprise domain."

Additionally, information technology officers in the State of Alaska have been instructed to block all traffic to and from hosts, external to the enterprise, where any version of the SolarWinds Orion software has been installed.

On Sunday, CISA issued Emergency Directive 21-01 that calls on all federal civilian agencies to review their networks for signs of compromise and disconnect or power down SolarWinds Orion products immediately.

"The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks," said CISA Acting Director Brandon Wales. "Tonight's directive is intended to mitigate potential compromises within federal civilian networks, and we urge all our partners—in the public and private sectors—to assess their exposure to this compromise and to secure their networks against any exploitation."

Since at least March, Russian hackers have inserted malicious updates into IT management platforms, hitting the U.S. Departments of Commerce, Treasury, and Homeland Security, as well as a security firm called FireEye.

SolarWinds has hundreds of thousands of clients. On Monday, the company told the Security and Exchange Commission that at least 18,000 were potentially attacked.

Both FireEye and Microsoft have accounts of what the threat entails. It appears that is so vast that no one really knows the extent of it.

Attackers used Orion software as a door into computer systems, where they were able to steal administrative tokens, and then go in and out of the system with data.

The attacks were first reported by Reuters on Sunday.

SolarWinds said in a statement that hackers had managed to alter the versions Orion, a network monitoring tool, that were released in March and June.

"We have been advised this attack was likely conducted by an outside nation state and intended to be a narrow, extremely targeted, and manually executed attack, as opposed to a broad, system-wide attack," SolarWinds wrote.

Maersk's Cargo Operations Hit Hard by Cyberattack

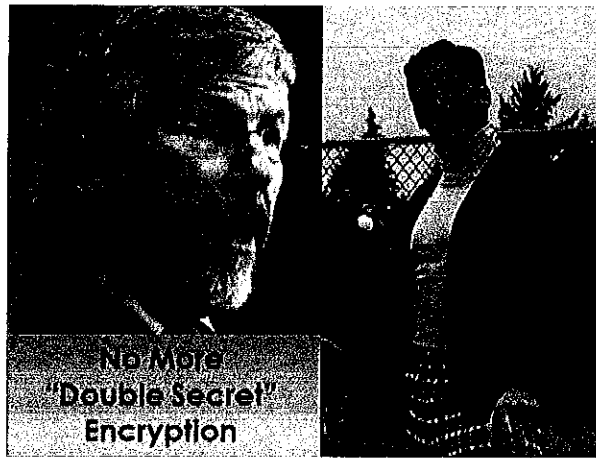


PHOTO COURTESY OF A.P. MOELLER-MÆRSK

BY THE MARITIME EXECUTIVE 09/28/2017 08:47:22

New details emerged Wednesday on the extent of the "Petya" ransomware attack on A.P. Moller-Maersk (Maersk Group), one of the world's most prominent maritime conglomerates. The attack has affected Maersk's container bookings and its terminal operations, with as-yet-unknown implications for the firm's revenue.

In an update posted at 10:45 hours GMT, Maersk said that the attack has been contained, but that it has been forced to shut down multiple systems in order to prevent the "Petya" malware from spreading. The firm said that it has not lost any data, and the majority of its business units – Maersk Oil, Maersk Drilling, Maersk Supply Services, Maersk Tankers, Maersk Training, Seafar and MCL – have not



A young Otter fought his fraternity's "Double Secret Probation" in National Lampoon's *Animal House*. His older dead ringer, an attorney for the National Intelligence Agency is fighting encryption. To bolster his political case the lawyer is cheering for terrorist hi-jinks, in the same way 9-11 pushed through the Patriot Act. The Carlyle Group, with an Insider on President Obama's Intelligence Advisory boards, recently acquired two cyber-security firms, Novetta Solutions and CoalfireSystems. You can't make this stuff up, it's there for the pickin'.

Posted by PEU Report/State of the Division at 8:59 PM

Wednesday, September 16, 2015

Chertoff & Carlyle Group Bet on CyberSecurity: Buy Coalfire



Businesswire reported:

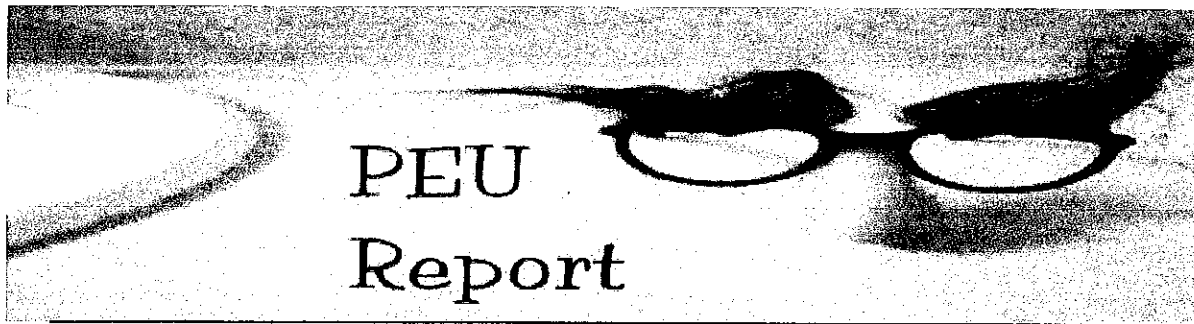
Global alternative asset manager The Carlyle Group (NASDAQ: CG) and The Chertoff Group, a global security and risk management advisory firm, today announced they have acquired a majority stake in Coalfire Systems, Inc.

Founded in 2001 and based in Louisville, Colo., Coalfire is a global cybersecurity and technology services provider specializing in cyber risk advisory, compliance assessments, technical testing and software services for private enterprises and government organizations. With its technical depth and breadth of IT services, Coalfire serves clients in sectors including technology, retail, payments, healthcare, financial services, education, local and state government and utilities.

This deal comes just weeks after Carlyle bought Novetta Solutions. At the time I wrote:

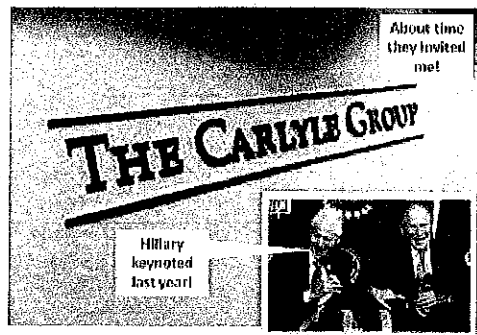
Carlyle Managing Director Julius Genachowski serves on **President Obama's two intelligence boards**, so he is in a unique position to see government intelligence needs and advise Carlyle's triumvirate to invest accordingly. His bio on Carlyle's website stated:

Mr. Genachowski has **long advised President Obama on technology issues.**

[More](#)

Wednesday, September 23, 2015

Carlyle's Investor Meeting Hears from Another Ex-President



PE Hub reported:

Former President **George W. Bush**, brought a smile to faces at **Carlyle Group's** annual meeting last week. Our spies tell us "Dubya" put on an altogether friendly, light-hearted keynote speech talking about family and life post most-powerful-man-in-the-world.

It's not clear how much the former president commands for his keynote presence, though several media reports pegged it between **\$100,000 and \$175,000**. Sources tell us George W. also was the featured speaker at this year's annual meetings for **Blackstone Group** and **Vista Equity Partners**. No one from Blackstone or Vista returned requests for comment.

W. had an impact on several of Carlyle's air travel affiliates. He served as a board member for CaterAir, back when airlines provided catering to the whole plane, not just first class. W.'s rendition practices were rumored to boost the bottom line for Carlyle affiliate Landmark Aviation, which Carlyle just round-tripped for over \$2 billion. Lots to yuck-yuck about between W. and Carlyle's PEU boys.

Don't forget W. let the Bin Ladens fly home after Carlyle's 2001 investor meeting when virtually everyone else was grounded. W. earned this invite a long time ago.

Posted by PEU Report/State of the Division at 10:19 PM

Tuesday, September 22, 2015

Carlyle Upscales Silicon Valley Home Park

Insider Architect of the Implosion

"I had a choice. I could be an insider or I could be an outsider. Outsiders can say whatever they want. But **people on the inside don't listen to them**. Insiders, however, get lots of access and a chance to push their ideas. People — powerful people — listen to what they have to say. But insiders also understand one unbreakable rule: They **don't criticize other insiders**."—Larry Summers, Ph.D.

Testimonials

The *PEU Report* is absolutely brilliant and has given me faith that someone out there has **noticed what is going on** in the world. —Ex-Bloomberg reporter

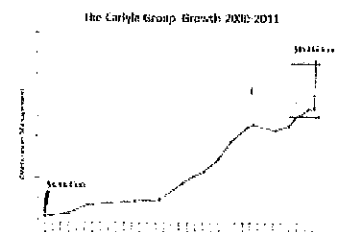
I really can't say enough how much I enjoy your commentary on *PEU*. You manage to dig into the details and sum it up in a way that is so succinct and entertaining. —Ex-Bloomberg reporter

When Tim Geithner, the former Treasury secretary, takes over as president of Warburg Pincus, the private-equity firm, even a high-school dropout can discern a pattern. —Another person who noticed

PEU = Private Equity Underwriter

As income and wealth rises to the top, so does political power.

The Carlyle Group



Broke \$100 Billion Under

As in robber baron old and PEU new. Old schoolers have long dined on the bones of many. The lunchroom is a place for the new generation, including Hunter Biden, to express their appetite for power and greed.

Posted by PEU Report/State of the Division at 9:06 AM

Tuesday, September 29, 2015

Carlyle Group: Employee Owned PA Consulting Goes PEU



THE CARLYLE GROUP

"support a step-change in our rate of growth"

WEDNESDAY

PA Consulting Group and The Carlyle Group announce agreement on future investment and joint partnership plan

"continue to maintain our independence"

"our discussions have borne fruit because the PA team have recognized a cultural affinity between the two groups" "sharing of value created"

NASDAQ reported:

PA Consulting Group and The Carlyle Group (CG) announced they have signed an agreement for Carlyle to invest in PA for a **51 percent shareholding of the company**. The investment values PA at \$1 billion and is expected to close in December 2015.

That means Carlyle is the majority shareholder and can make decisions without regard to the other 49%. PA's press release described the firm as follows:

PA is an employee-owned firm of over 2,500 people, operating globally from offices across North America, Europe, the Nordics, the Gulf and Asia Pacific. Our specific expertise is in energy and utilities, financial services, health, life sciences, consumer and manufacturing, government, defence and security, transport and logistics.

Our deep industry knowledge together with skills in management consulting, technology and innovation allows us to challenge conventional thinking and deliver exceptional results with lasting impact.

Ask the 2,500 PA employees in two years how they like Carlyle ownership. I'd love to hear their assessment of Carlyle's culture and values on their once employee owned company. Will they see Carlyle's vulture culture and callous values? That would be my wager.

PA Consulting is in a unique position to chronicle the impact of private equity ownership on a company. However PA is in a double bind. They cannot be honest and keep Carlyle's good name, a longstanding prime objective. When all else fails throw out the measure or the messenger. It's the PEU way.

Update 2-20-20: Carlyle is ready to cash in on PA Consulting and prefers to sell the company to another private equity firm. That way the public doesn't see how much cash Carlyle pulled out of PA during five years of ownership.

Posted by PEU Report/State of the Division at 8:21 PM

Monday, September 28, 2015

Alaska Should Aggressively Pursue Investment Returns



USAID to Help Young Biden: The Burisma File Economic Policy

Journal reported : Senate Bill 2277 "directs the U.S. Agency for International Development to guarantee loans for...



Hunter Biden & The Carlyle Group: Ukrainian Gasbags Business

Insider reported : Hunter Biden, the youngest son of Vice President Joe Biden, has been appointed to the board of directors ...

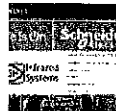


PEU Lover Bill Clinton The American people were subject to former President Bill Clinton last night. Jeffrey Epstein's close friend spoke at the Democratic...



Mitt Romney's Foreign Policy Adviser: PEU & Biden

Partner Three months ago Vice President Joe Biden discounted Mitt Romney's foreign policy as out of date and "back to the future." ...



Carlyle Performing Airport Body Temperature Scans The Carlyle Group's latest product in its COVID-19 portfolio is airport body scanners that detect passengers with fever. At the L...



Milken Global Institute Starts 10-12 The Milken Global Institute, the U.S. version of Davos, begins tomorrow. This is the first gathering since President Donald Trump pardoned ...



Rubenstein's PEU Life: How to Greed Carlyle Group co-founder David Rubenstein authored the book "How to Lead: Wisdom from the World's Greatest CEOs, Founders and Gam...



Rubenstein Says Get Used to Deaths, Go Back to Work

What's this Washington insider and billionaire's wife doing in Alaska?



The *Alaska Dispatch* is owned by Alice Rogoff Rubenstein, wife of Carlyle Group co-founder David Rubenstein. Harvard Economist Kenneth Rogoff recently weighed in with a column in the *Alaska Dispatch*. It stated:

Alaska has a **sovereign wealth fund slightly in excess of 100 percent of state GDP**, more than enough to cover both **state debt of about 20 percent of GDP** (even including local debt) and unfunded state pension liabilities.

There is certainly scope to manage the sovereign wealth fund somewhat **more aggressively**, at the very least the **amount in excess of the state's debt**. Other resource-dependent countries like Norway try to strike a balance between risk and return. It would probably behoove Alaska to **look at other sovereign wealth funds** and how they are managed.

Rogoff recommends rolling the dice on 80% of the funds assets, which generally means private equity. Numerous Middle East sovereign wealth funds invest with The Carlyle Group. Carlyle co-founder David Rubenstein regularly visits Alaska. Rogoff's piece closed with a short bio:

Kenneth Rogoff is a professor of economics at Harvard and former chief economist for the International Monetary Fund. He is **the cousin** of Alaska Dispatch News owner and publisher Alice Rogoff.

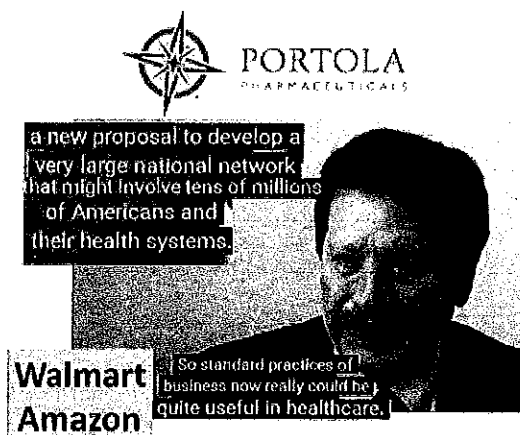
Rogoff did not mention public pension funds which have questioned private equity's outsized fees that dampen returns. Kenneth Rogoff went for the happy comparison.

It's all in the PEU family, where image counts for much.

Posted by PEU Report/State of the Division at 10:01 PM

Sunday, September 27, 2015

FDA Nominee Served on Portola Pharmaceuticals Board



Yahoo Finance reported :
The tradeoff between reopening the country and exacerbating the coronavirus outbreak is "the big problem w..."



Carlyle Adds Two COVID-19 Investments, TriNetX and Victory

Innovations

The Carlyle Group added disinfecting equipment maker Victory Innovations and research organization TriNetX to its substantial coronavirus...



Supreme Avoids Carlyle PEU Supreme sponsored an Instagram

video by comedian Katt Williams. Williams tackled the coronavirus, President Trump and Black Live Matter...

News Release

Mon, 20 March 2017

2017-017

The Carlyle Group Acquires Arctic Glacier from H.I.G Capital

Investment From Carlyle's Long-Dated Fund To Support Arctic Glacier's Growth Strategy in North America

Montclair, NJ – Arctic Glacier Group Holdings, Inc., H.I.G. Capital, LLC and The Carlyle Group (NASDAQ: CG) today announced that Carlyle Global Partners, Carlyle's long-duration investment fund, has completed the acquisition of Arctic Glacier from an investment fund managed by H.I.G. Capital and its existing shareholders. Terms of the transaction have not been disclosed.

Arctic Glacier is a producer and distributor of high-quality packaged ice to consumers in the United States and Canada. Arctic Glacier operates 46 production plants and 52 distribution facilities across Canada and the northeastern, central and western United States servicing more than 75,000 retail accounts.

"Arctic Glacier has established a leading position in the North American packaged ice market due to the company's investments in, and our employees' complete dedication to, the highest levels of product quality and customer service," said Fred Smagorinsky, Chief Executive Officer of Arctic Glacier.

"H.I.G. Capital has fully supported the execution of our strategy and made significant investments in our business over the course of its ownership. Our management team is excited to begin the next phase of our growth trajectory by partnering with The Carlyle Group. Carlyle's long-term investment vision, substantial supportive resources and collaborative approach will be tremendous assets for Arctic Glacier as we pursue our mission of becoming the top packaged ice company in North America," said Smagorinsky.

"Arctic Glacier is a great fit for Carlyle Global Partners due to its leading market positions, strong customer relationships and outstanding management team," said Tyler Zachem, Managing Director and Co-head of Carlyle Global Partners. "We look forward to partnering with the Arctic Glacier team to support the company's growth strategy."

The Carlyle Group was advised by Credit Suisse, Ernst & Young LLP, Kirkland & Ellis LLP and Latham & Watkins LLP. The sellers were advised by Piper Jaffray and Ropes & Gray LLP.

* * * * *

We use cookies to enhance your experience on our site. By using our site, you agree to our use of cookies. For more information, see our Cookies Policy.

ACCEPT

DENY

Fred Smagorinsky
+1-917-246-4101
fsmagorinsky@arcticglacier.com (mailto:fsmagorinsky@arcticglacier.com)

The Carlyle Group:

Elizabeth Gill
+1-202-729-5385
Elizabeth.gill@carlyle.com

H.I.G. Capital:

Rick Rosen
rrosen@higcapital.com (mailto:rrosen@higcapital.com)
+1-305-379-2322

Peter Gudwin
+1-212-506-0500
pgudwin@higcapital.com (mailto:pgudwin@higcapital.com)

#

© 2020 Carlyle Investment Management L.L.C. All rights reserved.

[Transparency & Reporting](#)

[Cookies Policy](#)

[Privacy Notice](#)

[Terms of Use Policy](#)

We use cookies to enhance your experience on our site. By using our site, you agree to our use of cookies. For more information, see our Cookies Policy.

ACCEPT

DENY

Congress of the United States

Washington, DC 20510

December 6, 2019

Sami Mnaymneh
Founder and Co-Chief Executive Officer
H.I.G. Capital, LLC
1450 Brickell Avenue 31st Floor
Miami, FL 33131

Tony Tamer
Founder and Co-Chief Executive Officer
H.I.G. Capital, LLC
1450 Brickell Avenue 31st Floor
Miami, FL 33131

Dear Messrs. Mnaymneh and Tamer:

We are writing to request information regarding H.I.G. Capital's (H.I.G.) investment in Hart InterCivic Inc. (Hart InterCivic) one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.¹ For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"² owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimmed on security in favor of convenience," leaving voting systems across the country "prone to security problems."³ In light of these concerns, we request that you provide information about your firm, the portfolio

¹ Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, <https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/>; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, <https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html>.

² ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It," Jessica Huseman, October 28, 2019, <https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it>.

³ Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>.

companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early 2000s, almost twenty vendors competed in the election technology market.⁴ Today, three large vendors—Election Systems & Software, Dominion Voting Systems, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.⁵ Private equity firms reportedly own or control each of these vendors, with very limited “information available in the public domain about their operations and financial performance.”⁶ While experts estimate that the total revenue for election technology vendors is about \$300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.⁷

Concentration in the election technology market and the fact that vendors are often “more seasoned in voting machine and technical services contract negotiations” than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems—leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.⁸ In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider “the cost to purchase or lease, operate, and maintain a voting system over its life span ... [and to] know how the vendor(s) plan to be profitable” when signing contracts, because vendors typically make their profits by ensuring “that they will be around to maintain it after the sale.” The EAC has warned election officials that “[i]f you do not manage the vendors, they will manage you.”⁹

Election security experts have noted for years that our nation’s election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States’ election infrastructure as “critical infrastructure” in order to prioritize the protection of our elections and to more effectively assist state and local election

⁴ Bloomberg, “Private Equity Controls the Gatekeepers of American Democracy,” Anders Melin and Reade Pickert, November 3, 2018, <https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy>.

⁵ Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

⁶ Id.

⁷ Id.

⁸ Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf;

Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

⁹ U.S. Election Assistance Commission, “Ten Things to Know About Selecting a Voting System,” October 14, 2017, <https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/>.

officials in addressing these risks.¹⁰ However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk.¹¹ In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state “using some machines that are no longer manufactured.”¹² Moreover, even when state and local officials work on replacing antiquated machines, many continue to “run on old software that will soon be outdated and more vulnerable to hackers.”¹³

In 2018 alone “voters in South Carolina [were] reporting machines that switched their votes after they’d inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana.”¹⁴ In addition, researchers recently uncovered previously undisclosed vulnerabilities in “nearly three dozen backend election systems in 10 states.”¹⁵ And, just this year, after the Democratic candidate’s electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county’s Republican Chairwoman said, “[n]othing went right on Election Day. Everything went wrong. That’s a problem.”¹⁶ These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

H.I.G. reportedly owns or has had investments in Hart InterCivic, a major election technology vendor. In order to help us understand your firm’s role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the *Stop Wall Street Looting Act*.¹⁷
2. Which election technology companies, including all affiliates or related entities, does H.I.G. have a stake in or own? Please provide the name of and a brief description of the services each company provides.

¹⁰ Department of Homeland Security, “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector,” January 6, 2017, <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.

¹¹ AP News, “US election integrity depends on security-challenged firms,” Frank Bajak, October 29, 2018, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>; Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

¹² Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

¹³ Associated Press, “AP Exclusive: New election systems use vulnerable software,” Tami Abdollah, July 13, 2019, <https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1>.

¹⁴ Vice, “Here’s Why All the Voting Machines Are Broken and the Lines Are Extremely Long,” Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.

¹⁵ Vice, “Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials,” Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

¹⁶ New York Times, “A Pennsylvania Country’s Election Day Nightmare Underscores Voting Machine Concerns,” Nick Corasaniti, November 30, 2019, <https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html>.

¹⁷ Stop Wall Street Looting Act, S.2155, <https://www.congress.gov/bill/116th-congress/senate-bill/2155>.

- a. Which election technology companies, including all affiliates or related entities, has H.I.G. had a stake in or owned in the past twenty years? Please provide the name of and a brief description of the services each company provides or provided.
- b. For each election technology company H.I.G. had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
 - i. The name of the company
 - ii. Ownership stake
 - iii. Total revenue
 - iv. Net income
 - v. Percentage of revenue dedicated to research and development
 - vi. Total number of employees
 - vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
 - viii. Other private-equity firms that own a stake in the company
3. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.
4. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.
5. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.
6. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.

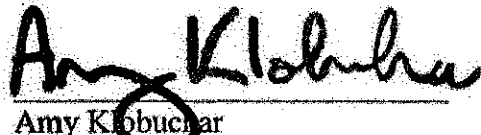
7. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,



Elizabeth Warren
United States Senator



Amy Klobuchar
United States Senator



Ron Wyden
United States Senator



Mark Pocan
Member of Congress

The natural progress of things is for liberty to yield and government to gain ground. --THOMAS JEFFERSON, 1768

[Contact](#) [Privacy](#) [Q](#) [f](#) [U](#) [G+](#) [in](#)

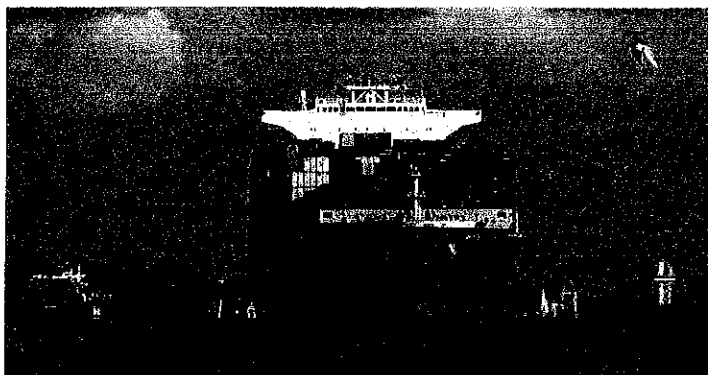


LIB UNYIELDING

[Home](#) [Latest Columns](#) [Quick Takes](#)
[LU Web Crawler](#) [About](#) [Store](#)

Uranium jerky: Coincidences with shipping, big data, and a special niche of the industry – Part VI

By J.E. Dyer [📅](#) November 2, 2020



Pixabay

[f](#) Share [🐦](#) Tweet [📺](#) Flip [🔗](#)

This article, the sixth in a six-part series, continues an exploration of some strange and remarkable incidents in and related to the history of the uranium trade in the years 2008 and 2009. The justification for having this interest, in the middle of the most crucial U.S. election in at least 150 years, is laid out in the introduction to **Part II**.



Space Force Genuine \$2 Bill
 Made In The USA | Satisfaction
 Guaranteed | Certificate Of Authenticity
 Included

[D](#) X

The first five parts of the series reviewed incidents and trends with direct implications for two particular episodes: the involvement of Goldman Sachs in trading and possessing physical uranium starting in 2009 (discussed in **Part I**); and the weird history of the freighter *M/V Arctic Sea*, which supposedly went missing in the Eastern Atlantic for 15 days in 2009 – yet actually didn't (laid out in **Part II**).

Part II and **Part III** surveyed some very unusual details ("the deets") that involved a vast cross-section of actors, from Russia to the Clintons to George Soros and his connections in Eastern Europe.

In **Part IV**, we looked at hints that the supposed "hijacking" of *Arctic Sea* was related to the ship carrying special material, possibly nuclear, at some point in her voyage. Part IV concluded with a look at the ship's fate after 2009, which was an unusual interlude for the next two years until she was sold to a charter freight company in late 2011.

x

Our Privacy Policy has been updated to support the latest regulations.

[Click to learn more.](#)



Anonymously.

Trending: Could Trump sue Lin Wood for legal malpractice?

Part V continued with a look at some unique and interestingly contemporaneous developments surrounding the *Arctic Sea* transit in 2009, with a focus on the movement of uranium and other nuclear-related material. It was a time of eye-opening and untoward nuclear-linked events, from mafia involvement in radioactive waste disposal to bribery in the uranium transport industry – a pattern of corruption that encompassed firms and activities with links to the Clintons, and allegedly even involved the Clintons themselves.

When we left the topic, a Russian firm that was reportedly bribing the Clintons was in turn being bribed by a U.S. logistics firm that specializes in uranium transport. We're still calling that coincidence, for now. As Part V noted, there was a strange, coincidental coincidence in which the consulting and investment firm of a pair of Clinton cronies figured prominently.

In Part VI, we turn to some additional coincidences of timing and relevance from this remarkable period.

This article is about coincidences with no obvious direct, specific connections to the *Arctic Sea* incident or a demonstrated link to Goldman Sachs's uranium foray. Nevertheless, they have an obvious generic connection to quite a few of the plot features we've surveyed to date. The first one leads off Part VI's focus on the shipping side of the equation.

The NSA of global trade

That coincidental circumstance is the founding in 2010 of the shipping-data tracking company CargoMetrics, by former Coast Guard officer and maritime-affairs specialist Scott Borgerson, who is **alleged to be Ghislaine Maxwell's boyfriend**. (He says he's not.) Maxwell was reportedly living in a house owned by Borgerson for much of 2019, until she bought a place of her own in New Hampshire – the home at which she **was arrested by the FBI** on 2 July 2020.

Maxwell's connection to Borgerson goes back to around 2013, reportedly encompassing a common interest between the two in the future of the Arctic and its environment.



✕

Our Privacy Policy has been updated to support the latest regulations.

Click to learn more.



Scott Borgerson; Ghislaine Maxwell at the Arctic Circle conference in 2014. Arctic Circle video via The Australian

But **CargoMetrics** is of particular interest to us given the company's mission, which is to **maintain running data on global shipping** – cargo and ship movements – to a level of such granularity that investment and futures-trading decisions can be made about the goods being shipped and the industries represented by them, based on analysis of the trends thus revealed.

That, at least, is a description designed to sell the company products, which now include a quantitative investment fund, to futures traders and investors, whose interest is in the trends more than the goods.

But a telling feature of CargoMetrics' M.O. is the one expressed in **Borgerson's trademark slogan** from the outset: "We aim to be the NSA of global trade."



Here is how a summary of a Borgerson presentation put it in CargoMetrics' earliest years:

It is incredibly costly to buy every possible source of trade data, and have a supercomputer to run algorithms in real time to cross-reference sources against vessel movements. CargoMetrics must be generating government-scale quantities of fresh data every day. According to Dr Borgerson, an early investment in Amazon cloud servers is paying dividends. He refused to say more about the inner workings of CargoMetrics, beyond that "we archive all the data -- it's a searchable Google of trade".

What CargoMetrics started as in 2010, therefore, is a firm that keeps a gigantic database. The database can pump out not only algorithmic interpretations of trends, but reams and reams of information about, very specifically, what is being shipped where, and how much.

CargoMetrics' commercial service may not be intended to provide even more specific data on a one-stop shopping basis, such as the derived (or overtly present) identities of shippers, sellers, and buyers. As far as I can tell, Borgerson has never suggested that it is. But it's minable for information that would help derive those specifics.



Our Privacy Policy has been updated to support the latest regulations.

Click to learn more.



Data-fied. Public Domain; LU Staff

In that sense, it has a very particular similarity to NSA's trademark data store. Remember, NSA's *intended* service isn't unmasking Americans, as individuals, in their discrete communications events. But the data that flow through the NSA mechanisms generate a minable source from which to derive such information. The limits of the intended service haven't stopped government agencies from mining the NSA-brokered data trove for exactly that specific, granular information about U.S. persons.

There are a lot of customers who would have an interest in such information about shipping and cargo. The late Jeffrey Epstein and Ghislaine Maxwell would certainly be among them. Their whole profession was centered on holding certain types of information over powerful political and corporate officials; i.e., having "dirt" on them.

Being brokers of such information could also be very profitable. What people are shipping around the world is one of the most important things to know about what's going on in it, especially when it comes to quantities like arms, drugs, cash, human traffic, energy commodities and products – and, among other high-value mineral commodities, nuclear material.

Where big data go, one guy's never far behind

Borgerson doesn't explicitly hawk his product in those terms. (He **stepped down** as CEO of his company about a month ago, after the media frenzy began over his connection to Ghislaine Maxwell.) We'll see below the commercial-focused direction he took CargoMetrics after its initial debut as a big-data vendor.

But tracking ships and cargo, at the level of patterns and expectations that would help maintain a security posture, is certainly important to homeland security, and it's through this nexus that we find a link of exceptional interest in 2009.

Bear in mind that Borgerson wanted CargoMetrics to be the "NSA of global trade." Obviously, that was a gleam in his eye well before the company was founded in 2010. CargoMetrics needed investors to get it off the

ground, and in 2007, Borgerson **had met a fellow former Coast Guard officer, Randy Beardsworth**, at a Coast Guard Academy dinner. Borgerson had been named a fellow of the Council on Foreign Relations the same year, and was making a reputation as a maritime affairs expert.

Beardsworth was a partner in Catalyst Partners, a D.C. consultancy specializing in homeland security. He and Borgerson hit it off, and in 2009, when Borgerson was looking for investors, he approached Beardsworth for advice.

Although this may have been solely because of their earlier connection, it seems like a good bet that it had something to do with what Beardsworth was doing at the time: **chairing a government interagency group**, working for the new Obama administration on a plan to consolidate the National Security Council and the Homeland Security Council (which were separate advisory bodies when Obama took office). Borgerson was a CFR

Our Privacy Policy has been updated to support the latest regulations.

Click to learn more.



Scott Borgerson (R), in discussion with former Iceland Pres Ólafur Ragnar Grímsson, CFR conference on the Arctic, 2013. CFR video, YouTube

At the top of the totem pole for that consolidation project, just under Barack Obama, was Obama's Homeland Security Adviser and counterterrorism "czar," John Brennan.

Prior to initiation of the consolidation review for the HSC and NSC, Randy Beardsworth had been on the **Obama transition team** after the 2008 election, working with Brennan on the homeland security and counterterrorism portfolio. In fact, Beardsworth's **background in homeland security** included his being among the first executive-level officials of the Homeland Security Department when it was created under George W. Bush, a career detail that would have brought him in contact with the first director of what became the National Counterterrorism Center (NCTC) — John Brennan.

It matters that Beardsworth was the ops chief for Border and Transportation Security, supervising, among other things, the Transportation Security Agency (TSA). We'll go into that in more depth in a separate article; for the purposes of this one, the relevant points are that (a) TSA's mission, which included keeping tabs on a no-fly list, was one of the main reasons John Brennan wanted his own contract workers from The Analysis Corporation (TAC) to be embedded at the NCTC (see links below); and (b) Beardsworth was well aware of the significance of big-data gathering on millions of individuals to homeland security.

None of that means Beardsworth had improper intentions. I assume he didn't. However, it's been *Brennan's* genius for years to get himself in the middle of government activities that seem to have the most burning

necessity for national security, producing opportunities for information-wielding and profit that, shall we say, he may or may not be exploiting.

The point in this case is how quickly Borgerson's big-data story rubs up against Brennan, and in a timeframe highly relevant to everything else we've uncovered so far about Brennan's role in Spygate and Russiagate.

Note this: the interagency group in 2009 was looking at a plan to consolidate the NSC and HSC in such a way that the HSC staff would work under Brennan at the NSC. Whatever sentiment about that might have leaped to the fore in 2009, there can be little doubt how most of us would feel about it in 2020.

Our Privacy Policy has been updated to support the latest regulations.

[Click to learn more.](#)

John Brennan in an interview with Graham Allison at the John F Kennedy School of Government, Harvard, in 2016. Harvard U. video, YouTube

There's more. When Borgerson applied to him for funding advice, Beardsworth commended Borgerson to an acquaintance, Doug Doan, a West Point graduate who had a venture capital firm called Hivers and Strivers, specializing in start-up investment in former military entrepreneurs. Doan had been a fixture around Washington for some time, and had his own experience with homeland security from the DHS start-up under Bush (see the Institutional Investor article linked above).

Randy Beardsworth's DHS background was in policy and management on the government side. Doan's was in contracting for homeland security technology and data requirements. He and his wife – Lurita Doan, who **became Bush's General Services Administration (GSA) chief** in 2006 – ran a company called New Technology Management, Inc. (NMTI), which among other things was at the forefront of **automating Customs and Border Protection operations** after 9/11.

NMTI's venture with what became CBP started before 9/11. But 9/11 kickstarted its urgency and changed its focus: "The company completed a proof of concept at seven crossings in Arizona and was set to begin a five-year rollout across the country when the terrorists' strike occurred," according to the 2002 report by Washington Technology. "Now the

multimillion-dollar project has gone from a five-year rollout to two years, and **the emphasis is on catching terrorists instead of drug runners**, Doan said [emphasis added – J.E.J.]”

That emphasis, in other words, was about having an automated database with information on *people* in it, focused on the data needed for catching “terrorists instead of drug runners.” This too fit the criteria of John Brennan’s special area of interest, as manifested in his management of TAC after he left the newly created NCTC in 2005. As we’ve reviewed in earlier reporting, TAC had **obtained long-term analytical and database maintenance contracts** with NCTC and the FBI, for exactly this kind of data, by the end of 2009.

Courtesy of both NSA and law enforcement, the database and the systems that used it saw private information on millions of Americans flow through them – and by 2012, Brennan had **arranged to loosen the valve** for

Our Privacy Policy has been updated to support the latest regulations.
Click to learn more.

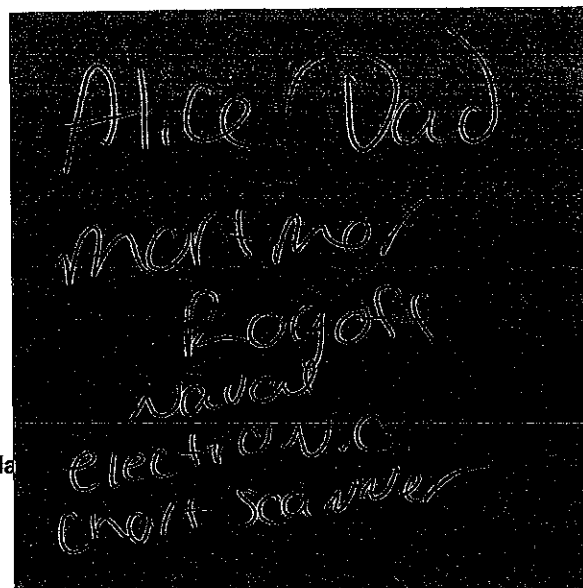
hindsight, quite directly analogous to the possibilities of CargoMetrics being the “NSA of global trade.” Mining databases for siftable data that reveals more than it’s formally intended to is right up Brennan’s alley. There’s no smoking gun indicating he knew what Borgerson was up to. But if Brennan and Beardsworth were working on a homeland security organization project at the same time Beardsworth was talking with Borgerson about a start-up so obviously relevant to homeland security interests, it would be atypical for Brennan not to hear of it.

Meanwhile, Doug Doan hooked Borgerson up with the financing to get CargoMetrics off the ground in 2010. I assume Doan’s role was an innocent one, like Beardsworth’s. Borgerson’s intent was to make his gigantic data store serve, for ship movement and cargo information, the same role as the NSA database for the counterterrorism mission of the FBI, NCTC, and DHS. It was to be the basis of trend and relational analysis; Borgerson’s advertising patter emphasized the commercial utility of it.

But again, it seems extremely unlikely that when Borgerson shopped his proposal to homeland security veterans in 2009, no one saw the possibilities of his big-data idea for keeping tabs on what industries *and* individual companies and shippers were doing. Why should such information be stovepiped at Treasury or Commerce, after all, or in U.S. intelligence channels where the population of data was limited to formal national security priorities?

C. Borg
Part

Our Privacy Policy has been updated to support the law.
Click to learn more.



Don't even think about it. Guard gate at the National Counterterrorism Center (NCTC) in McLean, VA.
Google Street View

These were the same questions that set the framework for Brennan's policy changes on "counterterrorism" information at the FBI and NCTC in 2012. The beauty of CargoMetrics and its data is that, although they effectively capture millions of private business transactions in their net, the information itself isn't privacy-protected. As a thought experiment, it's no stretch to conclude that Brennan, if no one else, would see the tremendous opportunities in harvesting such data.

As for the general timing of CargoMetrics' debut, the trend of technology naturally factored into a start-up in 2010. The idea of mining Big Data for relational analysis and trend-based decision-making was reaching maturity.

Here

But it's still interesting that CargoMetrics was launched within months of Goldman Sachs's initial involvement in moving uranium around, and the explosive shipping incidents of *Arctic Sea* and *Francop*, all in 2009. The interest of homeland security specialists with a link to John Brennan, in the same period, can't fail to be an arresting detail, especially since it involved financing the venture.

Another Clinton angle (this one with Obama-era links too)

- We need not, of course, belabor the connection of Maxwell and Epstein to the Clintons. Everyone knows it's there. But that, also, is food for thought. Journalists tracking down the link between Maxwell and Borgerson date it to about 2013, which would be several years after Borgerson launched CargoMetrics.

Link of Corey & Maxwell

- The "professional" hook for their relationship is routinely reported as a shared interest in the Arctic and its environment, which among other things led to both of them participating in 2014 in the summit conference of a group called Arctic Circle, an NGO started by the president of Iceland the previous year (2013) with Borgerson's participation.

← Alice & A.C.C.?

← and Alice?

? — Corey Borgerson? How got involved w/ Arctic Circle

Privacy - Terms

Ghislaine Maxwell launched her TerraMar Project, a maritime environmental initiative, at the same time, and as numerous Internet sleuths have noted, she **partnered with the Clinton Global Initiative** to get “sustainable development goals” adopted by international institutions. The partnership was to the **tune of \$1.25 million**.

But there are a couple of features of that Borgerson-Maxwell-Arctic story that merit particular mention. One is that a key instigator of the Arctic Circle group is a lady named **Alice Rogoff**, who at the time was the wife of the CEO of the **politically super-connected Carlyle Group**, an elite private equity firm. (Its operations are on a par with the Blackstone Group.)

Ms. Rogoff and her husband, David Rubenstein, who **founded the Carlyle group** in 1987, divorced three years ago. But the Carlyle Group has a revolving door with the highest echelon of the Washington, D.C.

✕

Our Privacy Policy has been updated to support the latest regulations.

[Click to learn more.](#)

time. (Cogentrix, which Goldman Sachs had begun acquiring controlling interest in back in 2003, was a factor in the firm’s deliberations about getting into hands-on uranium dealing in the 2008-09 period.)

It must be no surprise then that the **Clintons** (see [here](#) as well) and **Barack Obama** have made tidy sums from giving speeches at Carlyle-sponsored events. (George W. Bush, who sat on Carlyle’s board before becoming president, had a somewhat **unfortunate history** with the firm that seems to have made speaking engagements less likely.)

Alice Rogoff (R) speaks with Alaska Sen. Lisa Murkowski at the Arctic Circle conference in 2018. Arctic Circle video

But the interesting feature that is Alice Rogoff, per se, goes beyond that. In 2012, Scott Borgerson appeared at an event he later described as pivotal for him: a conference held in Alaska under the banner of an

initiative called Arctic Imperative (a precursor to the Arctic Circle initiative). It was the second in a two-year series of the gatherings, and Rogoff was the driving force behind it.

Notably – to flesh out her profile – Rogoff bought the flagship newspaper in Anchorage a couple of years later, the *Daily News*. This gave her a high profile in the state, and in fact, she acquired a home there, at which she hosted President Obama during a visit he made to Alaska in 2015. She also hosted Ghislaine Maxwell in 2014, when Maxwell went along for the ride with an Iditarod team.

And that's not just a shallow sample of the company Borgerson has been running in. It appears to mean a bit more than that. In his 2016 interview with Institutional Investor, Borgerson credited a meeting with an unnamed CIO of "a large investment firm," which he declined to identify, at the 2012 Arctic Imperative conference in Alaska, with kickstarting an

X

Our Privacy Policy has been updated to support the latest regulations.

[Click to learn more.](#)

Imperative conferences.)

That data-to-trading experiment was a real-world proof of concept for the quant fund Borgerson had begun to envision in the first couple of years after taking CargoMetrics live as the "NSA of global trade." As the Institutional Investor story observes, that was a major shift in emphasis for the company. (For one thing, it meant buying out the original venture capital investors, who had bought in on the starting premise of focusing on the data product.)

After the "large investment firm" came on board, says Institutional Investor, "Live trading using CargoMetrics' models began in December 2012." Over the next year and a half, CargoMetrics geared up to begin operating a fund, something that required support from outside investors. Blackstone became one of them; meanwhile, another investor which had already taken interest in Borgerson's quant-fund plan for CargoMetrics was Callaway Capital Management, a Washington, D.C.-based investment firm started by Daniel Freifeld.

✕

Our Privacy Policy has been updated to support the latest regulations.

[Click to learn more.](#)

Then-Sec. of State Hillary Clinton speaks at U.S-EU Energy summit in 2010. Dept. of State video, YouTube

Freifeld had been a senior adviser on Eurasian energy issues to Secretary of State Hillary Clinton, after being an adviser to the Hillary campaign in 2007-08. The picture of Borgerson as a semi-anonymous maverick data-monger starts to fade a bit as these various facts emerge.* Borgerson may not have known the Clintons or Obama's top administration officials, but the people who ran in their orbit knew Borgerson.

Borgerson was developing his quant-fund plan with the help of such connected people between 2011 and 2013. And *that's* when he and Ghislaine Maxwell ran into each other through their shared interest in the Arctic. We need not emphasize, but merely note, that the collision occurred when Borgerson's company entered the field of serious fund management.

That's the second interesting feature of the Borgerson-Maxwell nexus: the timing of the quant-fund breakout versus the connection with Maxwell. Of equal note is that CargoMetrics' **quant-fund backers** include not only the Blackstone Group but Paul Tudor Jones, Howard Morgan of Renaissance Technologies, shipping-industry giants Idan Ofer, Clarksons PLC, and Maersk Tankers – and Hillary pal **Eric Schmidt of Google**. We should all have such backing for our experimental quant-fund start-ups.

How Ben "Echo Chamber" Rhodes ended up in the Uranium Jerky series

Speaking of shipping: one of the most peculiar features of the revelations about the Deep State in the last several years is one we **looked at in 2018**. The precipitating incident involved a private security firm approaching the wives of Ben Rhodes and Colin Kahl – yes, that Rhodes and Kahl – apparently hoping to gain information that would shed light on a client's complaint about fictitious accounts being set up in his name by the banking giant Royal Bank of Scotland (RBS).

The client was a Taiwanese shipping company owner named Nobu Su. The private security firm was the Israeli company Black Cube, for defaming which there was a minor cottage industry in the mainstream media in 2017 and 2018. The gist of the story was that Su had hired Black Cube to get

background information for him on RBS's alleged use of his identity to launder money through fake bank accounts. (RBS was found by investigations in the U.S. and UK to have laundered money in the same period as HSBC and other banks. The question in Nobu Su's case was about his own identity being implicated.)

X

Our Privacy Policy has been updated to support the latest regulations.

[Click to learn more.](#)

It seems like such a nice place. Royal Bank of Scotland lobby in St. Andrew Square, Edinburgh. RBS video, YouTube

The timeframe of the alleged money-laundering was 2007 to 2009. The investigation by Black Cube wasn't until 2017, however. Reporting in 2018 alleged that Black Cube was actually contracted for the job by "aides to Donald Trump," but Israeli media confirmed the approaches to Rhodes's and Kahl's wives were made under the contract with Su.

Two features of this tale are of special interest. One is that it involved money-laundering in relation to sanctions-busting (e.g., sanctions against Iran), arms trafficking, and narcotics. Such money-laundering was a big problem with some of the world's largest banks, including HSBC, RBS, and BNP Paribas of France.

Notably, the client, Mr. Su, was said to be the party who started the Black Cube probe with "Iranian nuclear" interests. An article at *Haaretz* asserted that "A source close to the company said the purpose of its data collection was to serve the client's business or legal interests, and had nothing to do with Trump. The source also said **correspondence regarding Iranian nuclear issues related to the business interests of the client** who hired the spy firm [i.e., Su hiring Black Cube; emphasis added]."

And as the placement of this incident in our narrative suggests, it's significant, with this especially interesting feature, that Su's business is shipping.

Su reportedly believed that "the 2008 financial crisis, and the financial predicament Su consequently found himself in, made him a convenient target for blackmail." But his shipping business and reported company interest in "Iranian nuclear issues" were likely to be the tiebreakers for any decision by RBS to launder money through accounts in his name.

That supposition would be strengthened by the other special feature of the tale. Black Cube zeroed in on Rhodes and Kahl in 2017, some eight to ten years after the alleged money-laundering. Rhodes's and Kahl's involvement in Iran policy in the Obama administration dated to the time the JCPOA was being negotiated. The agreement was negotiated starting in 2013 and announced in July 2015, so what they had knowledge of from that perspective would have been after the fact for Su's timeline.

As regards Su's timeline: **Rhodes**, for his part, had become a speechwriter for Obama in 2007, and before that had been an assistant to former Representative Lee Hamilton (D-IN), helping to draft the Iraq Study Group Report which surveyed, among other things, the post-war findings on WMD in Saddam's Iraq.

Kahl was Deputy Assistant Secretary of Defense for the Middle East from 2009 to 2011: prior to that he was a fellow at the Center for a New

x

Our Privacy Policy has been updated to support the latest regulations.
[Click to learn more.](#)

overtures in May 2017, one possibility is that RBS activity from 2007 to 2009, which Nobu Su knew about because it affected him personally, had continued through the period of Rhodes's and Kahl's time on the JCPOA team. What RBS might thus have been laundering money for circa 2015, and in whose name, would make very interesting reading.

Ben Rhodes in a 2018 interview, CBS News video

This information isn't of interest because it's a smoking gun. It's of interest because it illuminates a dark corner of sanctions-busting, shipping, the sanctions on Iran, and which personalities potentially had knowledge of what. In the intelligence profession, you don't ignore such clues; you pursue them.

The collateral relevance of other factors we have looked at in the Uranium Jerky series should be obvious. If U.S. intel and law enforcement haven't at least investigated the alleged fake accounts set up by RBS, and

followed all the related threads to see where they go, that needs to be done.

The new wind across the Great Lakes

In the case of the next, final coincidental circumstance, there's a connection few readers (other than ours) may know about. That connection is to Obama – and it became most evident at the very end of his administration, and in his first months out of office in 2017.

This link maps to the St. Lawrence Seaway and the Great Lakes again. The circumstance is the 2009 **purchase of Manitowoc Marine** of Wisconsin, maker of the Navy's Littoral Combat Ship, by the Italian shipbuilding giant Fincantieri. Regular readers will remember uncovering this in **the investigation of the Italian connection to Obamagate**, involving Link Camous University in Rome and Joseph Mifsud. the

✕

Our Privacy Policy has been updated to support the latest regulations.

[Click to learn more.](#)

President Trump visits Fincantieri Marinette Marine (formerly Manitowoc Marine) in Jun 2020. White House video

In the course of running the details down, we encountered former President Obama visiting Milan for a conference in May of 2017, and having a special visit with Italian luminaries including the chairman of Fincantieri, Giampaolo Massolo, at the Italian Institute for International Political Studies, of which Massolo is the president. During the same trip, Obama also met **with previous Prime Minister Matteo Renzi** (whose government had been replaced shortly beforehand).

Obama's Milan visit was remarkably timed, as coincidences go: his meetings with senior Italian officials were on 9 May 2017, the day James Comey was fired by President Trump.

It was also at exactly the same time that an Italian government investigative team was accompanying the FBI on visits to two U.S.-located servers used for business by an Italian entrepreneur, who was being probed by Italian law enforcement over allegations of cyber-attacks on government officials. Giulio Occhionero **lodged information with the**

court afterward that in the course of these visits to the U.S., the law enforcement agents apparently tried to plant data on the servers that seemingly pointed to Hillary Clinton's 30,000 "missing" emails.

Digging out these nuggets highlighted some other developments whose importance had become evident only in hindsight. These included, in particular, the prominent presence of a Mifsud crony and senior Italian Social Democrat politician in an Italian **delegation to the Democratic National Convention** in July 2016.

Another was the interesting emphasis in the Obama administration's last months on holding a state dinner for then-PM Matteo Renzi, in October 2016. (Alert readers will recall that NSC staffer Eric Ciaramella, officially working for Vice President Joe Biden, was also prominent in the arrangements for the Renzi visit.)

x

Our Privacy Policy has been updated to support the latest regulations.

Click to learn more.

visit.

Pamela Paparoni
@PamelaPaparoni



Pres.#Obama a Milano in #ISPI con i vertici Istituto.
#Congratulazioni @ispionline #GiampieroMassolo
@francobruni7 #CarloSecchi @paolo_magri

1:45 PM · May 9, 2017



♥ 1 See Pamela Paparoni's other Tweets

(This tweet's image was from the same event, but was posted more than a month later. It shows Obama in discussion with Giampiero Massolo.)

mmachiavelli
@mmachiavelli



#Massolo Il mondo che verra
unilink.it/lectio-magistr...
@PaoloMessa @Michele_Arnese @mrtlgu @michelepierrri
@francescosisci @barbaracarfagna

11:20 AM · Jun 20, 2017 from Firenze, Toscana



♥ 4 👤 See mmachiavelli's other Tweets

For our purposes in this article, however, the coincidence of interest is that Fincantieri completed its purchase of *Meritux* in January 2000.

Our Privacy Policy has been updated to support the latest regulations.
[Click to learn more.](#)

✕

It is not uninteresting, for that matter, that Fincantieri was also constructing a **special-purpose vessel** for Russia during the same time period (as well as a class of diesel and battery powered submarine intended by Russia for export). The special-purpose vessel is a platform designed for the transport of nuclear waste, and it was delivered for service in 2016.

An awful darn lot of pathbreaking things happened in the first year or two of the Obama administration. More of them than the public realizes involved uranium and shipping, including patterns in which both factors intersected. It is by no means out of bounds to survey the big picture and recognize that the never-solved conundrum of *Arctic Sea* may have been linked to some of them – and that their meaning went beyond coincidence, and beyond the mere hope of incidental profits for the political officials (like the Clintons) with a stake in them.

As argued in the introduction to Part II of this series, after the survey in Part I of Goldman Sachs's unique and little-known initiative with buying and selling physical uranium, we must at least consider that the events may not have been as much about the profits as they were about the uranium.

* I know of nothing against Borgerson as regards his CargoMetrics idea or company. The point of painting the larger picture of his connections is not to impugn him, but to illustrate that he's been more conventionally plugged in to the establishment networks than is conveyed by most coverage of him, and that he was on the establishment's radar. With stints at the Fletcher School and the Council on Foreign Relations, as well as time plying the NGO circuit for his Arctic interests, he is hardly an outsider. What's of interest is the service his idea offers to actors with a "secret intelligence" level interest in, basically, knowing everyone's business. That takes on a special shading when the business involves moving things around like uranium, dual-use technology, controlled commodities, and components for nuclear energy and weapons.

🔗 Share 🐦 Tweet 🔄 Flip ⚙️

Posted in: Business, Email Featured, Foreign Affairs, National Security, Politics
 Tagged: Alice Rogoff, CargoMetrics, Clinton Foundation, Fincantieri, Ghislaine Maxwell, Hillary Clinton, John Brennan, Obama Administration, Scott Borgerson, shipping, transportation, uranium

Privacy · Terms

J.E. Dyer

J.E. Dyer is a retired Naval Intelligence officer who lives in Southern California, blogging as The Optimistic Conservative for domestic tranquility and world peace. Her articles have appeared at Hot Air, Commentary's Contentions, Patheos, The Daily Caller, The Jewish

Our Privacy Policy has been updated to support the latest regulations.
Click to learn more.



Comments

For your convenience, you may leave comments below using Disqus. If Disqus is not appearing for you, please disable Adblock to leave a comment.

1 Comment [libertyunyielding.com](#) Privacy Policy Login

Recommend Tweet Share Sort by Best

Join the discussion...

LOG IN WITH OR SIGN UP WITH DISQUS ?

Name


OldArmyBrat59 • 2 months ago

The upshot... The International world of the Globalists is set up to monetarily reward the Globalists. AND the Globalists are the Deep State. This entire saga smells of something that has always smelled of rotted shrimp and that's the weird and brutally corrupt international shipping business. What's ironic is that this business of essentially nationless and stateless monetary players operate shipping lines, ship ownership, cargo tariffs, bills of lading, and port authority has also become the backbone of the derivative financial markets and hedge funds convert money and goods for percentage shares as overhead. The entire Byzantine construction then offers the opportunity for the shipment of nearly anything, for a price, anywhere and the shadow interlocking and "transnational" interests are obscured. Merchant Marine operations have always been dicey and weird... even in the age of wooden ships and sail. But global trade and world wide networks have made that function even more difficult for the average person to understand. The one thing that is easy to gather in is the huge potential profitability of such complex exchanges, and with that the inherent and often endemic corruption that goes with it. It boggles the mind. It also screams for major international reforms. And that

Sponsored Content

Michigan AG says her son was 'devastated' ... Internet Providers Don't Want You Buy!... One Thing All Cheaters Have In Common,...
zen-insider.com www.peoplewhiz.com

Our Privacy Policy has been updated to support the latest regulations.
Click to learn more.

 NO PULL Harness

If You Are A Dog Owner This No Pull [Shop Now](#) Dog Owners Watch Out. [Shop Now](#) Why This Harness Will Make [Shop Now](#)

[Pics] Young Wives of Wealthy Older Men Cartoon of the Day: Privilege alert Cartoon of the Day: In a handbasket
Mentertained

Seattle Top Attorneys 2020
America's Top Attorneys

**[Photos] 21 Famous People Who
Went Missing And Were Never...**
Chocolate.com

**[Photos] 29 Times People Should
Have Really Checked the...**
History Chronicle

**Our Privacy Policy has been updated to support the latest regulations.
Click to learn more.**

X

STYLING: TONY

**Pennsylvania bakery offering Trump, Biden cookies says one
is way outselling the other**

NEXT POST >

Which side will riot if it doesn't get its way?

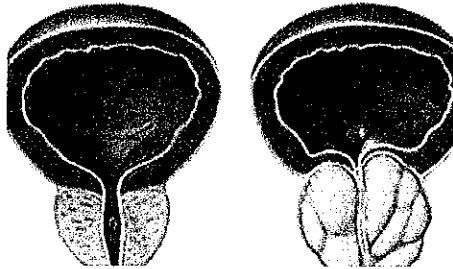


**Our Privacy Policy has been updated to support the latest regulations.
Click to learn more.**

Sponsored Stories



**[Photos] This Bride's Wedding Dress
Surprised Even the Groom**
History Chronicle

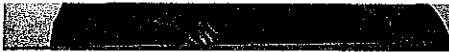


Do this Immediately If You Have Enlarged Prostatic (Watch)
healthtrend.live



Our Privacy Policy has been updated to support the latest regulations.
Click to learn more.

×



One Thing All Cheaters Have In Common, Brace Yourself
www.peoplewhiz.com



The Israeli-made Face Mask Everyone Is Talking About In the US
The Jerusalem Post

Recommended by



**Political News
Megasite**

Tap Here

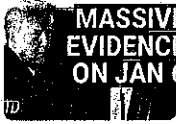
**Today's Featured Videos from
Whatfinger:**



Several witnesses in Georgia say Democrats altered military ballots to cheat in 2020 election...



Declassified: What Is Pence's Game Plan for January 6th? with Gina Shakespeare of Epoch Times...



Trump: 'Massive amounts of evidence' to be presented; Trump veto overridden; Senate runoff concern...

X

Our Privacy Policy has been updated to support the latest regulations.

Click to learn more.

Orlando yoga vaccine administrators inoculated menus before qualified citizens

Joe Kinsey, Outkick:

Chicago teacher's union leader: We should strike if forced to return to the classroom

Mike DeBonis, WaPo:

Pelosi's likely final term as speaker is set to begin with a scramble for votes

Nikki Schwab, Daily Mail:

It'll cost ya: Donald Trump's D.C. hotel charging \$2K for rooms during inauguration

AFP:

Crowds thronged Wuhan, where pandemic began, to celebrate New Year

Chris Melore, StudyFinds:

Drug reverses age-related cognitive decline in a matter of days by erasing 'blockages'

Colleen Shalby et al., LAT:

40% of hospital workers in California refuse to take COVID-19 vaccine

Daniel Greenfield, FrontPage:

Authorities coddle ecoterrorists who cut off gas to thousands of freezing Coloradans

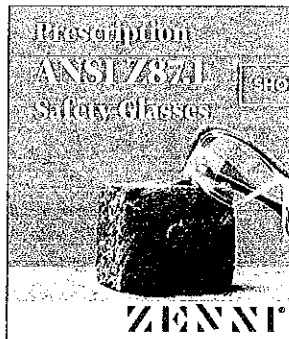
Leah Barkoukis, TH:

Proposed House rules for next Congress do away with 'gendered' family terms

Ian Gary, FACT Coalition:

Defense authorization act, defying Trump veto, ends anonymous U.S. shell companies

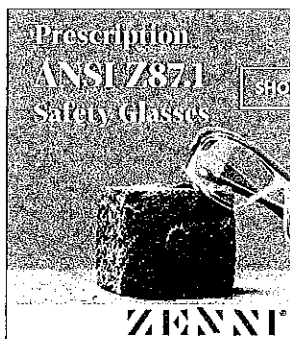
[More LU Web Crawler >](#)



Liberty Unyielding

Our Privacy Policy has been updated to support the latest regulations.
[Click to learn more.](#)

✕



Blog Roll

- [EAGnews](#)
- [Hot Air](#)
- [Instapundit](#)
- [JammieWearingFools](#)
- [Le-gal In-sur-rec-tion](#)
- [Linkiest](#)
- [Newsbusters](#)
- [PJ Media](#)
- [Right Wing News](#)
- [The Lid](#)
- [The Optimistic Conservative](#)
- [The Volokh Conspiracy](#)
- [Weasel Zippers](#)

Our Privacy Policy has been updated to support the latest regulations.
Click to learn more.



EDITOR IN CHIEF
Howard Portnoy

EDITOR AT LARGE
J.E. Dyer

CONTRIBUTING EDITOR
Renee Nai

CONTRIBUTING WRITERS
Myra Adams

Jeff Dunetz

Joe Newby

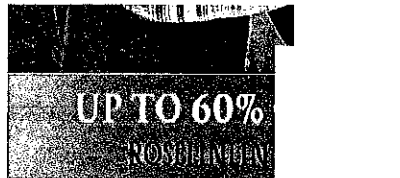
Kenric Ward

SITE DESIGN
Tyler Johnson



**Our Privacy Policy has been updated to support the latest regulations.
Click to learn more.**

x



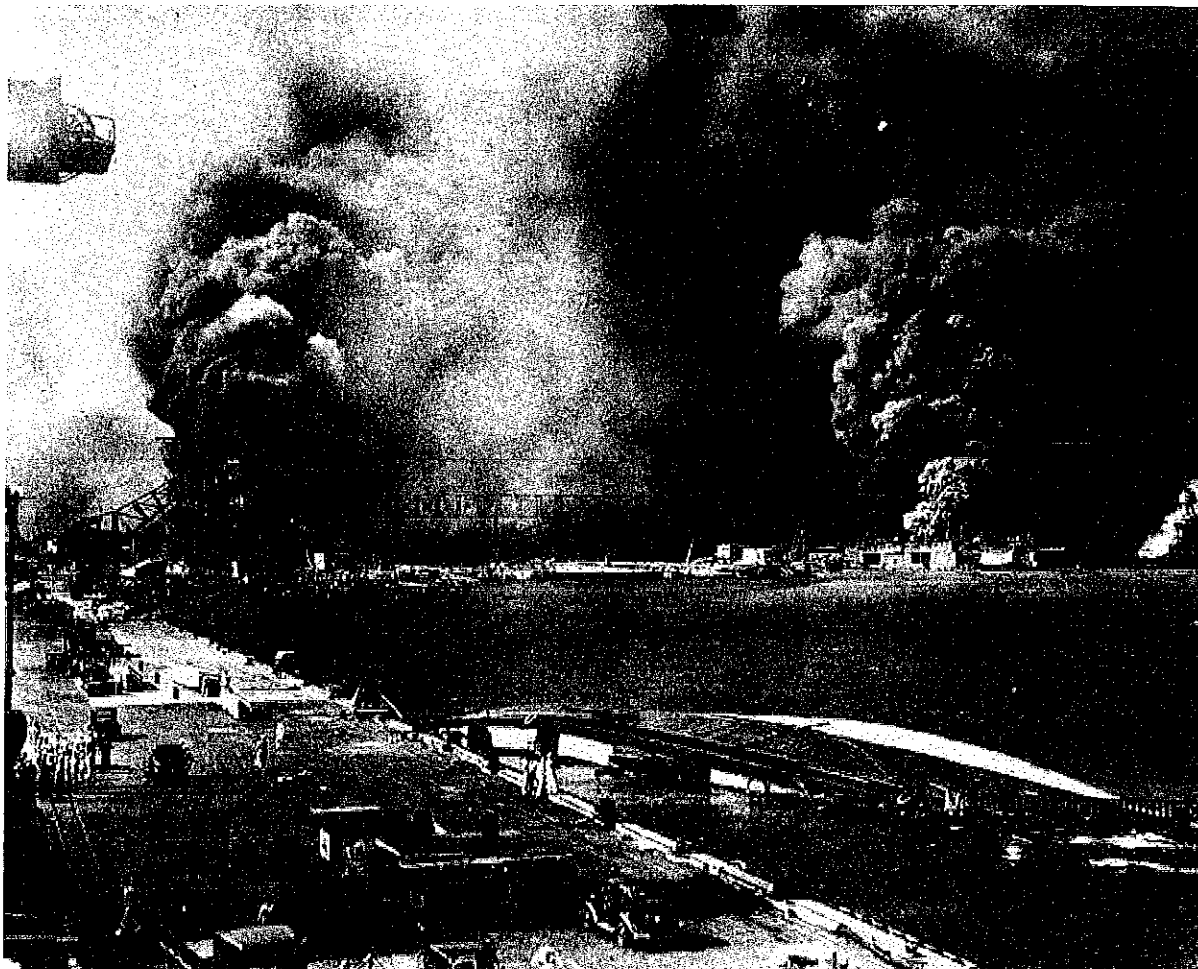
Page 1 of 1

Intel Experts Claim the US Was Hit By a "DIGITAL PEARL HARBOR"

By Joe Hoft

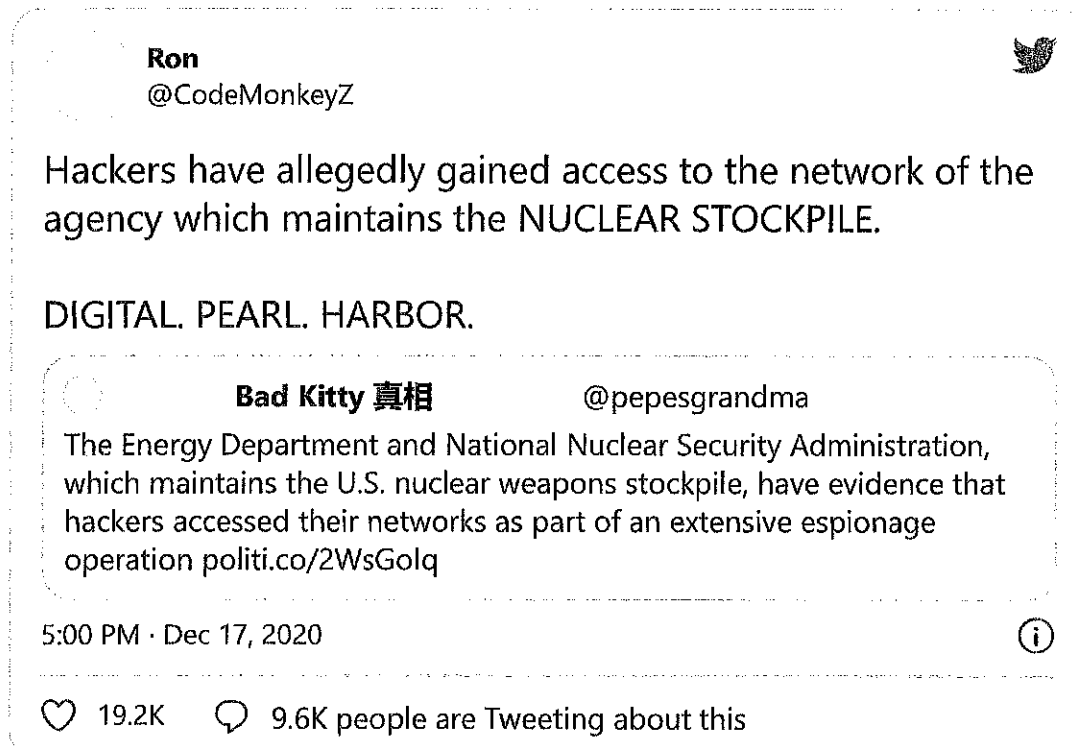
Published December 18, 2020 at 8:25am

860 Comments



On December 7, 1941 Japanese forces **hit the US base at Pearl Harbor** in a surprise attack just before 8 AM in the morning. The Japanese managed to destroy or damage nearly 20 American naval vessels, including eight battleships, and over 300 airplanes. More than 2,400 Americans died in the attack.

Today intel experts are comparing the latest intelligence breach on the US government to a "Digital Pearl Harbor."



There is now a call for Executive Order 13848 – a report is due to the President today:

GP

Ron

@CodeMonkeyZ



SCOTUS is compromised.
SolarWinds is a DIGITAL PEARL HARBOR.

We demand EO13848!

3:24 PM · Dec 17, 2020



♥ 74.1K 💬 26.6K people are Tweeting about this

President Trump has the people behind him and an election win of historic proportions. Democrats and their media claim Biden broke the all-time record by 10 million votes. We all know this did not happen:

Ron @CodeMonkeyZ · Dec 17, 2020



Replying to @CodeMonkeyZ

Election infrastructure was allegedly attacked and he now has his back to the wall.

The courts have failed him.

His own political party has failed him.

Ron

@CodeMonkeyZ

Trump still has immensely popular support within the US populace, and the fierce loyalty of the military.
Trump has EO13848 which allows him to take drastic measures and could potentially be used to restore the Republic.

5:29 AM · Dec 17, 2020



♥ 25.2K 💬 4.7K people are Tweeting about this

We're facing a digital Pearl Harbor!

Ron

@CodeMonkeyZ



The SolarWinds hack, Digital Pearl Harbor, will be remembered as one of the most sophisticated and large

remembered as one of the most sophisticated and large scale attacks on American infrastructure.

Lou Dobbs  @LouDobbs

Prelude to War: @MorganWright_US lays out how a foreign power infiltrated our federal agencies to carry out a cyberattack #MAGA #AmericaFirst #Dobbs

8:03 PM · Dec 17, 2020

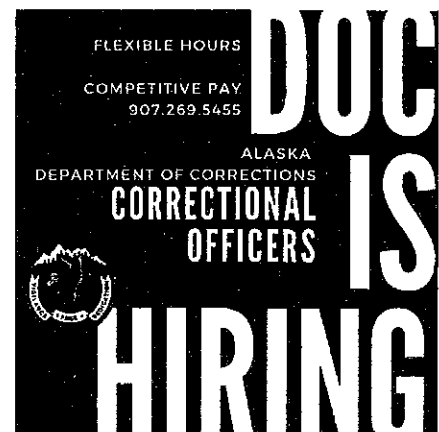


❤️ 14.6K 💬 7K people are Tweeting about this

America is under attack.

[HOME](#)[THE NEWSLETTER](#)[STATE POLITICS](#)[THE FEDS](#)[OPINIONS](#)[COMICS](#)[ARCHIVES](#)[CONTACT/ADVERTISE](#)[HOT TOPICS](#)[SEPTEMBER 1, 2021 | AFTER SHORT QUARANTINE, MURKOWSKI DOES NOT](#)[SEARCH ...](#)[HOME](#)[INDUSTRY](#)[ADVERTISEMENT](#)

Alaska and China sign \$43 billion agreement to develop LNG pipeline, part of Trump's war on the trade deficit

[FOLLOW TMS ON FACEBOOK](#)

Alaska Gov. Bill Walker and AGDC head Keith Meyer sign a joint development agreement with China's state-owned energy company, banking and investment agencies to develop Alaska's natural gas prospects. (Screenshot of New China TV's coverage of the event.)

POSTED BY: MATT BUXTON NOVEMBER 8, 2017

It's a fair bit more than a non-binding MOU, but just how much more is unclear.

Alaska Gov. Bill Walker and his team will be bringing home an agreement with Chinese investors and energy companies to develop Alaska's natural gas stores on the North Slope worth \$43 billion. Walker and his gasline team have been traveling to Asia with President Donald Trump this past week.

The joint development agreement was signed in Beijing by Walker, Alaska Gasline Development Corporation head Keith Meyer and representatives from China's state-owned energy company, Sinopec, and two of China's financial investment firms. The financial investors are the Bank of China and the China Investment Corporation, which is China's \$813 billion version of the Alaska Permanent Fund Corporation.

"This agreement has all five necessary signatories—the buyer, the lender, the investor, the developer and the state," Walker said in a prepared statement. "There are more steps before a final investment decision is reached, but having the largest LNG buyer in the world participating in this project means the Alaska LNG project has favorable market engagement at the highest level."

The terms of the financing weren't immediately available, but **the announcement from AGDC** describes it as follows: "Under the agreement, the parties have agreed to work cooperatively on LNG marketing, financing, investment model and China content in Alaska LNG, and get a periodic result by 2018."

The language would suggest the group is taking a similar approach that Alaska and the major North Slope energy producers made on the Alaska Liquefied Natural Gas Project to take a "gated" approach that allows investors to cut and run at certain points in the project's development, albeit all on a much faster timeline.

The existing AKLNG plan calls for an 800-mile pipeline connecting the North Slope and an export terminal in Nikiski along with the proper treatment facilities along the route. **A update from February indicates the cost**



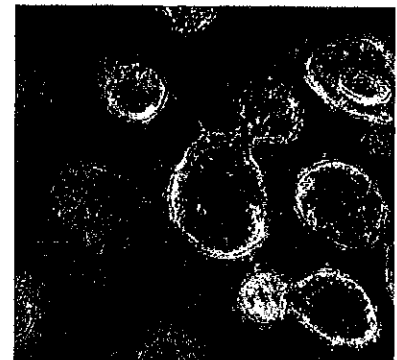
The Midnight Sun
4,250 likes

Like Page



The Midnight Sun
3 hours ago

With surging cases, Gov. Dunk efforts on expanding health care balking at measures that would curb covid-19.



MIDNIGHTSUNAK.COM

Alaska's hospital capacity

Ask not what Alaska's hospitals

3 Comment 4

RECENT POSTS

Alaska's hospital capacity matters, but fewer covid-19 cases would be even better
GARA: I'm Running to Create A Brighter Future
Friday in the Sun (Sept. 3): The World is on Fire edition
Dunleavy asks Legislature for do-over on public health nursing veto as covid surges

estimate of the project is between \$37 billion and \$45 billion, well within the reach of the proposed financing deal.

The road to tonight

Speculation swirled throughout the afternoon after Walker sent legislators a notice he'd be holding a 15-minute briefing on a secure phone line from Beijing to give an update on an unspecified issue. Because Walker attended the trip with the plan to pitch the gas project to Asia buyers (the Asia market has long been thought to be the target market for Alaska's natural gas) speculation immediately went in that direction.

Confusion was sown by an afternoon announcement of trade agreements by the White House that included a non-binding agreement (a memorandum of understanding) between the Alaska Gasline Development Corporation signed with a Korean gas utility. Another non-binding MOU in a long list of non-binding MOUs did little to excite people long following Alaska's fruitless efforts to build a gas line to accompany the trans-Alaska pipeline system, but late in the afternoon it became clear that the MOU was from earlier in the year and the likely announcement had to do with something else.

This time it's a JDA

The **first report emerged by Reuters** early in the evening, giving Alaskans enough time to tune into a **live video feed of a signing ceremony attended by Trump and China President Xi Jinping**. Trump and Xi watched from the stage as the \$43 million joint development agreement was signed alongside procurement agreements for \$1.4 billion in aircraft engine frameworks and \$4 billion chipsets.

In his remarks Trump didn't discuss the Alaska natural gas project directly, but he spoke broadly about fixing the trade deficit between the two countries.

After short quarantine,
Murkowski does not have
covid-19

TAGS

2018 Elections 2018

governors race **2019**

session 2019 special session

2020 elections 2020

session akleg recaps alaska

democratic party **alaska**

legislature alaska

politics alaska

republican party amy

demboski **bill walker**

casey reynolds cathy giessel

charisse millett congress

coronavirus crime dan

sullivan donald

trump don young ethan

berkowitz forrest dunbar

Friday in the Sun

gabrielle ledoux health care

hillary clinton jason grenn joe miller

john coghill kevin meyer lance

pruitt **Lisa**

Murkowski lora reinbold

mark begich **mike**

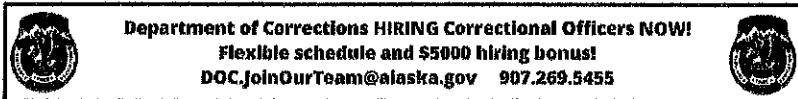
“We will have a more prosperous future if we can achieve a level economic playing field,” he said. “Right now it is a very one-sided and unfair one.”

Then added a thoroughly Trump-style flair to an otherwise milquetoast speech.

“But, but, I don’t blame China,” he said, to laughs. “After all who can blame a country for being able to take advantage of another country for the benefit of its citizens? I give China credit.”

We’ll bring you more developments as they become available.

Follow @mattbuxton



MORE FROM TMS

GARA: I'm Running to Create A Brighter Future

Friday in the Sun (Sept. 3): The World is on Fire edition

Dunleavy asks Legislature for do-over on public health nursing veto as covid surges

After short quarantine, Murkowski does not have covid-19

\$1,100 PFD emerges after bitter fight in the House

dunleavy obamacare

pete kelly **the budget**

the dividend tuckerman

babcock university of alaska vetoes

vince beltrami

SHARE

TWEET

PIN

SHARE

MAT-SU

Mat-Su Borough Attending China Trade Trip

Mat-Su | Patty Sullivan | Monday, April 23, 2018

Representatives from the Matanuska-Susitna Borough will be attending the China trade trip in May with Alaska Gov. Bill Walker and some 20+ other entities.

Mat-Su Borough Manager John Moosey said they are attending to explore and develop trade opportunities with China for the Borough.

Photo caption: In 2010 a test shipment of coal was exported from Port MacKenzie to Japan.

The following is a press release from the Alaska Gov.'s office.

ALASKA BUSINESSES SELECTED FOR OPPORTUNITY ALASKA: CHINA TRADE MISSION

April 18, 2018

No. 18-045

JUNEAU – Governor Bill Walker today announced the delegation for *Opportunity Alaska: China Trade Mission*, which will include fisheries, tourism, and investment businesses, as well as a baby food maker, an architecture firm, and a university.

The group, which departs in May, will represent some of the best Alaska has to offer, and highlights the wide scope of our shared interests with our largest trade partner. From fresh crab air-lifted to Shanghai, to international shipping routes, to Beijing tourists traveling to see the northern lights in Fairbanks, Alaska's economic powerhouses have ties that span the Pacific. The delegation will travel with a mission to empower Alaska businesses at home and abroad by reinforcing Alaska's reputation for unique products and incredible experiences in the world's largest consumer market.

Opportunity Alaska: China Trade Mission Delegation

A2A Railway Development
Corporation
Alaska Pacific University

Alaska Skylar Travel	Golden Harvest Alaska Seafood
Alyeska Resort & Hotel	Icicle Seafoods
Alyeska	Kachemak Bay Seafoods
Anchorage Economic Development Corporation	Matson
	Mat-Su Borough
Bambino's Baby Food	Mat-Su Economic Development Corporation
Bering Straits Native Corporation	Nana Regional Corporation
Borealis Basecamp	PT Capital, LLC
Chena Hot Springs Resort and Holdings	RIM Architects & Design, LLC
Copper River Seafoods	Sealaska Corporation
Denali Visions 3000 (49th State Brewing Co.)	Trident Seafoods
	Trilogy Metals US Inc.
Explore Fairbanks	Visit Anchorage
Fairbanks Economic	

Development Corporation

The delegation, including Governor Bill Walker, will travel to China May 19 through May 30, 2018, to meet economic partners, engage with key decision makers, expand Alaska markets, and meet potential customers, industry, and government officials.

###

—End—

MAT-SU BOROUGH

China Trip, Rec. Bond Projects & More

Mat-Su | Patty Sullivan | Friday, August 10, 2018

Hear insights on the China Trade Trip. Learn of the progress on the recreation bond projects, and more as Matanuska-Susitna Borough Manager John Moosey, Mayor Vern Halter, and Assembly Member Randall Kowalke present to the Greater Palmer Chamber of Commerce.

Listen to the audio of the event and look through the pdf of the Powerpoint presentation, both are posted here.

This is the fourth similar presentation this summer. Others included:

- The World Trade Center, Anchorage
- The Greater Wasilla Chamber of Commerce
- The Valley Board of Realtors

For more information contact Patty Sullivan, Public Affairs Director, patty.sullivan@matsugov.us (mailto:patty.sullivan@matsugov.us)



—End—

Documents


PDF of Presentation  </component/cck/?task=download&>


Audio


Audio of Mayor Halter, Manager Moosey, Assembly Member Kowalke

 0:00 / 3:52 

Photos

</images/content/19414/Moosey.jpg>






</images/content/19414/KowalkeChamber.jpg>

</images/content/19414/PalmerChamber.jpg>



CONTACT US
[Contacts \(/contacts\)](/contacts/)

JOIN US
Job Opportunities
<https://www.governmentjobs.com/careers/matsugov>
Volunteer Opportunities
<https://www.governmentjobs.com/careers/matsugov/transfer/jobs>
Serve on a Borough Board
[\(/boards\)](/boards/)
Employee Mail & Services
[\(/join-us/employeeservices\)](/join-us/employeeservices/)

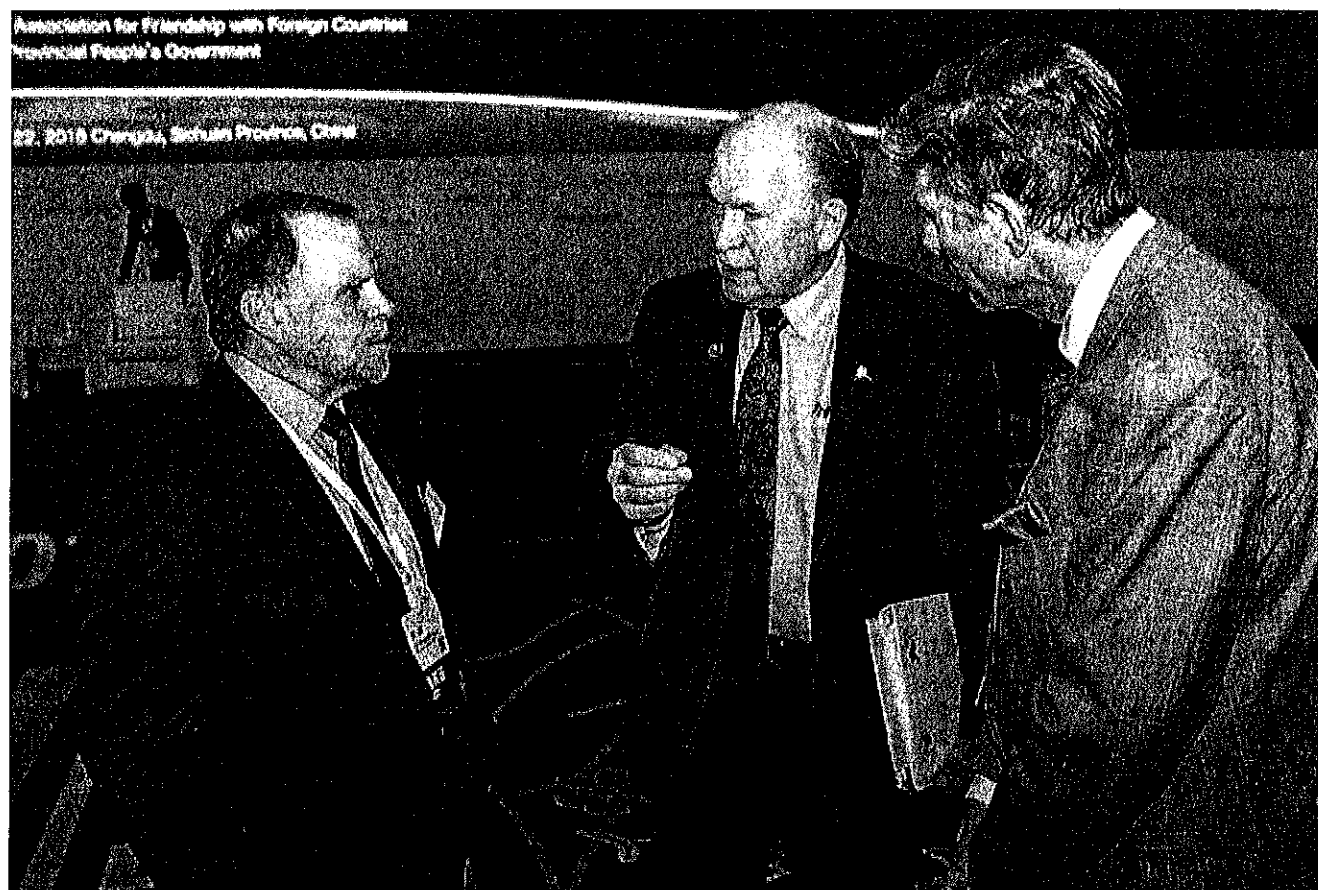
FOLLOW US
    

https://www.frontiersman.com/our-eagle/news/mat-su-borough-officials-meet-with-chinese-economic-advisors/article_89076a1c-6f58-11e8-abf1-7febc11edaff.html

Mat-Su Borough officials meet with Chinese economic advisors

by TIM BRADNER

Jun 13, 2018



Mat-Su Borough officials met up with Governor Bill Walker during a recent trip to China

Talk about timing: Just as a U.S. China trade war looms, Gov. Bill Walker landed in Beijing May 21 accompanied by Alaskans with stuff to sell.

The Chinese quickly grabbed the opportunity to make at least a small dent in a huge U.S. trade imbalance between the Asian giant.

By a stroke of luck, Walker's first meeting on arriving in Beijing was with China's Vice Premier Liu He, who had just returned from trade meetings in Washington, D.C.

Liu has become China President Xi Jinping's chief economic advisor and negotiator in the trade talks, and is in a key position to move Alaska-China trade relations along, particularly the potential exports of Alaska liquefied natural gas.

Meanwhile, David McCarthy and Jason Motyka of 49th State Brewing Co., two Alaskans on the trip, want to make sure the Chinese are drinking some good Alaska-made beer while rebalancing the trade deficit.

McCarthy and Motyka are working on a plan to ship their beer by air to serve a fast-growing craft-beer culture in China. "The seven and a half-hour flight is just long enough to keep our product fresh and chilled," Motyka said at a June 6 press conference convened by Walker with Alaska and who went on the trip.

"The 'Alaska' brand means a lot in China. It's seen as a mysterious place," Motyka said.

49th State has just built a new beer-making plant in Anchorage that has excess capacity, and the ability to export barrels of brew will allow the company to use the capacity, Motyka said, although the plant is mainly intended to serve the Alaska market.

China has a large, well-established domestic beers but as the country prospers and its demographics change, younger consumers want to try something new.

Alaska's new organic baby-food startup, Bambinos Baby Food, also struck a strong chord, said Zoi Maroudas, Bambino's CEO, who was along on the trip. "This is an opportunity to introduce pure, natural products, and help nourish healthy babies in China," Maroudas said.

Bambinos is ant the micro-size now as an Alaska startup but the governor noted that the Chinese appear anxious to want help small Alaska firms grow to be able to meet their customers' demands. China Investment Corp., the nation's huge sovereign wealth fund, has already met with Maroudas on ways of helping Bambinos develop.

Chinese consumers are sensitive over food quality, particularly baby food, after a series of scandals over contaminated food.

Matanuska-Susitna Borough Assemblyman Randall Kowalke and Borough Manager John Moosey on the trip, too, and appeared at the Thursday press briefing. Moosey said he and Kowalke had two objectives, one being to make sure the potential Chinese partners in the Alaska LNG Project were aware of the borough's Port MacKenzie its ability to efficiently support construction of the giant \$43 billion project.

Secondly, the two wanted to check out the China operations of a New Zealand company that is a potential purchaser of timber from Mat-Su.

Moosey said he was struck by comments from Chinese finance groups that there could be huge savings for the Alaska LNG Project if the LNG export plant were built at Port MacKenzie rather than at Nikiski, on the Kenai Peninsula.

"Their bankers are well aware of this potential," Moosey said, even if the Alaska LNG Project itself, which is led the state, doesn't seem to be.

State Rep. Andy Josephson, D-Anch., was along on the trip to learn more about the potential for Alaska resource exports and also to do his own due diligence on the pending deal with Chinese companies to purchase liquefied natural gas from Alaska and perhaps invest in the Alaska LNG Project.

Josephson met with Sinopec, Bank of China and China Investment Corp., Alaska's three main Chinese partners, and came away impressed with the depth of knowledge of the Alaska project they exhibited.

"They are asking very tough questions, such as the durability of agreements with the three major North Slope gas producers to supply gas to the project, and the status of the Federal Energy Regulatory Commission's procedures," Josephson said.

Josephson co-chairs of the House Resources Committee in the current Legislature, a panel with a direct responsibility to review the project, which is now led by the Alaska Gasline Development Corp., the state gas corporation.

Trident Seafoods' Stefanie Moreland and Lindsey Whitt, External Affairs Manager for Matson Navigation, were on the trip and were at the Thursday briefing.

Trident is a major Alaska seafood company with an established presence in the China market. In spite of that, Alaska's reputation as a source of high-quality seafood needs to be constantly reinforced, she said.

Whitt said Matson hopes to develop new seaborne trade, and a direct Anchorage-Shanghai shipping route is being explored.

"I was honored to lead this trade mission and watch so many Alaskan leaders work to grow their businesses and bring jobs home," Governor Walker said. "Perhaps what impressed me most was the consistent push to build an Alaska brand that makes the world realize the quality of our fresh seafood, the natural beauty of our state, and our many opportunities for economic growth."

Alaskans on the trip attended more than 25 meetings in Chengdu, Beijing, Shanghai, and Hangzhou. While in Beijing, several from Alaska met with JD.com, the world's third-largest internet company by revenue, with 900 million users, and also traveled to Hangzhou to meet with Alibaba Group, the world's largest retailer.

These visits underscored opportunities to increase sales of Alaska seafood, beer, travel packages, and baby food directly to Chinese consumers.

Walker said an intriguing possibility is an Alaska-China link in helping train athletes for winter sports including the winter Olympics planned for China in 2022. Members of the Alaska group met in Beijing with China Sports Minister Guo Zheng, who oversees China's Olympic team.

This discussion has already led to agreements for the Chinese downhill ski team to train at Alyeska Resort and for their cross-country ski team to train at Alaska Pacific University facilities. Follow-up meetings will take place this month in Alaska.

Walker is also keen to promote direct flights between Alaska and China to facilitate growing Chinese tourism. "Just as the cruise industry has brought huge economic opportunities to coastal Alaska communities, direct flights will provide the benefits of new, diverse tourism statewide," the governor said at the Wednesday briefing.

Alaska is still new getting into the Chinese market, although Alaskan firms have sold

seafood and timber to Chinese buyers for years. “Chinese companies have 1,500 deals in 50 states of the U.S. but only three of these are in Alaska,” the governor said.

“As a result of this trip we’re working our way up,” he said.

Economic Development Opportunities in China 2018

China's economic drivers

***1.4 billion people in China**
(more than 4x greater than U.S.)

Growing middle class who like to travel

Poor air quality driving LNG needs
(willing to buy all the gas Alaska can provide)

*National Bureau of Statistics 2017

Economic Development Opportunities in China 2018

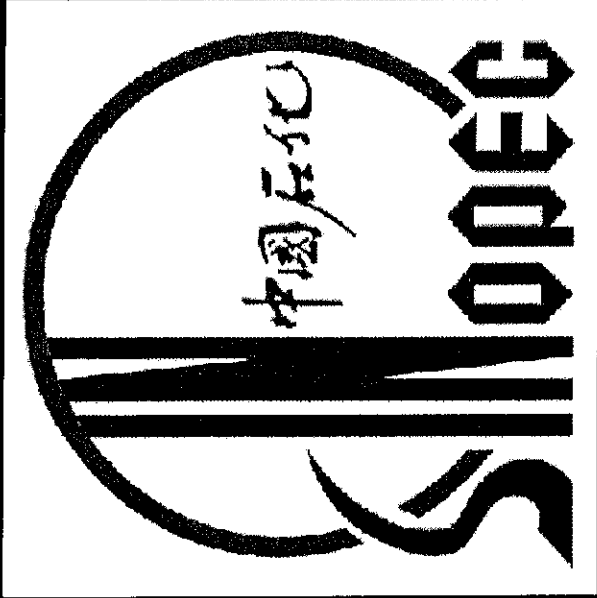
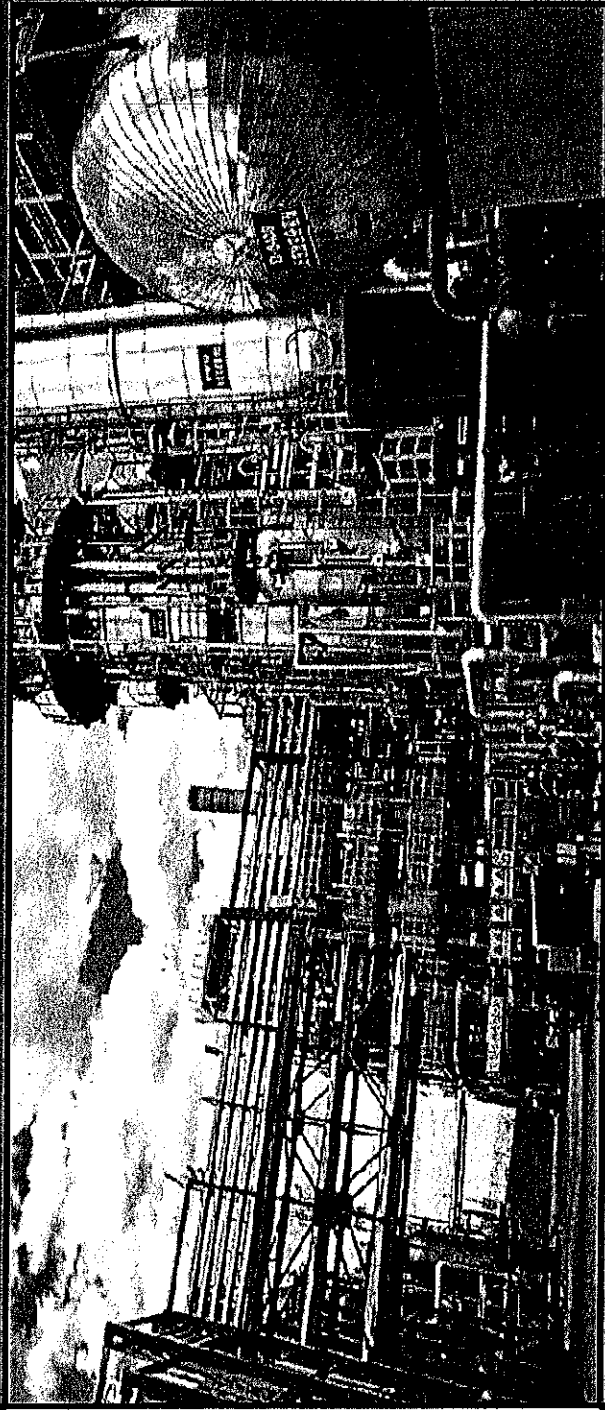
What we have to offer

Port MacKenzie and Rail

Chijuk logs to China

Potential LNG

Tourism for growing class of Chinese tourists



World's largest oil refining, gas and petrochemical conglomerate



The leading online commerce provider in China

Alibaba Group

Port of Shanghai



World's busiest container port

Port of Shanghai



Handles **32 million** containers per year

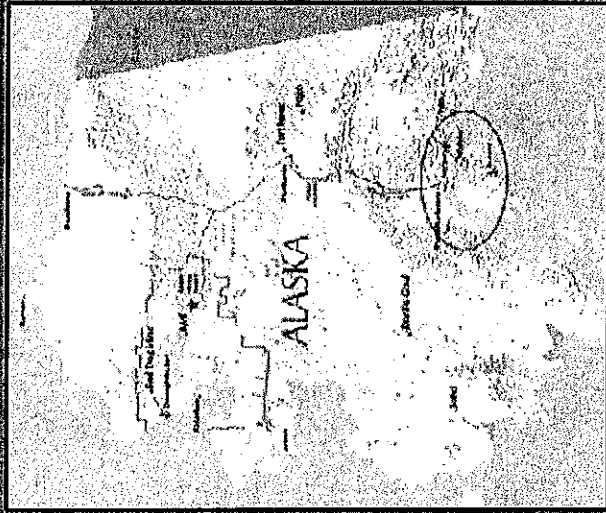
Touring the Port of Taicang, China



TRILOGY METALS, INC.

Port MacKenzie and a rail spur connecting it to the rest of the Alaska Railroad infrastructure would definitely reduce our transportation costs and become an important part of our logistical supply chain plan."

—Trilogy Metals Inc., CEO Rick Van Nieuwenhuyse



Borough Manager John Moosey meets with Trilogy Metals, CEO Rick Van Nieuwenhuyse

**8 Billion pounds of copper, 3 Billion pounds of zinc and over
1 million ounces of gold equivalent precious metals**

ANCHORAGE DAILY NEWS

Mat-Su

Price tag for cyberattack on Mat-Su Borough now tops \$2 million

✎ Author: Zaz Hollander ⓘ Updated: October 12, 2018 📅 Published October 11, 2018



iStock / Getty Images

Get your first month of unlimited digital access for only
\$1.99

Subscribe Now >



computer systems for weeks this summer.

The borough's systems still aren't totally back online as officials finish recovering from the pervasive malware and build in security upgrades deferred in the past.

The devastating attack took out 650 desktop computers and servers three months ago, knocking offline everything from landfill receipts to borough email.

Now borough administrators are asking the Mat-Su Assembly to move \$1 million into emergency reserves to help cover the costs. The Assembly meets Tuesday night.

The request is for \$500,000 from a repair and renovation reserve and another \$500,000 from a capital expenditures reserve.

The money is paying for recovery — "cleaning" virus-infected computers and servers — but also improving the security system with upgrades deferred in past years, borough IT director Eric Wyatt said Thursday.

"I couldn't just bring us back to where we were," Wyatt said. "I have to bring us back to an improved state."

About 35 to 45 percent of the spending is for improvements that should put the borough two or three years ahead on security projects, he said.

But the cyberattack effects still linger in the system.

Parents trying to register children for swimming lessons can't do that online yet, though that's a few days away, officials say. Earlier this week, the borough's popular property parcel viewing site came back up.

Limited access is slowing some public records requests. The borough records management system survived completely but some historical email has been lost, Wyatt said. Ongoing projects, like road or building projects, also aren't entered in that system until they're complete so some of that data may be lost.

Employees generally can't use external storage devices like thumb drives right now to prevent more infection from viruses.

The borough declared an emergency over the cyberattack in late July, requesting help from state disaster money but that request hasn't been approved.

Officials also expect to tap a cyber insurance policy with possible reimbursement of up to \$1 million. That policy won't cover all of the costs, but it will cover aspects, Wyatt said.

The cost of responding to the attack is approaching \$2.1 million, according to a memo attached to the Assembly proposal.

That number could rise slightly due to the cost of establishing whether hackers stole data and any future notifications that might be necessary, Phillips said.

Get your first month of unlimited digital access for only
\$1.99

Subscribe Now >



Officials initially said it cost an average of \$1 million to recover. But, Wyatt said, widespread and severe attacks over the sun drove up the "price tag" to an average of \$3.5 million for an organization the size of the borough.

Within just a month of a March malware attack, the city of Atlanta had already spent \$2.7 million, the Atlanta Journal-Constitution reported. That total didn't include legal fees, and was expected to rise substantially.

That number could hit \$17 million, the Journal-Constitution reported in August.

The paper also reported that the Colorado Department of Transportation was estimated to have spent \$1.5 million to get computers back up and running after ransomware attacks in February and March.

Meanwhile, Wyatt said, some victims of cyberattacks are taking six months or more to recover.

"We're actually doing pretty well," he said.

The city of Valdez was also the victim of malware in which electronic data was held for "ransom" that the city didn't pay, acc to a report in the Valdez Star. The city rebuilt its IT systems but employees now have totally new email addresses.

About this Author

Zaz Hollander

Longtime ADN reporter Zaz Hollander is based in the Mat-Su and is currently focused on coverage of the coronavirus in Alaska. also covers the Mat-Su region, aviation and general assignments. Contact her at zhollander@adn.com.

Comments

MAT-SU BOROUGH

Mat-Su Declares Disaster for Cyber Attack

Mat-Su | Patty Sullivan | Tuesday, July 31, 2018

At the Assembly meeting tonight, Matanuska-Susitna Borough Manager John Moosey reported that he had declared disaster today due to the severity and magnitude of a cyber attack.

At the close of the meeting, Assembly Member Ted Leonard called it a terrorist attack.

Here is an excerpt from the declaration.

"... the Borough's computer infrastructure, including computers/laptops, most Borough servers, networked telephones, and the email exchange have been compromised; and

WHEREAS, the cyber-attack has caused major disruption in Borough services and loss of productivity, which may continue for a prolonged time; and

WHEREAS, the Borough's IT department staff are working a great deal of overtime, and IT service providers have been engaged at significant expense, and, ...".

Manager Moosey told the audience the declaration gives us access to our insurance, the emergency part of the budget and possible FEMA assistance. The declaration is posted here.

Mat-Su Borough IT Director Eric Wyatt gave the Assembly the latest update on the crisis. His below quote and full audio are posted here.

"We learned that one of the prongs of the attack, the trojan horse, is called the Emotet what we have learned is this is the worst of its type in the nation according to top anti-virus companies that do this internationally..another component Cryptolocker what is sometimes called the was ransomware portion also called Bitpaymer also the worst of its type in the nation, other embedded component (malware) called Dridex that is also the worst of its type. And so the group that we are facing that has unleashed this particular attack is a very well organized group and they're using the most sophisticated tools and have done a lot of damage across the country to include us." —Eric Wyatt, IT Director, Mat-Su Borough

Our victim number is 210 for this virus, Wyatt said, meaning that 209 others are victims before us. In Alaska, so far Valdez also has the virus.

Resident Kurt Bunker, an IT consultant working with Borough IT, testified to the Assembly about the crisis response.

"I'm proud to be working with your team. The incident response has been incredible. The FBI commented several times during design sessions with me how rapid and how efficient you guys have been in containing and dealing with the effort. I think your IT teams have done a wonderful job. Everybody's very exhausted. I'm mumbling because I'm beyond exhaustion for the last six days. I think everybody needs a pat on the back and some encouragement and this is going to be a long journey to recover. ... This is cyber crime and this is the future that we are dealing with."

Mayor Vern Halter thanked Wyatt for a "thorough job" under "tough circumstances."

More phones were restored to departments today. By Wednesday most phones are expected to be in service.



—End—

CONTACT US

Information contact Public Affairs Director Patty Sullivan at 861-8877 or
Contact Us (Emails) patty.sullivan@matsugov.us (<mailto:patty.sullivan@matsugov.us>)

JOIN US

Job Opportunities
(<https://www.governmentjobs.com/careers/matsugov/>)
Volunteer Opportunities
(<https://www.governmentjobs.com/careers/matsugov/transfer/jobs>)
Serve on a Borough Board
([/boards](https://boards.matsugov.us))
Employee Mail & Services
([/join-us/employeeservices](https://join-us/employeeservices))

FOLLOW US

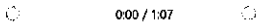


Documents

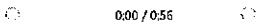
Cyber Disaster Declaration July 31, 2018 (</news?task=download>)

Audio

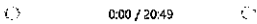
Worst of Its Kind, Eric Wyatt on the cyber virus characteristics



IT Consultant Kurt Bunker is proud to work on incident response with Mat-Su Borough



Full update by Eric Wyatt, IT Director Mat-Su Borough on the Cyber Attack 2018 before the Assembly





All Articles

How One Alaskan Borough Survived A Cyber Attack

OCTOBER 1, 2019

In today's cyber landscape, every city, town and village in America is vulnerable to hackers. And while some local governments are taking

steps to prevent and mitigate harm, many more municipalities remain completely unprepared, leaving their communities in danger of losing millions of dollars and priceless data.

This is an urgent issue for cities of all sizes. To help local leaders address it, the National League of Cities will release the *first-ever* cybersecurity guide for local leaders later this month. But in honor of National Cyber Security Month, we're bringing you a sneak peak of our report.

Case Study: Matanuska-Susitna Borough, Alaska

In Matanuska-Susitna (also called Mat-Su), a borough of about 103,000 people in southern Alaska, local officials felt secure. Before the attack, the borough monitored web, email, and network traffic; they'd already weathered DDOS attacks, viruses, malware, and ransomware; and they had a good backup/disaster recovery system designed to withstand the next big Alaskan earthquake.

But in mid-2018, several Alaskan local and state government organizations were hit by cyberattacks. Matanuska-Susitna was hit with an advanced malware suite on July 23, 2018, which took down 150 servers and nearly 600 desktop computers. Mat-Su and the nearby city of Valdez were completely incapacitated. The two governments were both infected with ransomware, but responded differently: Valdez decided to pay the ransom, whereas Mat-Su did not.

Upon investigation, Mat-Su found that the attack had infected and encrypted their backups. Primary cleanup and mitigation took three

months and cost \$2.5 million. To reduce the risk of a new infection, both cities completely rebuilt their networks and scrubbed all data imported to the new networks.

There are many models for cybersecurity, the most common of which, *prevention*, is no longer enough. After the attack, Mat-Su augmented its security protocols: today, its multi-level email filters capture more than 650,000 bad emails an hour. But despite the robust prevention processes, there are still dozens of targeted email attacks that get through daily. Alone, the prevention method has to be correct 99 percent of the time. For that reason, Mat-Su now uses the *detect and contain* approach as well.

Recommendations from the National Symposium for Cybersecurity in Government

Last week, government leaders, researchers and advocates gathered to discuss cybersecurity best practices at the Symposium for Cybersecurity in Government. The event was a collaboration between CompTIA/Public Technology Institute (PTI) and other state and local organizations to identify best practices and pitfalls for leaders.

There were five clear takeaways from the event. In order to detect and contain cyberattacks, Local governments, like Mat-Su, should:

- Get creative with budgeting
- Use trusted third-party security services,
- Routinely check the workforce for information gaps,

- Craft a culture of good practices, and
- Have a response plan ready to go should an attack occur

Any city could be attacked, so training staff to identify and curtail risks, as well as implementing measures to respond when attacks occur, is critical.

0

About the author: *Kyle Funk is the research assistant, urban innovation, at the National League of Cities.*

IN DEPTH | HACKING

The cyber-attack that sent an Alaskan community back in time

[!\[\]\(de95854c7ee024cfadc48187bbb781b2_img.jpg\)](#) [!\[\]\(cef08d8c15d8a8acd5e25ab0d65432c3_img.jpg\)](#) [!\[\]\(c244836fd67166dc60ebf5279a0f8377_img.jpg\)](#) [!\[\]\(c9651b690bdf1dda88278b8b3445c7b1_img.jpg\)](#)*(Image credit: Getty Images)*

By Chris Baraniuk 9th January 2019

In 2018, a remote Alaskan community's infrastructure was hit by a malware attack which forced it offline. It was only then they realised how much they depended on computers.

Article continues below

They still don't know where it came from. But when it hit, the Alaskan borough of Matanuska-Susitna was knocked for six. Malware rapidly spread across the borough's computer networks, disrupting a bewildering array of services. Hundreds of employees found themselves locked out of their work stations. Staff at local libraries received urgent phone calls telling them to quickly turn off all the public PCs. The animal shelter lost access to data on medications required by its furry residents.

It didn't stop there. An online booking system for swimming lessons went down, leaving people to queue up in person. One borough office had to switch to electronic typewriters temporarily. And Helen Munoz, an 87-year-old woman who has been campaigning for a better sewer system in the area, got an unexpected response to one of her regular calls to local administrators. "Our computers are down," she was told. She threw her hands up in disgust.

"The cyber-attack, God help us, just about stopped everything, you know," Munoz says. "In fact, the borough still isn't squared away with their computers."

ADVERTISEMENT

Matanuska-Susitna, known as Mat-Su, is still trying to recover from what happened, months after the attack began in July 2018. When the first signs of malware popped up, no-one expected the turmoil that followed. IT staff initially worked up to 20 hours a day, tasked with digitally scrubbing clean 150 servers.

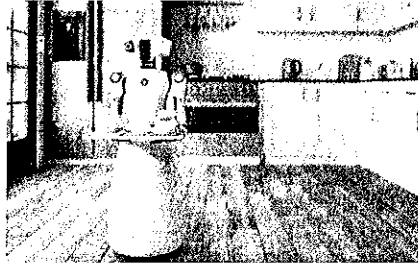
You might also like:

- **The cyber-attack that crippled a nation**
- **A new front in cyber-warfare**
- **The tiny code that can stop a warship**

Mat-Su, a largely rural borough stretching across an area the size of West Virginia or Latvia, is home to just 100,000 people. It seems a strange target for a cyber-attack.

This is the story of what happened.

Story continues below



How tech transformed our homes

Robots, AI assistants and more. How might tech continue to transform our living spaces?



The cyber-attack crippled many of the borough's activities (Credit: Getty Images)

On the morning of 23 July 2018, employees at the borough offices of Matanuska-Susitna in the tiny town of Palmer arrived for work as usual. Within a few hours, an anti-virus programme flagged unusual activity on some of their PCs.

The borough's IT director, Eric Wyatt, told his team to take a closer look. They found some malicious files, so they followed standard procedure: get staff to change their passwords and, meanwhile, prepare an automated programme to clear out any suspicious software.

But when they launched this defence mechanism, there was an unintended response.

The scale of these cyber-attacks was certainly new to Wyatt

Wyatt watched as the network lit up. It looked like a larger or second stage attack had been triggered. Perhaps someone was monitoring the IT department's defensive moves, or it was an automatic response by the malware. Either way, it had begun spreading further and, in some cases, it locked down more employees' files and demanded ransom payments.

This form of malware is known as 'ransomware' – an **increasingly common, and dangerous, threat** to computer systems. In recent years, ransomware outbreaks around the world have temporarily shut hospitals, halted production at factories, skewed operations at major ports and sent hundreds of offices into chaos. Some estimates put the annual total **cost of ransomware events at several billion dollars**.

The scale of these cyber-attacks was certainly new to Wyatt, who started his IT career in the US Air Force before working for defence and government contractors.



Malware ransom attacks are thought to have cost companies several billion dollars (Credit: Getty Images)

"I have over 35 years in this business and have dealt with this kind of thing during that time," he says. "This was certainly larger than anything I had seen, more sophisticated."

When he realised the incident was going to cause significant headaches, he went to see borough manager John Moosey.

Moosey listened as Wyatt explained what he knew about the situation. Moosey and Wyatt were soon on the phone to the FBI – and their insurer – explaining that they seemed to be the target of a large cyber-attack.

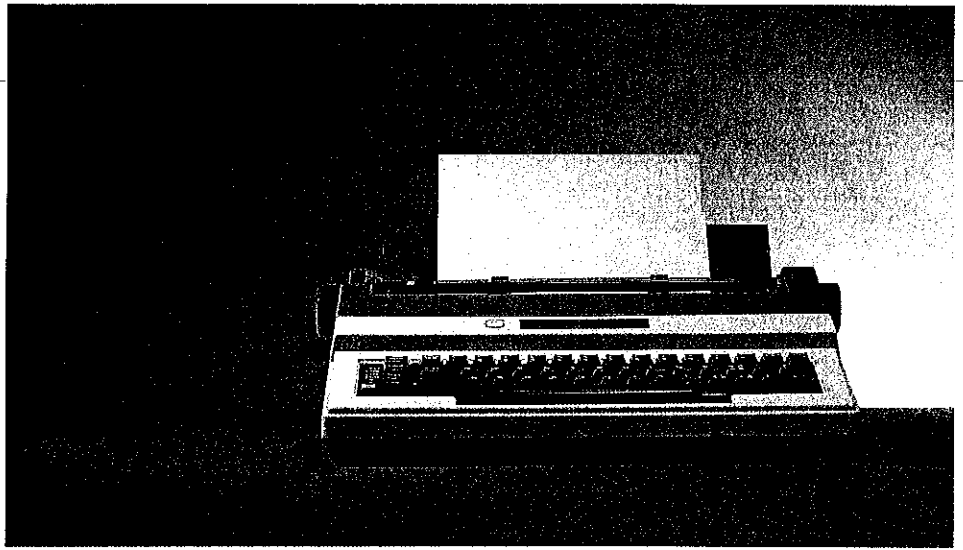
Almost all of the borough's office phones had to be taken offline. As IT experts were drafted in to help with the recovery, printers and computers were gathered up in droves – more than 700 devices in total had to be checked and scrubbed. "All data is considered suspect," read one update published a short time later.

They wanted the library to disconnect every computer and printer – not just switch them off, but unplug them too

"It really hammered us extremely hard," says Moosey.

In the borough's purchasing department, staff faced filling out forms with pen and ink while their computers sat idle. Then they had a bright idea. In the cupboard were a couple of old electronic typewriters. They dusted them off and used them, a **move that made international headlines**.

As systems were taken offline, and staff switched to mobile phones and temporary webmail services, many functions of the borough were forced to slow down. Computer programs had been designed to help process everything from data on construction sites to credit card payments at the local landfill – but now they were all out of action.



The borough's purchasing department were forced to dust off their old typewriters because all computers were impounded (Credit: Getty Images)

"The virus was amazingly terrible," says Peggy Oberg, a librarian at the Big Lake Public Library in south central Mat-Su.

In the space of one week, Big Lake library welcomes between 1,200 and 1,500 people through its doors. Many of them rely on internet and computer services there.

Oberg remembers the call she got from the IT department. They wanted the library to disconnect every computer and printer – not just switch them off, but unplug them. Staff were also asked to turn off the public wi-fi.

In 20 years, Oberg had never had a call like it.

Staff at a number of the borough's libraries were also unable to place books on hold, search for new items patrons requested, or communicate through the usual channels with other colleagues around Mat-Su. For a few weeks, they were partially cut off.

I don't mind technology, but when I can't get a sewer system built I get very uptight – Helen Munoz

Oberg spent two months worrying that the data for library groups and services would be lost forever.

"I was kind of sick thinking about them possibly not being able to recover that," she says. Thankfully, she later found that the files had in fact been restored, nine weeks after she'd last had access to them.

Mat-Su's local animal shelter takes in between 200 and 300 stray or unaccounted-for animals every month – from stray domestic pets to livestock found on open roads. Staff computers at the shelter were taken away. Without records of medications and previous cases, employees didn't know how much to charge people who came to collect pets or missing cattle. The website with photos of animals up for adoption also couldn't be updated.



The borough's animal shelter could not keep track of which animals had been vaccinated (Credit: Getty Images)

Helen Munoz is an 87-year-old resident of Palmer. She moved to Mat-Su in the 1970s with her husband, whose family ran a septic tank and sewerage business. Lately, she has made it her mission to force an improvement of Mat-Su's own sewage system. She has a place on a committee overseeing the development of a new waste-water treatment plant.

Munoz was frustrated by the way the hampered communications affected the borough. "I don't mind technology, but when I can't get a sewer system built," she tells me, "I get very uptight."

Others were equally worried. As one local resident put it in a comment to a Facebook update about the cyber-attack: "It's pretty amazing how this can effect [sic] our day-to-day.

"So far it's changed the way I had to pay for the dump, the email proof of my dog getting his rabies vaccine hasn't shown up, and when I pay my taxes it looks like that's going to be different too."

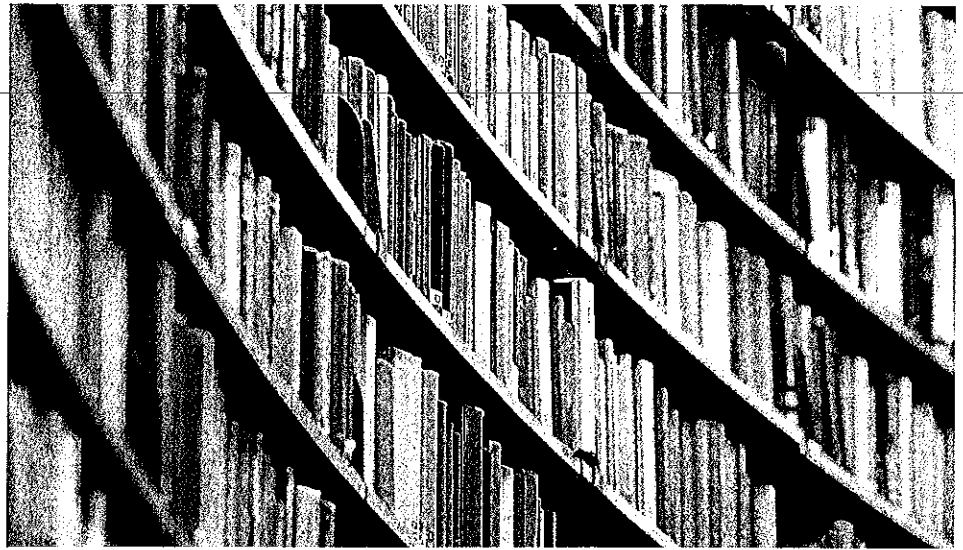
Shortly after the attack began, investigators found evidence that the malware had been on the borough's systems since May

Meanwhile, Mat-Su estate agents, who regularly sign in to an online system for local land registry data, found themselves locked out. Even the system for signing up children for swimming lessons went down.

"Everyone had to stand in line, it was all done the old-fashioned way," says Nancy Driscoll Stroup, a local lawyer and critic of the borough.

The incident has so far **cost Mat-Su more than \$2m (£1.59m).**

Shortly after the attack began, investigators found evidence that the malware had been on the borough's systems since May. This raises Stroup's curiosity – she notes that a borough delegation visited China on a trade mission that month. While no-one has made any official link to the Chinese, there have been allegations of Chinese involvement in other recent hacking episodes.



Libraries were unable to search for books, nor place any on hold for patrons (Credit: Getty Images)

As they combed through the digital wreckage, Wyatt and his colleagues realised that the malware had deposited data, in files named with a specific number, on victim computers. After investigating, they realised this number, 210, identified Mat-Su as the 210th victim of this particular version of the malware; the other 209 victims are still unknown.

They also gleaned some clues now about how the attack started. Wyatt has some hints it was a targeted phishing attack, in which an organisation working with the borough was compromised in a separate attack. Wyatt says he has evidence that this allowed someone to send a carefully composed malicious email, containing the first batch of malware, to a Mat-Su employee.

By cloaking an attack within a seemingly innocuous message, malware creators increase the chances that someone clicks on a link or downloads the attachment that spreads the malware to their computer. From there, it can attack other computers on the same network.

The only people to blame are the people who write these viruses – Eric Wyatt

Wyatt doesn't blame anyone for being tricked, though. "The only people to blame are the people who write these viruses," he says.

Over the ensuing 10 weeks, a dedicated team gradually brought the majority of Mat-Su borough's affected services back online.

In August 2018, Wyatt appeared in a **YouTube video published by the borough** explaining the extent of the recovery operation. IT contractor Kurtis Bunker was also filmed saying he thought the FBI had been "pleasantly surprised" at how Mat-Su's staff responded to the attack.

Not all members of the public were understanding. "Who or why would anyone 'hack' a little rinky dink town?" scoffed one Facebook user. But many were supportive. And various organisations that have links or business relationships with the borough were also part of a larger effort to make sure the cyber-attack didn't spread any further.

Home	News
Sport	Reel
Worklife	Travel
Future	Culture
Music	TV
Weather	Sounds

Terms of Use	About the BBC
Privacy Policy	Cookies
Accessibility Help	Parental Guidance
Contact the BBC	Get Personalised Newsletters
Advertise with us	AdChoices / Do Not Sell My Info

Copyright © 2021 BBC. The BBC is not responsible for the content of external sites. [Read about our approach to external linking.](#)

An Alaskan borough turns to typewriters and handwriting after its computers were hacked

click to share free access x

August 1, 2018



After a devastating cyberattack forced a borough in Alaska to shut down many of its computer systems, officials there turned to an unlikely savior: typewriters.

Staff in Matanuska-Susitna, a south-central borough of Alaska, began relying on typewriters after hackers locked them out of their computers and email server, according to the BBC. The perpetrators used what's known as a ransomware attack, deploying malicious software to take control of digital systems and then demanding payment from the victims to get their data back. While the borough works to bring its systems back online, officials "reenlisted typewriters from closets" and wrote receipts and lists of library members by hand, according to Bleeping Computer, a technology website.

The borough said that beginning in mid-July, hackers seized its desktop computers, most of its servers, telephone system and email exchange. On the borough's home page, visitors are greeted with an arresting banner: "Mat-Su Declares Disaster. Worst of its Kind Cyber Attack."

Borough Manager John Moosey declared the cyberattack a disaster Tuesday, according to a statement by public affairs director Patty Sullivan. Moosey told members of the public at a Borough Assembly meeting that the declaration grants the borough access to its insurance, funds dedicated to emergencies and possibly the assistance of the Federal Emergency Management Agency.

The borough anticipates that the major disruptions caused by the cyberattack may continue for a "prolonged time." The loss of services and productivity, the borough said, is compounded by the high cost of hiring IT specialists and the "great deal of overtime" that the borough is paying IT department staff.

Borough IT Director Eric Wyatt said the perpetrators deployed hacking tools that were the "worst of its type," citing international cyber experts who have experience with the kind of ransomware that was used. The computer virus that infected the borough has claimed 209 previous victims, he said. "The group that we are facing that has unleashed this particular attack is a very well-organized group, and they're using the most sophisticated tools and have done a lot of damage across the country to include us."

The data encrypted by the hackers was turned over to the FBI, Wyatt said in a report earlier this week, in the hope that federal agents can recover the decryption keys needed to retrieve the information.



ADVERTISEMENT

SECURITY

Recovery Has Not Come Cheap for the Alaskan Borough Targeted by Hackers

The cost of the summer cyberattack that devastated the Matanuska-Susitna Borough computer system has already topped \$2 million. Now officials are asking for more.

October 12, 2018 • Zaz Hollander, Alaska Dispatch News

(TNS) — PALMER, Alaska — It's cost more than \$2 million to respond to the cyberattack that paralyzed Matanuska-Susitna Borough computer systems for weeks this summer.

The borough's systems still aren't totally back online as officials finish recovering from the pervasive malware and build in security upgrades deferred in the past.

The devastating attack took out 650 desktop computers and servers three months ago, knocking offline everything from landfill receipts to borough email.

ADVERTISEMENT

Now borough administrators are asking the Mat-Su Assembly to move \$1 million into emergency reserves to help cover the costs. The Assembly meets Tuesday night.

The request is for \$500,000 from a repair and renovation reserve and another \$500,000 from a capital expenditures reserve.

The money is paying for recovery — "cleaning" virus-infected computers and servers — but also improving the security system with upgrades deferred in past years, borough IT director Eric Wyatt said Thursday.

ADVERTISEMENT

"I couldn't just bring us back to where we were," Wyatt said. "I have to bring us back to an

improved state."

About 35 to 45 percent of the spending is for improvements that should put the borough two or three years ahead on security projects, he said.

But the cyberattack effects still linger in the system.

Parents trying to register children for swimming lessons can't do that online yet, though that's a few days away, officials say. Earlier this week, the borough's popular property parcel viewing site came back up.

Limited access is slowing some public records requests. The borough records management system survived completely but some historical email has been lost, Wyatt said. Ongoing projects, like road or building projects, also aren't entered in that system until they're complete so some of that data may be lost.

Employees generally can't use external storage devices like thumb drives right now to prevent more infection from viruses.

The borough declared an emergency over the cyberattack in late July, requesting help from state disaster money but that request hasn't been approved.

Officials also expect to tap a cyber insurance policy with possible reimbursement of up to \$1 million. That policy won't cover all of the costs, but it will cover aspects, Wyatt said.

The cost of responding to the attack is approaching \$2.1 million, according to a memo attached to the Assembly proposal.

That number could rise slightly due to the cost of establishing whether hackers stole data and any future notifications that might be necessary, Phillips said.

Mat-Su was one of many governments hit by similar attacks.

Officials initially said it cost an average of \$1 million to recover. But, Wyatt said, widespread and severe attacks over the summer drove up the "price tag" to an average of \$3.5 million for an organization the size of the borough.

Within just a month of a March malware attack, the city of Atlanta had already spent \$2.7 million, the Atlanta Journal-Constitution reported. That total didn't include legal fees, and was expected to rise substantially.

That number could hit \$17 million, the Journal-Constitution reported in August.

The paper also reported that the Colorado Department of Transportation was estimated to have spent \$1.5 million to get computers back up and running after ransomware attacks in February and March.

Meanwhile, Wyatt said, some victims of cyberattacks are taking six months or more to recover.

"We're actually doing pretty well," he said.

The city of Valdez was also the victim of malware in which electronic data was held for "ransom" that the city didn't pay, according to a report in the Valdez Star. The city rebuilt its IT systems but employees now have totally new email addresses.

©2018 the Alaska Dispatch News (Anchorage, Alaska) Distributed by Tribune Content Agency, LLC.



ADVERTISEMENT

SECURITY

Alaska Hacks May Have Lurked in Network for Months

A malware attack targeting multiple city networks may have been hiding in the Matanuska-Susitna Borough's computer network.

• Zaz Hollander, Alaska Dispatch News

(TNS) — PALMER, Alaska — The computer malware that penetrated the safeguards of one of Alaska's largest municipalities last week may have lurked in the Matanuska-Susitna Borough's computer network for more than two months.

The borough is still recovering from the "insidious" attack that clobbered phones, email and online systems and decommissioned some 650 desktop and server computers, officials there said Monday. Many of the disabled computers and multiple outlying offices remained offline.

The same virus hit Valdez, where it shut down all city computers and servers Friday.

ADVERTISEMENT

Both governments say they didn't store personal credit card information on any of the

computers or servers damaged in the cyberattack.

The attack appears to have been "lying dormant and/or undiscovered" within the Mat-Su network since as early as May 3, according to a memo distributed to employees Monday morning.

Some Mat-Su borough phones and email were restored by Monday after staff worked long nights through the weekend to restore systems, IT director Eric Wyatt said. The borough shut down systems last week to limit potential damage, though its website remained operational.

ADVERTISEMENT

Employees dragged out typewriters. Departments working without computers shifted to pen and paper.

Fire stations and any buildings outside the main borough headquarters in Palmer didn't have phone service Monday, according to public works director Terry Dolan. That was a deterioration since Friday.

The borough sent six-person teams to work on phones at two main fire stations, animal control and capital projects departments as of Monday afternoon, according to public information officer Patty Sullivan. Public works was expected to get a team Tuesday.

Phones went down because the system was rebuilt Sunday night, Sullivan said.

About 100 desktop computers hit by the virus got cleaned up and were expected back on desks by the end of the day, Wyatt said Monday. By the end of the week, another 200 computers for critical systems in finance, tax, and property departments were expected to be restored.

Still, it will probably be three weeks before normal operations are restored, he said.

Mat-Su rebuilt its domain Sunday and redesigned and augmented parts of the network to

deal with "this new and emerging threat," according to the memo.

At the borough's landfill near Palmer, computers and phones were still down Monday afternoon. Users got hand-written receipts from staffers doing math without the aid of computers, working with information that would have to be entered into the system later.

Officials urged the public to avoid the landfill if possible.

"We have a manual system in place. We're handwriting tickets," Dolan said. "It's going about as well as can be expected."

Borough officials said they initially feared the loss of a trove of historical information, such as financial documents and property information, because some backup systems were also damaged. But one layer held encrypted data that allowed at least some of the information to be recovered.

An investigation continues into the path the attack took.

At this point, Wyatt said, it appears an employee opened an attachment or clicked on a link that held the malware.

"Even if we find the person initially that was fooled by this phishing attack, this is not finger-pointing whatsoever," he said. "The only people to blame for this is the people that wrote this virus."

Both Mat-Su and Valdez are working with the Federal Bureau of Investigation. An FBI cyber expert in Anchorage wasn't available for comment Monday.

Wyatt said he met early with the Mat-Su school district to warn them and credited the public and roughly 20 entities as the borough worked through the damage done.

The borough IT memo Monday morning described a "multi-pronged, multi-vectored attack" that came not from a single virus but from malware with aspects including a Trojan horse — harmful software that appears legitimate — and at least one external hacker who logged into the borough's network.

The memo, from the borough's IT department, described the malware as an advanced persistent threat and a "Zero-day" attack so new anti-virus software isn't prepared for it.

The malware lays dormant for four to six weeks, and then a "Crypto Locker" component is launched, according to the Mat-Su memo. That's what happened in Valdez too.

The Alaska Municipal League hadn't heard from any other government members with problems. There were no reports of malware problems at University of Alaska, officials there said Monday.

There are no indications the malware infected any state assets, said Shannon Lawson, the state's chief information security officer.

Some organizations are targeted by malware like this, others are just unfortunate, Lawson said.

"These things don't take a lot to be very deadly in terms of damaging and just shutting things down," he said.

©2018 the Alaska Dispatch News (Anchorage, Alaska) Distributed by Tribune Content Agency, LLC.

ADVERTISEMENT



Featured Resources

CISCO SECURE

2020 Security Outcomes Study

Defending Against Critical Attacks

How Cisco Can Help Align with CMMC

Simplify Your Security Platform with SecureX

Protecting State and Local Government from Cyberattacks

ADVERTISEMENT

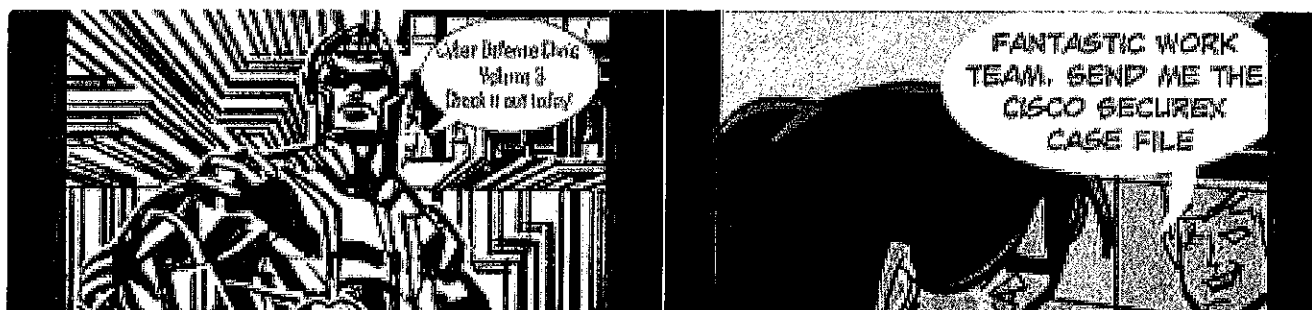
Tweets by @CiscoSecure



Cisco Secure
@CiscoSecure

Need some #Fridayfun reading? Follow the escapades of Mr. Black & his crony team of #hackers to see how Cisco #cybersecurity tools continually thwart their schemes in our new Cyber Defense Clinic comic!

cs.co/6010yA6V4#Comicbook #cyberdefense #security



Embed

[View on Twitter](#)

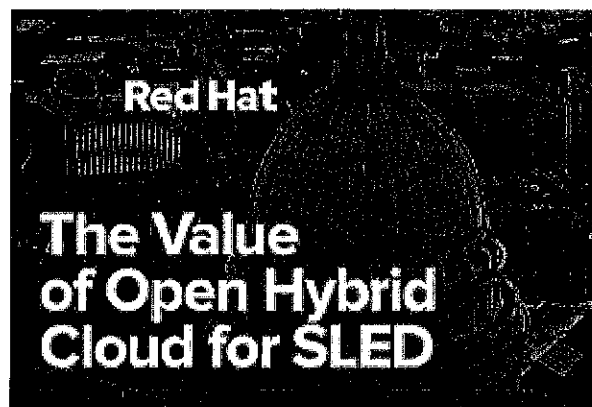
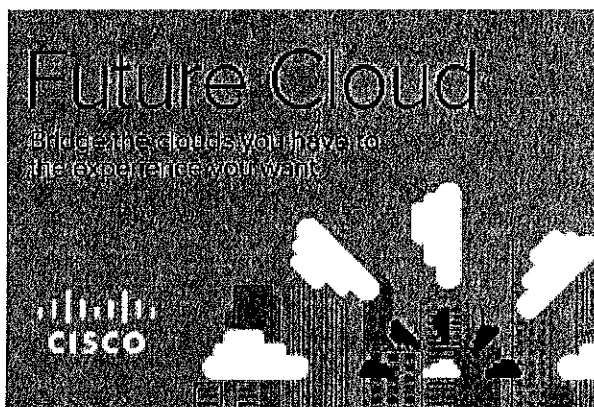
ADVERTISEMENT

Special Projects



Adapt and
Transform
Your Agency

verizon✓



Sponsored Article

Sponsored Articles

SPONSORED

State of Washington Teams with Deloitte to Use Red Hat OpenShift

February 12, 2021

SPONSORED

State IT Department Builds Digital Services with Red Hat OpenShift

September 17, 2021

SPONSORED

Denver supports remote work with Red Hat Ansible Automation Platform

September 17, 2021

SPONSORED

Getting It Right with Microsoft Teams: Lessons Learned and Best Practices

September 15, 2021

Load More

Events

Webinars

Papers

GovTech360 Podcast

Sponsored: Industry Q&As

About

Privacy

Contact

Advertise

Stay Up To Date

Get smart with GovTech. Your guide to technology in state & local government.

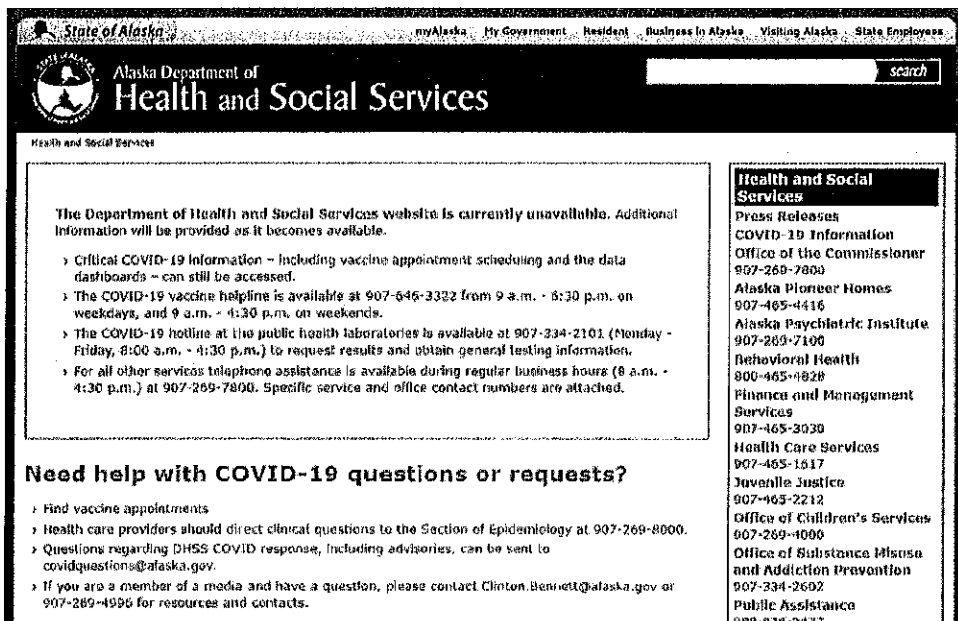
SIGN UP FOR NEWSLETTERS

GET THE MAGAZINE

©2021 All rights reserved. e.Republic
California Residents - Do Not Sell My Personal Information

'Sophisticated group' behind Alaska cyberattack, agency says

By Becky Bohrer - The Associated Press - August 5, 2021



A screenshot of Alaska's Department of Health and Social Services on the morning of Thursday, Aug. 5, 2021, shows a warning the site is unavailable after a malware attack. (DHSS)

A "highly sophisticated group" known for cyberattacks against governmental and other entities is believed to be behind the attack this spring that targeted the Alaska health department, a spokesperson for the department said.

Clinton Bennett, a department spokesperson, said a cybersecurity firm the department is working with had identified as responsible for the incident "a highly sophisticated group known to conduct complex cyberattacks against organizations that include state governments and health care entities." But Bennett, in an email, said the department will not comment on the group's identity, citing an ongoing investigation.

The department said the group had "exploited a vulnerable website and spread from there." The department said it would not provide additional details on the nature and scope of the attack at this time.

[Sign up for Alaska Public Media's daily newsletter to get our top stories delivered to your inbox.]

Information released Wednesday provided new details around the timeline of the attack, which the department previously said was identified on May 17. The department now says the first signs of a "potential attack" were identified about two weeks earlier, on May 2, prompting notification of law enforcement and the subsequent retention of outside cybersecurity services to help investigate.

By May 17, the review found that a server supporting the department's website had been compromised, the department said. The website was taken offline on May 17, the department has said.

The department, on its Facebook page May 17, initially described its website as being offline "due to an unexpected outage." The next day, it said the site had been the target of a malware attack.

RELATED: *Hackers have penetrated multiple Alaska agencies this year.* Here's what we know.

So far, there has been no evidence that protected health or personally identifiable information has been stolen, but the situation remains dynamic and systems continue to be monitored, the department said.

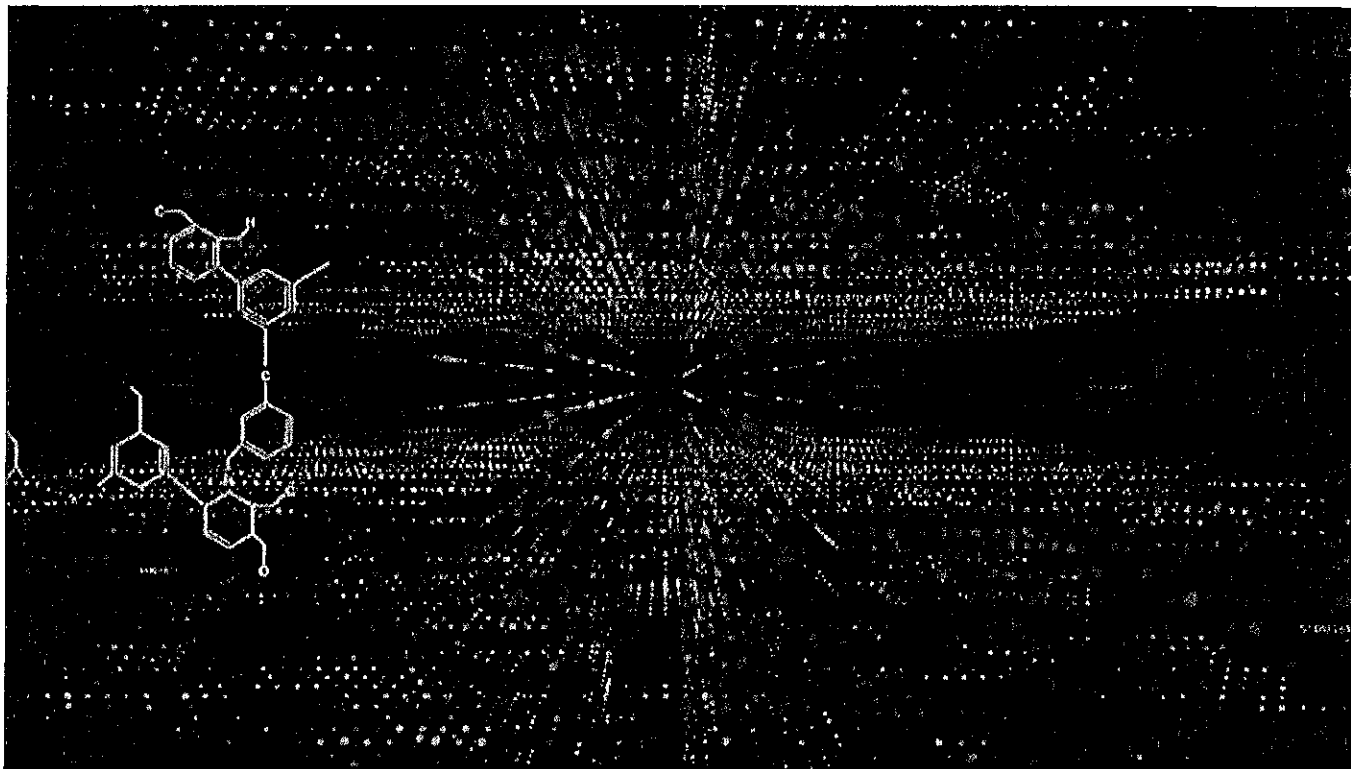
In a statement Wednesday, the department said work continued to "build back resilient systems" and restore online services. A timeline for the full restoration of services remained unclear.

Becky Bohrer - The Associated Press

Select Language ▼

ADVERTISEMENT

State health department: Alaskans' personal information was exposed in May cyberattack



The Alaska Department of Health and Social Services was the target of a cyberattack in May 2021. (GRAY-TV)

By Megan Pacer

Published: Sep. 16, 2021 at 3:47 PM AKDT | Updated: Sep. 16, 2021 at 5:43 PM AKDT



ANCHORAGE, Alaska (KTUU) - Months after Alaska's state health department was the target of a cyberattack that disabled many online services for Alaska residents, state officials say the attack breached stores of personal information and potentially exposed it.

In May, the Alaska Department of Health and Social Services was hit by a cyberattack that disrupted a long list of services, including background checks and obtaining death and birth certificates. The department's main website was down, but the state's data hub for tracking COVID-19 remained online.

On Thursday, the department announced that during the cyberattack in May, there was a breach of the Health Insurance Portability and Accountability Act (HIPAA) and the Alaska Personal Information Protection Act. In a press release, the department said it did not notify Alaskans of this breach sooner "to avoid interference with a criminal investigation."

In a press conference also on Thursday, department Cybersecurity Officer Thor Ryan said it was not up to the state health department to decide whether or when to alert Alaskans to the fact that their information was exposed. The timeline of when to make that information public was dictated by the investigating law enforcement entity, he said.

"It's not up to us to choose when we do that," Ryan said. "Under HIPPA, we are required to delay notification if there is an active law enforcement

During the press conference, department Commissioner Adam Crum said it was fair to say that the personal information of all Alaskans may have been exposed in this attack.



LIVE: Personal information potentially exposed in cyberattack

Alaska's News Source was live • Follow

Share

"The breach involves an unknown number of individuals but potentially involves any data stored on the department's information technology infrastructure at the time of the cyberattack," the release states. "Due to the potential for stolen personal information, DHSS urges all Alaskans who have provided data to DHSS, or who may have data stored online with DHSS, to take actions to protect themselves from identity theft."

Before the department shut down its systems, attackers "potentially had access" to the following information:

- Full names
- Dates of birth
- Social Security numbers
- Addresses
- Telephone numbers
- Driver's license numbers
- Internal identifying numbers (case reports, protected service reports, Medicaid, etc.)
- Health information
- Financial information
- Historical information concerning a person's interaction with DHSS

The department is utilizing the list of people who applied for a Permanent Fund dividend to send out emails that will include a code people can use to sign up for free credit monitoring the state is offering in light of this information exposure. Crum confirmed Thursday that the cyberattack is limited to the state health department, and the department is simply utilizing contact information for PFD applicants to reach more people.

Sylvan Robb, administrative services director for the department, said the opportunity to have that credit monitoring service is open to all Alaskans, and that the contract to provide that service costs about \$215,000.

To ask questions, call 1-888-484-9355 or email privacyofficial@alaska.gov. Alaskans will be able to sign up for the credit monitoring via a toll-free hotline the department is making available next Tuesday, Sept. 21. The phone number and website to sign up for the service will be provided on the department's [website](#).

The evidence from the investigation currently suggests the attack was contained within the state health department, said Scott McCutchen, the department's technology officer, though he said the possibility of lateral movement to other departments always exists.

In its last [press release on Aug. 4](#), the department wrote that "At this time, the investigation has found no indications that this was a ransomware attack and there is no current evidence that Alaskans' protected health information or personally identifiable information was stolen."

Nowhere in that release did the department state that there was the potential of personal information being exposed or compromised. However, the department did address it in an [accompanying frequently asked questions](#) document.

"At this time, Mandiant (a cybersecurity firm) has thoroughly examined the department's technology infrastructure and has currently found no evidence that Alaskans' protected health information or personally identifiable information has been stolen," a section from the frequently asked questions document states. "However, this is still a dynamic situation, and all systems are continuing to be monitored. If at any time DHSS becomes

Three months after the initial cyberattack, the department announced it had gotten its vital records section — the section responsible for processing birth and death certificates — back online, but that staff were working through a backlog of requests. The department had begun using a manual process to fulfill certificate requests and conduct background checks in June.

A press release from the department when the vital records section came back online said that those responsible for the cyberattack were “a highly sophisticated group known to conduct complex cyberattacks against organizations such as state governments and health care entities.”

Editor's note: This article has been updated with additional information.

Copyright 2021 KTUU. All rights reserved.



Around The Web

At 60, Courteney Cox Confirms The Rumors
wordsa

[Pics] Sandra Bullock's Son Is All Grown Up & He Might Look Familiar To You
Life Indigo

[Pics] Sean Hannity Is Living Peaceful Life With His Partner
Boite A Scoop

At 70, Jay Leno Lives Modest Life With His Partner
paydayville

[Pics] At 80, Anthony Fauci Is Still Together With His Partner
networth magazine

[Pics] Inside Joel Osteen's Mansion Where He Lives With His Partner
Hollywood Tale

[Pics] David Muir And His Partner Are Still Together
Docto Report

Search For Best Student Loan Refinancing. Take Advantage Of Low Rates Today
Yahoo Search