The case surrounding the events in Estonia (2007) have significant implications for cyber issues. What were the challenges to attribution with the Estonia Case Study? Why is this important to the future of understanding cyber threat situations?

|  |
| --- |
| Both NATO and the Estonian government came to the conclusion that Russia was behind the cyber-attack in Estonia.  Of course, Russia denied this action, and while they admitted the attacks came from servers in their country, they blamed the attacks on rogue operators.  They denied any official involvement or planning from the Russian government, despite the primary IP addresses used in the attack originating in their country. (Armistead and Armistead 2015, 11) Without any formal way to punish the government or push this issue further, why would Russia not pass the blame?  The Computer Fraud and Abuse Act (CFAA) was amended in 1994 and is the main statute that prohibits hacking and provides guidelines for how to prosecute hackers, “In spite of the uncertainty of the breadth of the CFAA and the inconsistent understanding of the meaning of the terms ‘without authorization’ and ‘in excess of authorization’”. (Toren 2017) The ambiguity in the CFAA leads it to be impotent because it makes it very difficult to enforce the regulations. This does not deter cyber criminals because they do not believe that they will suffer serious consequences.  In 2010, Mike McConnell, a former director of the National Security Agency (NSA), said, “…we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment — who did it, from where, why and what was the result — more manageable.” (Clark and Landau 2011, 1) I have stated in a couple forums that I believe Russia is the most dangerous cyber threat to the United States because they do not care about attribution or their world perception.  The devastating cyber-attack conducted against Estonia was described as a, “brute force, crude attack…without the elegance and precision.”  (Waterman 2017) This would cause some to argue that the attacks could not have come from Russia because it was so haphazard and ill planned.  However, Russia is known to hire defectors and criminals, like Edward Snowden, to carry out cyber-attacks for them.  They understand that some of these hackers will do their due diligence and some will not. This works in their favor because it will cause many to believe that the government could not have planned or carried out the attack.    Other than to help with defensive cyber, what benefit is it for the United States, or any other country for that matter, to know who attacked their systems? What can we do to Russia, sanction them like Iran?  If the Untied States and other countries are not willing to take action against them does it really do much good to know who did it and assign blame? Not knowing who was responsible makes a country look incompetent, knowing and yet doing nothing makes them look impotent. Both merely serve to embolden attacks. Cyber war is a soft war and many government officials are hesitant to take a serious stance against it, because it is harder to get public support for this. However, the world cannot deny that cyber attacks can have very serious consequences and can lead to death just like traditional war.    References:    Armistead, Thomas and Leigh Armistead. “A New Frontier in War: Cyber Warfare in Estonia,” Contemporary Review 289, no. 1686 (2015), pp. 288-293.    Clark, David D. and Susan Landau, “Untangling Attribution,” Harvard National Security Journal (2011), pp. 1-30.    Toren, Peter. “COMPUTER FRAUD AND ABUSE ACT.” GPSolo 34, no. 5 (September 1, 2017): 70–71. <http://search.proquest.com/docview/2061859964/>.    Waterman, Shaun, “Who Cybersmacked Estonia?” UPI, June 11, 2007. Accessed at: http://www.upi.com/Business\_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/. |

