The next big cyberthreat isn't ransomware. It's killware. And it's just as bad as it sounds.

Josh Meyer, USA TODAY

Tue, October 12, 2021, 6:33 AM

Even as most Americans are still learning about the hacking-for-cash crime of ransomware, the nation’s top homeland security official is worried about an even more dire digital danger: killware, or cyberattacks that can literally end lives.

The Colonial Pipeline ransomware attack in April galvanized the public’s attention because of its consumer-related complications, including long lines at gas stations, Homeland Security Secretary Alejandro Mayorkas said in an interview with USA TODAY's Editorial Board last week.

But, "there was a cyber incident that very fortunately did not succeed," he added. "And that is an attempted hack of a water treatment facility in Florida, and the fact that that attack was not for financial gain but rather purely to do harm.”

That attack on the Oldsmar, Florida, water system in February was intended to distribute contaminated water to residents "and that should have gripped our entire country,” Mayorkas said.

Secretary of Homeland Security Alejandro Mayorkas says his department will move "with tremendous speed and tremendous force."

It's no surprise that it didn't. USA TODAY and others reported on that hack, but it came amid a flurry of reports of other, bigger cyberattacks such as the SolarWinds intrusion of U.S. government agencies, technology firms like Microsoft and cybersecurity companies. .

But Mayorkas and other cybersecurity experts say the Oldsmar intrusion was just one of many indications that malicious hackers increasingly are targeting critical parts of the nation's infrastructure – everything from hospitals and water supplies to banks, police departments and transportation – in ways that could injure or even kill people.

"The attempted hack of this water treatment facility in February 2021 demonstrated the grave risks that malicious cyber activity pose to public health and safety," Mayorkas told USA TODAY in a follow-up exchange. "The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us."

Weaponized technology

Like Mayorkas, private-sector computer security experts recently have begun issuing warnings that so-called cyber-physical security incidents involving a wide range of critical national infrastructure targets could potentially lead to loss of life. Those include oil and gas manufacturing and other elements of the energy sector, as well as water and chemical systems, transportation and aviation and dams.

And with the rise of consumer-based products like smart thermostats and autonomous vehicles, Americans are now living in a "ubiquitous Cyber-Physical Systems world" that has become a potential minefield of threats, said Wam Voster, senior research director at the security firm Gartner Inc.

In a July 21 report, Gartner said it was seeing enough evidence of increasingly debilitating and dangerous attacks that by 2025, "cyber attackers will have

weaponized operational technology environments to successfully harm or kill humans."

It's time to worry about the next big cyber threat: killware.

"The attack on the Oldsmar water treatment facility shows that security attacks on operational technology are not just made up in Hollywood anymore," Voster wrote in an accompanying article.

Another example, Voster wrote, was the Triton malware that was first identified in December 2017 on the operational technology systems of a petrochemical facility. It was designed to disable the safety systems put in place to shut down the plant in case of a hazardous event.

"If the malware had been effective, then loss of life was highly likely," Voster wrote. "It is not unreasonable to assume that this was an intended result. Hence 'malware' has now entered the realm of 'killware.'"

A frightening target: Hospitals

So far, few incidents have come to light in which hackers succeeded in shutting down parts of the nation's critical infrastructure in ways that might have contributed to someone's death or serious injury.

However, U.S. officials are especially concerned about the rash of ransomware attacks on hospitals, which have had to divert patients and cancel or defer critical surgeries, tests and other medical procedures, as was the case in a nationwide cyberattack on Universal Health Services, one of the nation's largest health care providers, in September 2020.

MORE: Hospitals report rise in hacking during COVID

In hospital hacks, patients could die or suffer life-threatening complications but it would be nearly impossible to find out unless medical centers willingly offered that information, said a senior Department of Homeland Security official speaking on the condition of anonymity because he was not authorized to discuss ongoing security concerns.

A year ago, the FBI, DHS and the Department of Health and Human Services issued a warning about such attacks on hospitals, describing the tactics,

techniques, and procedures used by cybercriminals to infect systems with ransomware for financial gain.

“CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers,” the alert said. “CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.”

Authorities believe the problem may be significantly larger than has been reported, in part because private companies and even government agencies often don’t report ransomware hacks of their operational systems. Failure to report such attacks fuels the fast-growing criminal market in ransomware attacks, which can bring hackers millions in payouts, the DHS official said, "and it doesn’t help us learn the latest techniques and tactics used by the hackers."

In Alabama, a woman sued a local hospital earlier this year, alleging that its failure to disclose a cyberattack on its systems resulted in diminished care that caused her baby’s death.

Last year, an apparently misguided hacker attack caused the failure of information technology systems at a major hospital in Germany. That forced a woman who needed urgent admission to be taken to another city for treatment, where she died.

In both cases, the hospitals and doctors involved have denied allegations that they were responsible and no proven link between the hacks and the deaths were made.

Liability for loss of life

Cybersecurity experts have begun warning government and corporate leaders that they could be held financially or even legally liable if breaches of computerized systems they oversee are found to have had a human impact.

“In the U.S., the FBI, NSA and Cybersecurity and Infrastructure Security Agency (CISA) have already increased the frequency and details provided around threats to critical infrastructure-related systems, most of which are owned by private industry,” Katell Thielemann, research vice president at Gartner said in a report in September 2020. “Soon, CEOs won’t be able to plead ignorance or retreat behind insurance policies.”

The firm estimated that the financial impact of cyber-physical security attacks resulting in fatal casualties will reach over $50 billion within a few years.

“Even without taking the actual value of a human life into the equation,” Gartner concluded, “the costs for organizations in terms of compensation, litigation, insurance, regulatory fines and reputation loss will be significant.”

Who are the hackers?

While ransomware attacks continue to dominate the headlines, Mayorkas has quietly begun sounding the alarm about cyber intrusions like the one in Florida in which money wasn’t the primary motive.

U.S. cybersecurity officials have long known that water facilities and other critical infrastructure have been vulnerable for many, many years,” a senior DHS official said. “What made this one different was that there was an intruder who consciously exploited that vulnerability with malicious intent.”

“It is also significant because it is one of the few incidents where malicious cyber activity is crossing the line and can actually threaten the lives of people,” the official said, for instance by increasing the level of potentially toxic chemicals in the water supply. He said Mayorkas has mentioned the attack in meetings with state and local security officials.

Homeland Security officials would not comment on who might have been behind the Florida attack, including whether it was linked to a foreign power.

Several nations, including Iran, Russia and China have penetrated key elements of U.S. critical infrastructure, but there have been few instances of them taking any action.

U.S. officials believe more and more foreign governments and non-state actors are engaging in malicious cyber-activity – sometimes together – in ways that make it nearly impossible to attribute the attacks, or to determine whether they were driven by profit, political motives or both.

In 2015, an Iranian hactivist group claimed responsibility for a cyberattack two years earlier that gave it access to the control system for a dam in the suburbs of New York. In a criminal indictment, the Justice Department later said that seven Iranian hackers penetrated the computer-guided controls of the dam on behalf of that country's military-affiliated Revolutionary Guards Corps as part of a broader cyberattack against 46 of the United States' largest financial institutions.

DHS officials told USA TODAY that the water treatment facility indicated that the malicious actor attempted to change chemical mixtures to unsafe levels as part of the water treatment process. An operator detected the changes and corrected the system before it affected the water supply, those officials said.

"Independent of who was behind it, the fact that someone decided to exploit that vulnerability and was able to do it means that other attackers would be able to do it as well," the DHS official said.

This article originally appeared on USA TODAY: Cybersecurity experts warn of killware attacks that rival ransomware