Cyber Sabotage and the Key Bridge Collapse

By Cliff Kincaid

April 19, 2024

On April 16, the Washington Post reported that the Federal Bureau of Investigation (FBI) is conducting a criminal investigation into the Francis Scott Key Bridge collapse. Three weeks earlier, the same day of the "accident," Bill DelBagno, the FBI Special Agent in charge of the Baltimore Field Office, had categorically claimed there was "no specific or credible information to suggest that there are ties to terrorism."

The other explanation is cyber sabotage, a form of warfare used by Russia, China, and Iran against U.S. water facilities.

Rather than acknowledge the obvious, the Biden Administration narrative is developing, as reflected in the "news" coverage, that there were "electrical issues" or other "deficiencies" with the ship that somehow caused it to go off-course and strike the bridge, and that the crew was at fault.

I smell a rat. It is like the mysterious fuel tank explosion that supposedly caused TWA 800 to crash off Long Island in 1996, killing 230 people.

As a long-time media critic who has witnessed the paper's increasingly strange behavior under current owner Jeff Bezos, I believe the Post story about a "criminal investigation" was designed to divert the attention of the public away from a state of war with Iran that now exists and which threatens to

escalate dramatically and sink Biden's re-election effort.

Anyone with a casual familiarity with the Post understands that this Washington, D.C.-based paper is a mouthpiece for the U.S. intelligence community and that in this case it wants the public to believe that "accidents happen," rather than acts of war that were not detected or prevented by the FBI, CIA, and NSA.

Playing the tune offered by the Intelligence Community, which still can't figure out that the China virus came from a Communist Chinese lab, the media and their "fact-checkers" are unanimous that the collapse was not the result of terrorism and that the "authorities" can be trusted to inform us of the ultimate truth when they're good and ready. The "criminal investigation" by the FBI is supposed to convince us that the probe will be thorough before a member of the crew is likely blamed.

When a missile or missiles hit TWA 800, the FBI went through the motions of an investigation before calling upon the CIA to do a cartoon video to discredit the eyewitnesses to a missile attack. The joint FBI/CIA cover-up story then became that the fireball in the sky was the result of a fuel tank mysteriously exploding through a mechanical malfunction of some kind and the plane continuing to climb after it was broken in half by the missile. It was physically impossible.

Nevertheless, the media accepted the cover story, as then-President Clinton coasted to re-election.

In the same way, the Biden team doesn't want a terrorist attack on American soil as he campaigns for another term and wars continue to engulf Europe and the Middle East.

Various chronologies have been offered about what went wrong, in terms of the cargo ship going dark seconds before it crashed into the bridge. But these chronologies ignore the context of the war expanding in the Middle East, as Israel

contemplates military retaliation against Iran.

In my special report on the bridge collapse, I argue that the evidence suggests retaliation by Iran during a war-time situation through cyber warfare.

According to WBAL, a Baltimore television station, the official chronology of the Francis Scott Key bridge collapse shows the cargo ship at 1:25 a.m. on March 26 completely dark without any lights. At around 1:26 a.m., the ship's power appeared to come back on. Around 1:27 a.m., vehicles could be seen going across the bridge span just before the ship crashed into the bridge at 1:28 a.m.

Here is the chronology that really matters:

- In February 2024, the United States conducted a cyber-attack on the MV Behshad, an Iranian merchant ship in the Red Sea. U.S. officials said the operation was "a response" to the January 28 Iranian attack on Tower 22 in Jordan, killing three American soldiers.

This is the result of Biden's undeclared war on Iran that has now been pulled back, in the wake of the Iranian attack on Israel (backed by Russia) and the promise by the Jewish state to retaliate. Biden's people clearly don't want this war to "get out of hand," especially when Russia is backing Iran and a U.S.-Russia military confrontation could be the result.

On the "Just Security" website, two analysts sympathetic to the Biden Administration noted that the U.S. cyber-attack on the Iranian ship in February could have been "a simple jamming operation that interfered with transmission of information" or "another type of cyber operation" which could potentially explain why the Iran-backed Houthis' mistakenly fired a missile on a cargo ship bound for Iran rather than an American vessel.

In other words, these cyber-attacks are so effective that they

can affect the operations of ships and missile guidance systems.

The authors added, “U.S. and Iranian redlines in cyberspace are unclear, and even non-lethal cyber-attacks may have unintended consequences.”

As a veteran observer of corrupt federal agencies in action, such as in the TWA matter, I dispute the notion that the federal government will figure out what happened and tell us the truth. A cover-up is underway, in the same way we saw various federal agencies conclude that a mysterious fuel tank explosion brought down TWA 800 in 1996 in the face of hundreds of witnesses who saw a missile or missiles hit the plane.

These agencies include the FBI, CIA, and the NTSB (National Transportation Safety Board).

It’s significant that on February 21, only five weeks before the bridge collapse, the feds issued a “U.S. Maritime Advisory on Worldwide Foreign Adversarial Technological, Physical, and Cyber Influence,” alerting “maritime stakeholders of potential vulnerabilities to maritime port equipment, networks, operating systems, software, and infrastructure.”

Insurance companies are interesting in finding out what really happened, since they are on the hook for financial damages, with one firm declaring that “one question that is still in the air is whether there was any cyber-attack behind this incident” and declaring the investigation in their view “is still ongoing…”

While the president of the Westwood Insurance Group accepts the “official verdict,” he nonetheless says that “some in the security business” are wondering, “Just how difficult would it be for hackers to create a catastrophe like this?”

He says the answer is “sobering” and quotes security experts as saying that ships are easy to hack, track, send off course

and even sink.

He links to a 2018 article that begins this way: “Modern container ships already face a number of serious perils at sea. Now new research from Pen Test Partners shows just how vulnerable these ships are to new dangers from hacking—including being steered off course and sunk—thanks to their use of always-on satellite communications and general lax security practices on board.”

The article cites Pen Test Partners (PTP), a security services firm, which “demonstrated a number of methods for hacking into the satcom systems of ships, which can allow bad actors access to shipboard systems and wreak potential havoc for the vessels and the shipping industry.”

PTP says it has been providing “cyber security expertise” to a huge variety of industries and businesses since 2010 and is paid to hack and test security systems.

While the author of one PTP article believes it is “incredibly unlikely” that someone could take full remote control of a container ship, it is “entirely viable” that an attacker could impact the vessel’s power management system or Integrated Alarm and Monitoring System, “leading to the vessel blacking out and the associated loss of steering and propulsion.”

This appears to be the case with the Key bridge collapse.

E-Mail Cliff Kincaid: kincaid@comcast.net

- Cliff Kincaid is president of America’s Survival, Inc. usasurvival.org