The Law and Ethics in Cyberwarfare

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

The Law and Ethics in Cyberwarfare

To me, law and ethics in cyberwarfare and how cyber warfare law can be enforced are extremely important. There is no clear evidence in the cyber war that one state attacked another. People can simply refuse their actions because everything can be targeted from anywhere in the world. The targets can be nuclear plans, transportation systems, utility systems… and create huge damage to the target’s population. International cyber law can’t be approached unify because each state has much different technology and infrastructure (some state is very advanced; some are not so much). However, there is the principle that all the state agrees to respect the sovereignty, jurisdiction, and personal control. Therefore, the Tallinn Manual is prepared to point out state responsibility, but the question is how to accurately identify the real attackers. We all know there are so many ways to hide the real source of an attack. For example, one group in Russia can hack into China’s system to use them as bots to attack the US. So, who will be responsible for the attack: the China system if we don’t figure it out (the IP address of the attacker is in China right?). Another concern is that it usually takes too long to gather evidence on sophisticated attacks. In the end, the ability to accurately point out who is the responsible party and how to enforce them is the most important question that we need to figure out.