Threats to america

Technology, Internet

The conclusion of theCold Warinevitably surfaced gaps for the U. S. homeland security strategies. The attacks on 9/11 emerged a new security apprehension that involved terrorist groups who pose distorted threats to the U. S. Failures in intelligence due to events such as the Boston marathon bombing, WikiLeaks, and the first attempt at Osama Bin Laden's demise increase the need for concrete countrywide strategies, organized information databases, stricter punishments for criminals that breach security, and clear knowledge of intelligence policies and protocols.

The Economic Espionage Act of 1996 was passed in attempts to protect U. S. information and trade secrets (Uhrich, 2001). Despite its enactment twenty-two years ago, America is in the midst of monetary surveillance. All U. S. technologyis vulnerable and at risk. The current deterrence efforts are not enough to refrain the enemy and although America has inadequacies in privacy, other nations haven't developed a successful model either.

The information revolution has brought forth a majorclimate changewithin the last 10 years. Government agencies, militaries, law enforcement intelligence agencies, terrorists, hackers and criminals are on the net prowling information. Cyber espionage and criminal and foreign intelligence surveillance has gone into high gear post 9/11 due to the threats towards National Security being multifaceted and complex. Good intelligence is needed to meet the challenges in real time.

In modern day society it seems like privacy no longer exists. The root of privacy was established since America's declaration of Independence (Barr, 2015). During that time there was no telling how much everything in

America would evolve, especially with technology. The accessibility of technology today is endless, especially with surveillance. The sharing of information is very constant and technology is assisting the world with connecting in manners that most are unfamiliar with. Privacy is becoming more dynamic today because of the new developments linked with technology.

The similarities of interests between victims and international surveillance/cyber espionage provides an outlet in developing better protection in privacy within the cyber realm (Banks, 2014). With the advancement in technology the threats of espionage will continue to increase. Although the nation is underprepared for the vulnerabilities, there are numerous elucidations to conquer the breaching of privacy and security matters. The mutual groundwork relies on international cooperation as well as international legal agenda that fits the understanding of everyone involved.