**Reflective Writing**

When I first signed up for this cybersecurity ethics class, I didn’t expect it to make me rethink so much. I figured we’d just go over a few rules, maybe talk about data breaches or legal stuff, and that’d be it. But as the weeks went on, the class pushed me to think way deeper about people, choices, power, and responsibility in tech. There were a few topics that really stuck with me and changed how I think, not just about cybersecurity, but about what kind of person I want to be in this field.

One of the biggest ones was whistleblowing. I used to think whistleblowers were kind of disloyal. Like yeah, maybe they were trying to do the right thing, but wasn’t there a better way than leaking information? But then we read Vandekerckhove and Commers, and that made me slow down and look at it differently. They talk about the idea of rational loyalty that sometimes being loyal actually means speaking up when something’s wrong, not just staying quiet and following orders. That really made sense to me. If a company or government is doing something harmful, and no one’s listening internally, what else is a person supposed to do? I hadn’t thought about how hard that decision must be, or how much risk is involved. Now I see whistleblowers less like traitors and more like people stuck in impossible situations who are trying to act on their values.

Another topic that changed the way I think was cyberconflict. I never really considered cyberattacks as something that could be part of war. I thought of war as soldiers, tanks, bombs stuff you can see. Cyber stuff just felt like hacking or stealing info, not anything with real world consequences. But Michael Boylan’s piece on just war theory and cyberattacks hit me hard. He showed how digital attacks can take out hospitals, shut down power, or even kill people indirectly. That opened my eyes. Cyberwar isn’t some sci-fi idea or just political drama it’s already happening, and it can hurt people in very real ways. The fact that there aren’t many clear ethical rules for cyberwar makes it even scarier. Boylan made me realize we need to take digital warfare just as seriously as physical warfare. And that made me think more carefully about how I’d act if I ever work in a job that’s even remotely connected to offensive cyber stuff.

Then there’s privacy, which was honestly the biggest shift for me. I used to have the “I’ve got nothing to hide” mindset. I figured if people cared about privacy, they just shouldn’t post so much or use sketchy apps. But James Grimmelmann’s article changed that. He compared privacy to product safety, which honestly blew my mind. Like, we expect cars to come with working brakes and toasters not to start fires why shouldn’t we expect websites and apps to protect our data in the same way? The more I thought about it, the more I realized how unfair it is to blame users when systems are designed to trick them into giving up their info. The burden shouldn’t be on the person using the tech it should be on the people building it. Grimmelmann made me see that privacy isn’t about hiding bad stuff. It’s about protecting your freedom, your dignity, and your safety. Especially when some people activists, minorities, victims can face serious consequences when their data is exposed.

All of these topics really made me think more about what kind of cybersecurity professional I want to be. I don’t want to be someone who just does what I’m told, or who only cares about what’s legal or what’s profitable. I want to be the kind of person who asks questions, who speaks up when something’s wrong, who puts people first. This field isn’t just about locking down systems or writing secure code. It’s about protecting real people in a digital world that’s full of risk, power, and sometimes injustice.

If there’s one big takeaway I want my future self to remember, is ethics isn’t extra it’s essential. The choices we make in cybersecurity, even if they seem small, can affect people’s lives in huge ways. So whenever I’m not sure what to do, I want to slow down, think about who’s being helped or hurt, and make decisions that I can live with not just as a tech worker, but as a human being.