**# Why Cyber Warfare is Worse Than Conventional Warfare**

*Lancaster University reported in 2010 that for the first time in maritime history, cyber attacks are low-cost alternatives to physical attacks. It’s scary when knowing that cyber attacks also can harm nations and people a lot more than conventional attacks.*

What if another nation gains access to our Water Systems? What if a terror organization gains access to our Energy Systems? What if a hacker group gains access to our Bank Systems? What if they tomorrow shut down parts of our life depending infrastructure? The consequeces could be divastating. Epedemics will spread, anachy will break out and our economy will collapse. Thousands of people will loose their life.

Some years ago in 2013 the New York Times website got hacked and was shut down for about 20 hours. It’s believed that the attack was backed by Syrian president Bashar al-Assad. In 2014 Russian hackers gained access to White House and State Department emails. The government said it believes that the hack originated in China. In 2010, a virus called Stuxnet destroyed a fifth of Iran’s nuclear centrifuges by causing them to spin out of control. USA and Israel unleashed Stuxnet by attacking key vendors. These three events of cyber attacks didn’t cost lives—at least it’s not mentioned anywhere—but it’s believed that future cyber attacks will get worse.

**At first it might look like developers can’t do much. I mean, how can we possible protect a whole nation from collapse? No, that’s not possible. In the matter of fact it is possible—at least we can contribute to our safety. What we can do is to protect our systems and applications as good as we can. We shouldn’t welcome hackers through „open doors„. If you’re running a web application no matter if it’s an internal or external facing application, you may protect it from sql injection, cross side request forgery or other doors you could have closed otherwise. OWASP provides a list of the 10 most critical web application security risks that we can easiely follow. Make security part of your software developement lifecycle. Integrate security testing in your Continuous Delivery Pipeline and you have contributed a lot to our all security.**

**## Conclusion**Conventional warfare kills people, innocent people, and so can cyber warfare. The difference? Cyber warfare can and maybe will one day cause the death of many many people in very short time. As developers we got the power to protect our society from evel cyber attacks. What we have to do and what we can do is to make our applications secure as best as we can. Application Security should be a natural part of the Application Developement Lifesycle.

Sven Malvik