In his article “The New Front Line: Estonia under Cyberassault,” Michael Lesk takes a look into the new arena for warfare – cyberwarfare. He initially presents a situation in April 2007 where Russians protested in Estonia over a removed memorial statue, eventually leading to a violent protest and a series of DDoS attacks against Estonian computers.

Lesk describes how although Estonia is a small nation, they are modern and “Web-dependent country,” citing from sources that 80% of citizens use online banking and remote medical monitoring. When the DDoS attacks occurred and started infecting Estonian machines through the Estonian minister’s web site, they found that it traced back to a Moscow IP address owned by the Russian government. However, outside sources did not find sufficient evidence to find the Russian government guilt; the amount of data in the amount of time allotted could have been achieved by a multitude of corporations, and since Estonia is a small country, Lesk states that “its systems aren’t configured for that kind of load,” resulting in a successful attack.

Lesk goes on to explain that botnet attacks are not a new attack strategy, and that corporations have actually hired hackers to cause competition’s systems to fail. According to estimates and his own conclusions, Lesk estimates that the botnet attacks cost sums to a mere $100,000, which could be easily afforded by other organizations than the Russian government. Estonia successfully countered the attack by shutting down Internet connections to other countries, leaving people within the country still able to complete day-to-day tasks, but Lesk questions where we go from here, what steps should be taken to defend against future attacks.

The US government surely has the funding to invest in our nations cybersecurity, but in 2007 it was not doing so. In addition, Lesk believes that cooperating with foreign governments is essential to creating global cybersecurity defense measures. The US government also successfully “identified and indicted several major botnet operators,” demonstrating the government’s dedication to closing down botnets. Other than widespread defense, individual education is also imperative. Having security measures on personal machines with have anti-zombie software could also help reduce/prevent future DDoS attacks.

Since 2007, cyberwarfare has continued to an extreme (and unethical) extent. The US and other governments collect immense amounts of data on users, including visual data via device cameras, with the intent of “security” from terrorism or cyber threats, but is too great of an invasion of privacy to continue.