Ukraine Power Grid Hack

Part 1: Role play

IT WAS 3:30 p.m. last December 23, 2015, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

He watched as it navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline. A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm. Somewhere in a region outside the city he knew that thousands of residents had just lost their lights and heaters.

The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive. Then as the cursor moved in the direction of another breaker, the machine suddenly logged him out of the control panel. Although he tried frantically to log back in, the attackers had changed his password preventing him from gaining re-entry. All he could do was stare helplessly at his screen while the ghosts in the machine clicked open one breaker after another, eventually taking about 30 substations offline. The attackers didn't stop there, however. They also struck two other power distribution centers at the same time, nearly doubling the number of substations taken offline and leaving more than 230,000 residents in the dark. And as if that weren't enough, they also disabled backup power supplies to two of the three distribution centers, leaving operators themselves stumbling in the dark.
(from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/)

Read the above article. Imagine that you are the worker who first noticed the attack occurring.

1. You notice that multiple substations are being shut down. Can you think of anything to do?
2. How would you feel if you were the person that first observed this?
3. That you can think of, are there things that could've helped this attack be recognized automatically so that the interaction between the interface and the substation could be shut down?

Discussion questions:

1. Was an attack like this easily preventable?
2. Imagine you are an outside country looking in... What are the implications of an attack like this?
3. Image it turns out that Russia *was* behind the attack. How should other countries respond if at all?

Role play activity: Russia was the suspect of this attack. What should Ukraine do? Imagine that this was your country's power grid that was compromised. What would you do? Take one of the following roles:

1. The technical analyst that reports the issue
2. The ethics, law, and policy analyst that advises an official
3. The secretary of defense

Prepare questions and answers related to the topic. Present this as a role play in class.

Part 2: Research – This is homework. Write at least 300 words for each answer. Submit a report with proper citations (IEEE style).

Read the following article: http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html
Answer the following questions:

1. Are there any relevant international laws? Research the international laws on Cyber Attacks and see what you can find. If not, what type of options does a country have to react to this type of attack?
2. How would you write the rules and laws for cyber warfare if you were a law maker?
3. What are the national laws to declare war? What are the international laws to declare war?
4. If a country can prove that a cyber-attack happened from an opponent country, can it declare war to this country? What kind of actions should the country take into consideration in that situation? What kind of scenarios would justify a war?
5. The article mentioned international surveillance. Should countries treat incidents of international surveillance differently that those of cyber attacks?
6. In 2009, the United States Cyber Command (USCYBERCOM) was established with the goal of defending the country from cyber attacks. However, in recent years, the majority of the resources have been spent on launching attacks, such as the one described in this article. Should the USCYBERCOM be focused on one over the other?