1. Mark your confusion.
2. Show evidence of a close reading.
3. Write a 1+ page reflection.

The Risks of Cyberwar

The Ukraine war magnifies the chances of an attack on the West's electronic infrastructure.
Source: *The Week*, March 25, 2022

How big a threat is state-sponsored hacking?

Hacking that is supported—often secretly—by another government comes in a variety of forms, and not all of the effects are immediately visible. In the past, Russian hackers have stolen emails and targeted voter databases in efforts to influence U.S. elections, and North Korea stole a massive amount of data from Sony in retaliation for a comedy about a fictional plot to kill Kim Jong Un. But exactly how far state-sponsored attacks might reach is not clear. Last year, hackers who appeared to be linked to a state-sponsored group found vulnerabilities in Microsoft's Exchange software that may have let them download emails from thousands of companies; we still don't know what could be done with that data.

Could hacking attacks turn into cyberwar?

One intriguing question about the Ukraine war is why it has not been accompanied by a broader campaign of electronic warfare. While Russian hackers have attacked Ukraine's electrical grid before—notably in 2015—Ukraine's electrical and communications have remained up. The United States and other Western countries, too, have not been directly victimized by the expected Russian offensive. "I am still relatively amazed that they have not really launched the level of maliciousness that their cyber arsenal includes," Senate Intelligence Committee chair Mark Warner (D-Va.) said this week, not long after warning of coming Russian attacks.

How well protected is the U.S.?

In recent years, the U.S. has spent billions of dollars on both the government and the private sector shoring up its cyber defenses. That may have discouraged other countries from direct attacks; Russia has in general tended to favor a strategy of promoting disinformation over attacks on the infrastructure. Another level of protection from sustained electronic warfare may come from the fact that, much like nuclear war—though obviously on a less catastrophic level—cyberwar is a case of "mutually-assured destruction." A country that attacks another in overt fashion can expect a major attack in return. Indeed, last month, President Biden specifically warned that the U.S. will respond "if Russia pursues cyberattacks against our companies or our critical infrastructure."

What are the targets?

In a technologically advanced society, just about anything is fair game for hackers. Stock Exchanges would freeze if payment processors went offline. Wiper malware could delete important data held on government servers. The biggest, most concerning target would be physical infrastructure—everything from water and sewage systems to transportation networks. An attack on electric utilities could cause millions to lose power. Last May, the Colonial Pipeline, the largest fuel pipeline in the U.S., was taken out of commission by hackers, leading to fuel shortages and high gas prices in much of the Southeast.

What about the financial system?

Cybercrime has been a major problem for the financial sector for years, and it will only grow as the industry becomes increasingly digitized. Some Wall Street firms spend up to a billion dollars every year on cyberdefense; it hasn't always worked. The FBI estimates that cybercriminals seized $4.2 billion in 2020 alone. It's possible that a much more targeted and sustained attack could come in response to the international community's recent sanctions against Russia. In such a case, hackers might not be interested so much in stealing client information as in attacking banks' payments systems. Denial-of-service attacks involving millions of simultaneous connections, for example, could bring down websites and internal servers. Disruptions of ATMs and credit card transactions would interrupt daily life and cause billions of dollars in bank losses. The good news is that in recent weeks, banks around the world—many of which have already prepared with ransomware drills—have reportedly increased their monitoring of networks, prepping for a cyberwar scenario.

What should ordinary people do for protection?

There are a variety of basic precautions you can take—if you haven't already—to protect your information online. Some of this is familiar: For instance, you should use stronger passwords and enroll in two-factor authentication, now an option on many major websites and platforms. Make sure that your personal data is backed up not only to "the cloud" but also to hard drives, which don't have the same vulnerabilities. But consider some real-world precautions as well. What might you need if, say, your access to the internet was disrupted for an extended period, or if the power grid went down? Basic readiness measures include keeping extra cash on hand and storing extra food, water, and other essential supplies. In fact, some of the same measures many Americans recently took during the initial shutdowns of the Covid-19 pandemic could come in handy here.

Possible Response Questions

- What are your thoughts about a possible cyberwar? Explain.
- Did something in the article surprise you? Discuss.
- Pick a word/line/passage from the article and respond to it.
- Discuss a "move" made by the writer in this piece that you think is good/interesting. Explain.