There were a fair number of factors that led to the Estonia cyber incident. Starting with the technical concerns, due to the low population of the country and limited resources, Estonia decided to move to a paperless banking system. The processes started in the 1990’s and by the time of the attacks in 2007, 95% of the banking in the country was done online.1 Along with banking, more than 450 of the public sector organizations used the data exchange portal ‘esti.ee’ every day. This type of dependance on the internet for basic government services left an opportunity for attackers to try and exploit. What started as simple instructions on Russian internet forums to perform ping commands from Windows terminal, later turned to coordinated botnets that used more than 85,000 hijacked computers to deny service to the Estonian data exchange.

The human factors that led to the Estonian cyber incident was the abrupt removal of a World War 2 statue from the town square of Tallinn. It served as a memorial to the victory over the Nazi army, and when in April of 2007 Estonia announced they would be removing all war monuments, over 1,000 people protested at the statue's location. What started out peaceful turned into violent riots and caused the city over $4.5 million dollars in damage.2 This outcome led the Estonian government to make the decision to remove the statue abruptly during the night of April 27th, when no one was expected it. The decision only made matters worse as the riots in the streets then turned to riots in cyber space, where for the next 3 weeks the Estonian public service sectors would be severely affected by distributed denial of service attacks.

The business decisions that led to this were those that led to the overwhelming dependance on the internet for basic government services. While we cannot blame them for trying to provide the best for their citizens for the least amount of money, we can criticize them for not having had the proper infrastructure in place to deal with this type of attack. It is unacceptable to run most of your country's public works online while never anticipating cyber-attacks in the future. Any investment in security infrastructure preattack would have saved them more than what it cost on the backside of the attack.

I believe the most significant factor at play here was the human factors. To cause a problem at this scale there had to be a catalyst to unite a group of people to carry out the initial cyber riot, and removing the statue was the spark to that flame. The Estonian government should have learned their lesson from the set of physical riots that cost them $4.5 million in damages and left the statue in place. To not think there would be repercussions by trying to remove the statue in secret is absurd. The human factor of the government underestimating its population's technical capability is not to be overlooked here either. This is a significant case study because it shows for the first time that riots in physical space can transfer to the digital space as well.