**Course Name: Cyber Security and Privacy**
**Professor Name: Prof Saji K Mathew**
**Department Name: Department of Management Studies**
**Institute Name: Indian Institute Of Technology Madras, Chennai**
**Week: 08**
**Lecture: 24**

Hi everyone, Good morning. So, we the members of group 5, myself Mano and Bhuvan Dubey, we are here to present and discuss about the topic, about the article, 'Active Defence and Hacking Back'. by Scott Benito. He opens up with an article with a tagline where if we don't want, if you want to stop the bad guys from internet, we should need to fight them back. This is a tagline of this article where he starts with, and in this article, he interviews the primer, two primers, one is Dorothy and other person, Robert M. Lee, where he takes their perspective about active defence and hacking back strategies and explains why whether we need to go with active defence or not, with this justifications.

So, with the introduction from Dorothy, Dorothy Denning is a professor from Naval Postgraduate. He is a professor of Naval Postgraduate and also a fellow membership from the computer missionary and he was co-authored many articles and books and specifically one topic he discussed about active defence is that, when properly understood active defence is neither offensive or necessarily dangerous, where we describe about active defence. Second to move on with the next person, that is Robert M. Lee, he was the co-founder of an IT security firm Dragos, where the company works with US government on many particular project.

In specific to mention about the company Dragos, the security firm into October 2017 identified a malware which was specifically targeted to work on the industrial system, which may destroy or damage the industrial system products, which may cause damage to the people. Later in August, this malware was identified foot forth and then attacked with the Saudi Arabia country, but the attack however has been failed. So, this was a quick introduction from both the primers. So, from Sun Tzu, he says that security against defence implies defensive tactics; ability to defeat the enemy means taking the offensive. And also one of the other famous quote that Mao Zedong says the only real defence is active defence.

So, why active defence? To protect the most valuable information, something more than deployment of security software and network monitoring processes is required. Second, even high amount of spending on technology defences can secure the critical systems and help keep pace with the hackers. The main point of active defence, active defence in a sense, it comes after the attack or intrusion happens. Once an attack is happen or intrusion

is detected, what kind of an active defence mechanism a company and organisation takes in order to rectify it or else in order to fight back for the intrusion. Yes, a direct defensive action taken to destroy, nullify or reduce the effectiveness of a cyber threat against the asset.

This is the quote by Dorothy Denning. With an example mentioned in an article where Dorothy Denning explains an event, a hackers event happened for the Georgian government, where in Russian hacker tries to take sensitive information from Georgian government through the malicious code in one of their Georgian government systems. where he uses a malware, gets into the system and try to use the keyword USA and NATO to search for the documents. This incidence was identified by the Georgian government. In order to, instead of stopping the attack, they wanted to identify the attacker in the same way he was able to attack the, he was able to intrude into their system.

So, the Georgian government instead of stopping the attack or isolating the system, they prepared a spyware and install and inserted into the systems with the keyword NATO Georgian with wth the keyword, NATO Georgian document. So, since the you have hacker was searching with the keyword USA and NATO this documents spyware, which the document is consisted as spyware were identified by the hacker and it has been taken back to the control system of the hacker where the spyware on downloaded into the control system, opened up the camera, webcam of the hacker, take a snapshot of the hacker and send back to the Georgian government. This example, Dorothy Denning specifically mentions that the activity the Georgian government took, maybe some people may say it is an illegal activity because instead of isolating or protecting their government, they specifically created one more malware, is basically a spyware to identify, but in the perspective of Georgian government, it under their legal constraint, they wanted to identify the hacker and also to know what are the data's which the hacker has taken back and also they want to legally take action against the hacker. So, this was the active defense tactic which the Georgian government has taken back and with this the other examples are the monitor of intuition and if detected, response by blocking further network connections from the source or identify a shutdown, a botnet used to connect a DOS attempt. If need to be shut down we can or else we can also go with the active defense tactic which is followed by a Georgian government.

With this should hacking back be accounted, this is a question for to be discussed. So, in order to protect ourselves, we should also hack back if an organization is going to attack, from an intrusion or any bad actor. So, do you have any inputs on it ? Should hacking be accounted? An organization tries to, whether they should try to protect their system or else they should try to hack back the attacker, in order to get more details about the attack and also to get back the data. You mean to say it is kind of counter attacks

strategy but then it should be identified that who is actually hacking us. Yes, it is also a counter strike attack where it has two perspective, either you the organization tries to attack a hacker to identify and also take a legal action attack it seems.

More important is get back the data whichever is stolen in, in cases. With this in expert opinion why we do an active defense, that is hacking back? This is to gather intelligence about the source of intrusion. When an intrusion error did happens, we should gather more in some to help us to gather more intelligence sources from the intrusion and determine what data is stolen. When an attack happens we may think this, what is the specific sensitive information taken ? But the attacker may have also taken other information which we may not insights to. Then identify the attacker for law enforcement, to bring charges.

This is the important point where the company wants to identify the attacker and bring in force for the law enforcement support. We also have a con support where, why not do it? Again this could be illegal. If an attack, if an bad actor tries to attack an organization, if the organization tries to attack back an individual person, that is again comes as an illegal activity which is hacking. And the second is, no evidence that attacking, the attacker works. Some it is again we have to try the multiple ways to identify the vulnerabilities, to attack the, to find the ways to reach the attacker but sometimes it may not also work.

Next could compromise government operations. This may involve with the organization how sensitive data they are dealing with? The expert advice is hacking back without legal authentication is unethical. Targets are too evasive and networks are too complex, transversing in a system. So this is what the opinion on active defense.

Next. Thank you Manu. So we have seen why active defense is needed. Companies have been trying many different strategies. Spending has been going up but it is very tough to keep pace with hackers and what it is, we have seen the active defense which there are different strategies. We will look at some more details but often hacking back is confused with it.

We saw that hacking back is probably classified as something unethical, while active defense is something which is actively pursued by various organizations but often lines get blurred and the example which Manu gave about the Russian hacker, hacking the Georgian government systems and Georgian government using a sort of a deception to get more information on the hacker. Now do you think was that ethical or was it something which should not be pursued or not? Open for discussion. In such situation, in such situations actually the government tried to protect its people. So it is not about being

ethical or not. It is about securing your systems and infrastructure, mitigating the damage.

So I guess, it will be ethical to do it, to prevent further attacks from the intrusions. That's a good point. Any other inputs? Even in case of, you know legal terms at times there's something called as self-defense. At times in case of self-defense, you have to attack the other person and that is justified. Anyone else would like to give input? Also in this case, like we can see that it was due to the hacker's presence of inserting malware into the Georgian system.

So due to his attack, he got the malware like the government didn't exclusively try to hack back into the attacker system, but instead placed within one of their systems. So it got uploaded in the hacker system. So it was within their jurisdiction of, you know government's operations in securing the systems. They did not exclusively transfers to, transfers to the attacker's systems. So it was ethical from a opinion.

So I think most of the points are covered, that why it can be considered ethical. The Georgian government is taking an action for its national security. It did not go out of its network or out of its system to install anything. It was the hacker's own code that led to sharing of information about the hacker. But at the same time, there have been experts who have raised counterpoints, that the assumption is that the spyware will go back to the hacker system but the hacker may be using a lot of intermediate system from innocent people, where the spyware may get installed or worse, that attacker could be using a network computer which would then end up impacting a lot of other computers in that network - could be university, could be hospital, could be energy facility etc.

So we can see that, you know there are arguments on both sides. Now in this case it was a government taking an action. So probably it will tilt towards ethical in the interest of national security but a similar action by an organization will probably be in the grey area, right. So what, now the question is what is ethical active defense strategy and if you draw parallel from combat in the field, monitoring from the size that are coming in, is passive monitoring, but shooting them down, once it is inside your own airspace, that is active defense and there are some examples we have seen earlier, some more like thwarting a DDoS attack and creating a log, sharing of information, cooperating with law and law enforcement agencies. These are all different grades of active defense strategies and, and in fact the US homeland security show, calls it a gray zone.

On one end there is passive strategy of installing antivirus of building firewalls and on the other end there is an offensive cyber, right outright attacking the hacker and in between there are a range of options starting just from information sharing to intelligence gathering from the dark web or even going up to having a ransomware of your own, white hat

ransomware going on rescue missions. So you can see increasingly if you go towards the right it becomes greyer, risks are higher but also impact is higher. So how as managers, can we take ethical considerations while planning active defense for an organization? The writer of this article has published another paper which looks at some considerations for ethical and legal principles for cyber defense. Looking at authority that the organization should have authority to take whatever action, usually within the internal system, It is fine but once the strategy involves going outside, it would require authority from the government or the courts or the law enforcement agencies. Similarly third party immunity, there should not be any intentional harm to the third parties.

It should be deployed only to mitigate the threat. For example, if you are accessing a computer to shut down a botnet, it should not harm any other files or it should not, disabling a computer would not be needed, essentially. Another point is proportionality, that the cost that will be incurred should be proportional to the benefits that are expected out of certain actions. Something we saw into this class as well and human involvement is something which the writer highlights because ultimately even the automated defenses, they will have to be settings or thresholds to be defined by the human. Accountability will be to someone in the organization and hence even for automated system, some degree of human involvement should be there and last point, civil liberties, the right to privacy and free speech, even for a hacker should not be breached upon.

For example, personal information should not be shared. So these are inputs from the.