As private sectors of the united states

As technology advances, each waking day increases the connectivity of the world. The global technological advances have increased the world's connectivity and in the process have improved peoples living standards. Even though technology has improved the global economy, all the benefits, however, have a price to pay. The advancements made in technology have made many nations vulnerable to cyber-attacks, and the United States is not exceptional as it is also vulnerable like any other nation (Shackelford and Bohm 61). The new era in technology has brought with it a new threat to the world as an individual with the right technical skills, and one who has access to a computer with a network connection could destroy a nation just by the stroke of a few dials on a keyboard.

The public and the private sectors of the United States all rely on highly sensitive interdependent systems that lack resiliency. The more significant problem is that the current approach of the United States to cyber-attacks favors the civil liberties of the American Citizens disregarding the concerns for national security. The nations operations run under the misguided front that a cyber-attack falls under the category of criminal activity and that cyber-attacks are not a major threat to national security. Working under this presumption, law enforcement investigative approach to a cyber-attack follows the same rules as any other criminal matter; a path that could take days, weeks, or even months to solve the case which could be too late to prevent the catastrophic effects of a cyber-attack (Thomson and Van Niekerk 40).

The presumption that cyber-attacks do not pose significant threats to national security and that they are categorized as any other criminal activity

is the reason why I believe the United States is not adequately equipped to defend its cyber environment. AnalysisThe fact that computers can be purchased at low costs and are readily available makes cyber-attacks an attractive cheap way of attacking a nation, business or an individual. In the past warring nation used traditional military weapons to attack each other, the new era in technology empowers a country or individual to use tools as simples as a personal computer to achieve a military objective. The United States government cyberspace protection program is mainly focused on the nation’s critical infrastructure. Computer systems and network connections are the foundation of the nations’ critical infrastructure. The United States cyber environment is composed of three segments, which is the military, the private sector, and the civilians’ networks. However, the private sector is not equipped to defend its computer systems from major terrorist or criminal threats (Van Hoboken et al.

7). The civilian networks are also at risk as they are more vulnerable to cyber-attacks. The military networks are mostly secured although they are somehow vulnerable as they are dependent on civilian networks to connect and transfer information. Creation of a strong, safe and secure cyber environment is essential as it ensures a resilient critical infrastructure a factor that is critical for the nation’s well-being. The government is mandated with the task of protecting networks and computer systems that support critical infrastructure found in the United States (Van Hoboken et al.

9). The critical infrastructure is defined under the USA PATRIOT Act of 2001 as the physical and virtual systems and assets that are very important to the United States, to the extent that their incapacitation or destruction has a

great impact on security, the economy and the nation’s public health (Van Hoboken, et al. 1).

The defensive military operations against cyber-attacks consist of the active measures and the passive defensive measures. The nation’s network defense system protects the country from both domestic and international cyber threats. The passive defense measures include embedded encryptions, computer firewalls, and automated interference detection systems. On the other hand, the active measures include a defensive process that could involve the use of an offensive malware which is used against the perpetrator of the cyber-attack.

The central argument of this paper is to show how eliminating the notion that cyber-attacks are simple criminal acts will ensure that there is a timely response to a cyber-attack that targets the critical infrastructure. The presumption should be that any cyber-attack affecting the critical infrastructure of the nation is a national security matter and not a simple criminal activity issue. This should be the presumption until the cyber threat is neutralized by the federal authorities and determination is made on the nature of the cyber threat. It is such a belief that creates the way for the required reaction that aims at preventing the critical infrastructure from facing threats. The cyber environment is under the jurisdiction of the Department of Defense because cyber threats are categorized as potential threats to the national security (Thomson and Van Niekerk 42). The process of protecting the cyber environment involves the attribution and the characterization of the cyber-attack.

There are reasons as to why a nation should accredit and allocate the source of a cyber-attack before taking actions. First of all, attribution ensures that the wrong nation or person is not targeted for perpetrating a cyber-attack. The other reason is that there are laws that govern the response type allowed by the law which varies depending on the source of the attack which could be a state actor or a non-state actor. If the source of the attack is a state actor, it could be from state employees, such as military personnel and hired independent contractors. On the other hand, a person who is not acting on behalf of the nation is someone acting based on their reasons, or one could be a member of a terrorist organization. In case the attacker is acting on behalf of a certain nation, then the nation’s response should comply with the United Nations regulations and other customary international laws. If the culprit of the cyber-attack is acting on an individual basis, then it is the role of the domestic criminal law to govern the response. It is also a requirement of the international law that a nation should characterize a cyber-attack to avoid retaliating against a body that unintentionally launched the cyber-attack.

The United States may be able to act on hostile attack under its laws when it happened within the American soil, but international law does not allow the use of force in the case of an unintentional cyber-attack (Hansen and Nissenbaum, 1162). It is crucial that international law adjusts and protects nations that initiate a warranted response to a cyber-attack as a cyber-self-defense technique without going through the lengthy process attributing the attack. This is because in some cases, state survival is solely dependent on an immediate and aggressive response by the government. This is the

reason why by international law a nation should aim at meeting the traditional requirements when defending the critical infrastructure. The international laws should be on preferable terms such as when the critical infrastructure of a nation is targeted, the nation is allowed to engage in active defense measures, or they could as well launch a corresponding a cyber-attack without being liable to answer to the international court. This should be followed by regulations that require a state to keep a list of critical infrastructure which the nation should protect with all the nations active defense measures; the file should also be made public.

It should also be an international law that if the identified sectors that form the critical infrastructure of a nation are to be attacked through cyber-attacks, then the nation should be allowed to respond to the attack without the need of first characterizing the nature of the attack (Talihärm, 7). The major complication of cyber-attacks is the fact that cyber-attacks are anonymous. The anonymity of cyber-attacks raises the civilians concern for their civil liberties. The cyber-attacks perpetrated by a foreign nation cannot implicate the kind of constitutional freedoms concerns caused by cyber-attacks originating from America. The use of active defensive approach against United States citizens in the case where a cyber-attack arises from America may be a violation of certain civil liberties of Americans.

The problem with the constitution of the United States is that it puts great emphasis on the civil rights of Americans, even those of perpetrators of cyber-attacks. The United States law should adjust from the traditional definition of the civilian’s right to privacy, their right to be protected against an unreasonable search, and the right to due process. The explanation is

that there is a great necessity of responding to cyber-attacks going through the lengthy method of determining the identity and intent of the culprit. Cyber-attacks could have catastrophic effects within hours of launch, therefore adhering to the traditional laws will only delay the identification of the perpetrators and their intent, a long process which could allow the cyber-attack to cripple a nation’s economy by the time it is completed (Singh 23). The government responds to cyber threats that originate from the United States through the use of passive defense measures like files and systems encryption and advanced computer firewalls. The active defense measures use methods that acquire intelligence from the personal information collected from people’s computer, and they can change personal data on that computer system and the destruction of the personal computer. It is thus the active defense measures that threaten the constitutional rights of people. America’s aggressive defense approach is the use the computers of citizens who have no idea they are being monitored as investigative tools.

This is why the attribution of a cyber-attack is very important. The other complication with cyber-attacks is that it is possible to trace a cyber-attack to a specific computer system, but it may be impossible to locate the attack on a particular person who coordinated the cyber-attack. This is a major complication as it increases the chances of the government accidentally violating the civil liberties of innocent individuals (Brenner and Clarke, 259). There is a big problem with the United States presumption that cyber-attacks should be categorized as criminal activities and not a threat to the nation’s security. There are examples of how this assumption could have significant effects on the critical infrastructure. In February the year 1998, three young

teenagers, two of which resided in California and one in Israel, launched a cyber-attack on the United States Navy and Airforce and accessed eleven unclassified computer systems.

Since the cyber-attack was categorized as a criminal activity, it was left in charge of a domestic agency to solve it, an operation that took almost a whole month to trace the culprits and arrest them. If the government had not worked under the presumption that the cyber-attack was criminal activity, the federal authorities could have been charged with the case and quickly launched an aggressive investigation that would have quickly traced the source of the attack and ended it. The nation only got lucky as the hackers only purpose was good humor and to test their capabilities. The country was also fortunate as the whole month was taken by the domestic agency to investigate the case did not result in catastrophic consequences.

The cyber-attack should have been a waking call for the government to realize the devastating effects that might arise if the attack was a severe attack solved with the same presumption (Moore, 110). The United States has operated for a long time under the front that a cyber-attack is a simple criminal act, a presumption that has been applied regardless of the targeted area by the cyber-attack. However, there is shortcoming with the classification of cyber-attacks since the government categorizes a cyber-attack that targets a civilian or a local joint as similar to the one that targets a computer or network system linked to the critical infrastructure.

The problem with this presumption is that dealing with cyber-attacks using this view could take some days or even months to investigate the sources

and the purpose of the attack. If the local law enforcement agency can determine the source of the attack, it is a process that takes time which could be regarding days or even months which make it impossible to prevent the damage caused by the cyber-attack. A cyber-attack should not be treated as a criminal matter which can be addressed efficiently using the nation's justice system but as a national security issue. As such, it is the role of the American government to provide a clear distinction between cybersecurity and cyber defense. It is impossible to distinguish between defense and security when the cyber environment is concerned. It is up to the policy makes to decide whether to view and treat a cyber-threat as criminal issues or as a concern for the national security.

It is the role of the policymakers to decide on this while ensuring that the final policy balances between protecting the civil liberties of American citizens and the ability of the government to quickly and vigorously respond to cyber threats launched against the nation. The United States does not have the luxury to be wrong in their decisions as the inability of the nation to defend its computer and network systems, a critical part of the nation's critical infrastructure, could result in major damages on the United States (Deibert and Rohozinski 24).