Information Security Assignment

Erika Hernandez

NET 3730 and Cyber Policy and Ethics

Matt Paulson

October 6, 2021

Information Security Assignment

In this paper I’m going to answer the following questions. Is it morally permissible for a country like the United States or Israel to use a worm like Stuxnet to disrupt Iran’s development of nuclear weapons?

Where do you stand on the controversial encryption issue? Should governments like the United States be allowed to have an escrowed key to all encrypted communications? Is unfettered encryption a good thing for cyberspace?

Question 1

Yes, absolutely. I think it would be super important and the good of not only the country but the world. Time has shown us that Iran and Iraq aren’t the most trusting countries. They have lots of radical people in their country that no one can control. When a country like that has something like nuclear weapons at its disposal. That is almost like giving a gun to a toddler hoping that he won't shoot anyone.

I would imagine that the FBI or the CIA is already monitoring Iran. But to go as far as to put a worm or even spy on them. Yes, I think that would be appropriate. They can not be trusted and after 9/11 it has shown they have no mercy on the United States. I mean they spy on their people and they execute their kind. So they have no problem killing themselves in the process of getting back to Americans.

The fact that we all have the freedom to do what we want and have freedom of speech. We need to realize that not all countries have that luxury. That to get their message across they result in violence and killings. Which if they want to do that in their own countries so be it. But when they start to trickle down to other countries and impose their radical ideas and their messages, through violence. That is where I have a problem and I push the moral card aside and see that it's now a threat and protection of our citizens.

Question 2

This is a hard one for me, I had to think about this. I feel that when it comes to a persons secure information they should not have access to all personal data. But then when you think about it, the government knows your social security number. They know your drivers license number because they issued it. They know where you live because the mail is owned by the government. So what other information does the government not know? Well you cell phone they don't have access to your private pictures, they cant hear your phone calls.

So is that what they should or shouldn't have access too? Yes I think those things shouldn't be in the governments hands or have access to it. But with our phones and social media is that something they should have access too? I mean in some cases that public information. I watch a lot of true crime shows. So when they want the DNA of a person of interest they would need a court order to get it. Not all cases do they have the right to do that. Next's best thing they follow the person and wait until they throw garbage away.

When the person does throw garbage away they are then able to pick it up and test for it. This is legal and holds up in court, so going back to encryption. Yes some things should be encrypted and some things shouldn’t be. If they didn't allow to keep our private information away from the government. Then they would have access to everything and nothing would be ours to keep.

Conclusion

We want to be able to spy on countries we don't trust. Yet when it comes to having the government spy on ourselves we throw an evasion of privacy. I'm going to say what I say to employees at work. Don't do things you wouldn’t want your employer know you are doing. If you are doing things that you don't mind your boss knowing. Then you have nothing to worry about. But if you don't what your job to know things don't send, look or click while at work. Keep that stuff at home and you will be fine.