

The Future of Cybercrime

By **Luther Martin** – ISSA member, Silicon Valley Chapter



The [Active Cyber Defense Certainty Act](#) (ACDC Act), was introduced by US Representative Tom Graves in 2017. This Act proposed to “provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers, and for other purposes.” In other words, it would legalize retaliatory hacking by businesses that were the targets of cyber criminals. This bill was widely derided as being a very bad idea. But is there a reasonable alternative to it?

Global spending on information security technologies is approaching \$200 billion. That’s a lot of money that could be better spent on more productive things. It could be invested in hiring more workers, building more factories, etc. Or it could be spent on addressing some of the big problems facing the world today.

The [Copenhagen Consensus Center](#) tries to use a careful cost-benefit analysis to prioritize projects that would do the most good for the world. Their analysis covers issues like air pollution, armed conflict, climate change, education, and more, and it consistently shows that the damage caused by many of the world’s problems could be greatly reduced by relatively modest investments: perhaps \$1 billion or less. Spending even 10 percent of the world’s information security budget on projects like these could dramatically improve the lives of millions of people, so there are very real costs from spending so much on information security instead of on more useful things.

Fundamentally, the reason that we need to spend so much on information security is because governments do not enforce existing laws. In many countries,

cybercrime may be illegal, but is often effectively decriminalized as long as the targets of the cybercrime are in countries that are not friendly to the host nation of the cyber criminals. This makes information security a law enforcement problem, not a technology problem. This was noted by the authors of the paper “[Measuring the Cost of Cybercrime](#),” who said that their research “suggest[s] that we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response—that is, on the prosaic business of hunting down cyber criminals and throwing them in jail.”

Data breaches that cause over \$100 million in losses are distressingly common these days, and it simply does not seem reasonable that businesses should cheerfully accept such losses without some form of recourse. But if governments are either unwilling or unable to protect businesses from cyber criminals by enforcing existing laws, what are businesses to do? Even if businesses took the law into their own hands, perhaps like the ACDC Act might allow, and freely retaliated against cyber criminals that cause the large losses, it seems unlikely that they would be able to achieve anything approaching a reasonable idea of justice. It’s probably simply not possible to cause \$100 million in retaliatory damage to cyber criminals, whose assets almost certainly will amount to much, much less than that amount.

But it is easy to inflict that much damage on other businesses or on an economy as a whole. So a more effective way to respond to expensive acts of cybercrime might be to retaliate against businesses or the government of the country whose lack of effective law enforcement decriminalized the behavior of the cyber criminals. A better way might be simply

to make the government that decriminalized the actions of its cyber criminals liable for their actions.

There is actually a precedent for this in international law in the [Convention on International Liability for Damage Caused by Space Objects](#), sometimes known as the Space Liability Convention. This treaty assigns responsibility for all space objects launched from within a country to the government of that country. So if a foreign company launches a satellite into space from an American facility, the US government is responsible for any damage that that satellite might cause if it somehow ended up crashing and causing damage.

Extending this idea to cyberspace might be feasible. Under a treaty based on this idea, if a foreign cyber criminal operating from the US caused damage through cyber crime, then the US government would be responsible for that damage.

The alternative to this approach could be a dystopian future like described by William Gibson in his book *Neuromancer*, in which cyber criminals seem free to roam cyberspace and only fear retaliation from other cyber criminals or from agents hired by the targets of their cybercrime. If that’s not the future we want, we need to find way to get governments to enforce their existing laws. There’s simply too much to lose and a lot to gain from establishing reasonable rules for conduct in cyberspace and then enforcing them.

About the Author

Luther Martin is a Distinguished Technologist at Micro Focus. You can reach him at luther.martin@microfocus.com.