**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?**

The Estonia case is definitely a good example of potential issues with attribution, which are always tough to untangle. I will play the devil's advocate for a second and attempt to look at it from a different angle. There is no denying that these attacks essentially compromised if not temporarily crippled the Estonian communications network, as newspapers, mobile phones, emergency response systems, and the state’s largest bank were all targeted (Crosston, 2011). In addition, a concentrated attack effort was aimed at the offices of the president, prime minister, parliament, and the foreign ministry; however, even though Estonia declared that it was able to trace some of the attacks to Russian government offices, it did not in fact establish any direct governmental links (Crosston, 2011). Russia always maintained that the attacks came from renegade cyber nationalists, acting according to their own sense of warped patriotism but not on the orders of any official government office or agency there never was a definitive “smoking gun” piece of evidence proving formal Russian governmental policy as the chief culprit in the Estonian attacks (Crosston, 2011). Quite similarly, the Chinese hacking in Germany was strongly condemned by the United States and Germany, but no real evidence was ever presented and everything was vehemently denied by China (Crosston, 2011).

In my point of view, the Estonia case a a perfect real-world example of the attribution problem often theorized by cyber specialists: it is often too difficult to accurately trace a cyber attack to its origin; especially, in cases where an origination point can at least be compellingly argued, there is still no definitive way of proving just who was “at the trigger point” launching the attack (Crosston, 2011). It really is as simple as “how do you know who to retaliate against if you cannot be sure who threw the virtual punch?”(Crosston, 2011). Accurate attribution, therefore, is of highest importance, as it could lead to the commitment of military forces and expose a state to the most serious of consequences—battlefield casualties (Crosston, 2011).

So, why not hack someone back when we are almost hundred percent sure, but cannot definitively prove it? It will still send the message, that if you mess with us we will strike back. First and foremost, such act of hacking back will not be legal. The Computer Fraud and Abuse Act (CFAA) makes counter-hacking unlawful (Freeman, 2017). Therefore, the law in its current form needs to change, in order for counter-hacking to become legal. Furthermore, the argument about data owners who have the rights to retrieve their stolen data from the criminal who hacked their computer is still a very weak argument. Especially, since by doing that the person would still brake the law, simply because he/she would be acting without authorization from the criminal (Freeman, 2017). Therefore, our own laws and regulations must change and adapt to address the attribution issues.

Crosston, M. (2011). [World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence](http://www.au.af.mil/au/ssq/2011/spring/crosston.pdf). Retrieved from www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05\_Issue-1/Crosston.pdf

Freeman, J. (2017). Computer Fraud and Abuse Act (CFAA). Retrieved from https://www.freemanlaw-pllc.com/computer-fraud-abuse-act-cfaa/