→ Mark your confusion.
→ Purposefully annotate the article (1-2 mature, thoughtful responses per page to what the author is saying)
→ Write a 250+ word response to the article.

Inside America's Hacking Epidemic

by *The Week* Staff on October 29, 2016

Cyberattackers are waging war on banks, utilities, and companies — and might try to disrupt the U.S. election. Here's everything you need to know:

How frequent are hacks?

In the U.S. alone, government and private targets are pummeled by hundreds of thousands of hacking attempts every hour. Cyberattackers have breached the Pentagon, State Department, and White House; stolen the personal data of an estimated one half of Americans in attacks on banks and tech companies like Yahoo; and provided WikiLeaks with the personal emails of Democratic Party officials, as well as generals and former secretaries of state. These cybercriminals can potentially target every aspect of our lives that involves an internet connection. They could suddenly apply the brakes on smart cars or take over a passenger jet's avionics system. If they finally breached critical infrastructure services like the electric grid — as they attempted to do at least 79 times in 2014 — the results would be nightmarish, says Tony Lawrence, chief executive officer of cybersecurity firm VOR Technology. "Imagine if someone shut down the power to New York's traffic grid during rush hour."

Where do these attacks originate?

Some are carried out by international hacktivist groups like Anonymous, whose members style themselves digital Robin Hoods pursuing justice against the world's powerful. Two hacker groups of this type claimed credit for a major wave of "denial of service" cyberattacks earlier this month that blocked access to such sites as Twitter, Netflix, and Amazon. But most hacks are directed or sponsored by nation states; the two worst culprits are China and Russia. China's mysterious Unit 61398, part of the People's Liberation Army, has reportedly been responsible for at least 141 successful cyberintrusions on 20 major U.S. industrial sectors, including oil and gas pipelines. In Russia, hacking groups called Cozy Bear and Guccifer 2.0 have targeted foreign critics of President Vladimir Putin, and in December shut down part of the electric grid in Ukraine.

How do the hacks work?

About 91 percent begin with a simple phishing attack, in which an email masquerading as a legitimate communication from a well-known company invites the recipient to click on a link or open an attachment. That attachment or link is actually loaded with malware. If just one of the hundreds of people in a company or government agency targeted by this attack falls for the trick, his or her computer downloads that malware — giving the hacker a back door into the organization's entire network. Many hacks involve spear-phishing: a more personalized email, designed to look like a message from a friend or colleague. Another phishing technique is to encourage recipients to enter their account details into an official-looking form from a web company or a government agency.

How much damage can hacks do?

They can wreak absolute havoc — economically, politically, and physically. The North Korea–directed attack on Sony Pictures Entertainment unleashed a stream of embarrassing company memos, destroyed its computers, and caused Sony an estimated $100 million in damages. A "cyberphysical" attack on the electric grid wouldn't just cut off electricity for tens of

millions of Americans; it could also shut down the water supply, cellphone towers, trains, airport landing lights — the list is endless. That's the kind of damage terrorist groups like ISIS dream of inflicting. "These savages have so far only figured out how to use the internet to proselytize," says FBI Director James Comey. "What happens when they figure out how to use it to break into a chemical plant, or a blood bank?"

How can the U.S. respond?

The government has hired hundreds of cyberdetectives to monitor federal agencies for breaches, and more than 6,000 hackers have been recruited to U.S. Cyber Command — a military unit responsible for both combating and waging hack attacks. One such alleged U.S. offensive, the "Stuxnet" computer worm, silently destroyed 984 of Iran's nuclear centrifuges in 2010. Russia could be the next target. Vice President Joe Biden recently warned that the Obama administration is preparing to "send a message" to Putin for his country's alleged role in the hacks on the Democratic National Committee; some speculate the U.S. could, for example, hack into proof that Putin and his oligarch cronies have stashed billions in foreign bank accounts. One major risk of tit-for-tat hacking, however, is that it can escalate into all-out cyberwar.

What would cyberwar look like?

It would be silent but enormously destructive. The two sides could block access to the Global Positioning System, disrupt air traffic control and electric grids, and block access to the internet or fill popular websites with propaganda — causing widespread chaos and fear. Cyberwar is the only field of warfare in which the U.S. doesn't have a clear advantage over its foes, warned then–Joint Chiefs Chairman Martin Dempsey before he retired last year. "It's a level playing field," said Dempsey, "and that makes this chairman very uncomfortable."

Hacking the election

Russian-connected hackers have already played a big role in the 2016 presidential race, targeting Democratic nominee Hillary Clinton and her party with email hacks published via WikiLeaks. Cybercriminals could, in theory, take that interference to the next level by undermining the election process itself. While the country's electronic voting machines aren't connected to the internet, there are plenty of other weak spots for hackers to exploit on Nov. 8. They could target the computers that election officials use to prepare ballots or aggregate poll results, or hack official government websites to insert claims that polling locations have changed or closed early. In California, unknown hackers accessed the personal data of tens of thousands of voters via registration websites. In many cases, they were able to change voters' race, birth date, and address, or remove them from the poll books entirely. That interference was detected and reversed, but hackers have also been detected probing registration sites in 18 other states. Hackers probably could not change the results on Election Day — but they could cause confusion and undermine confidence in the democratic process. Hackers could do "just enough to create scandal," says Chris Porter, who runs strategic intelligence for the cybersecurity firm FireEye Horizons. "That's sufficient for Russian aims."

Possible response options:

- Do you think we will see a full-fledged cyber war in our lifetime? Explain.
- What about this article confuses you? Do additional research and write about what you learn.
- Choose one passage and respond to it.