8-29-2019

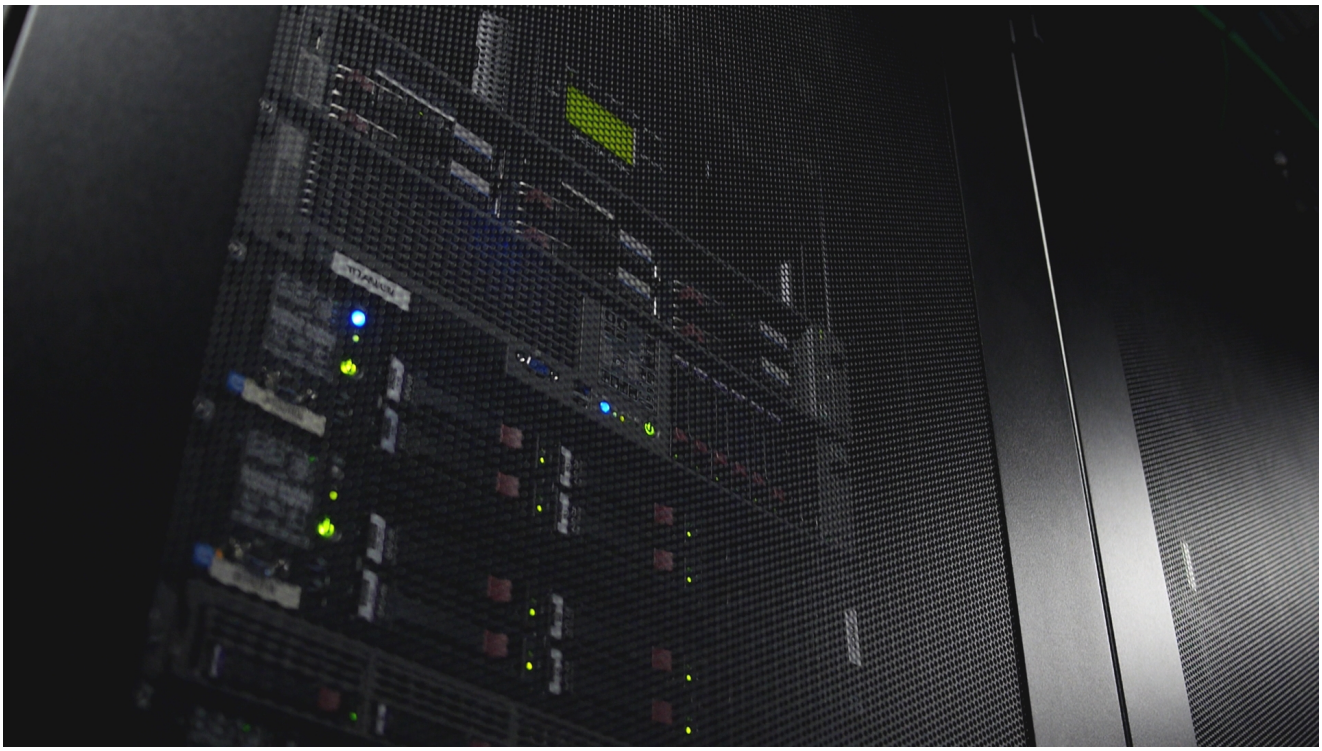
It's Not IF but WHEN: Three Challenges to Handcuffing Cybercrime

Andrew Rossow
University of Dayton, rossowa1@udayton.edu

W. David Salisbury
University of Dayton, wsalisbury1@udayton.edu

It’s not IF but WHEN: Three Challenges to Handcuffing Cybercrime

udayton.edu/blogs/cybersecurity/2019/2019-08-30-cybercrime-rossowsalisbury.php



Thursday August 29, 2019

By Andrew Rossow, Attorney at Law, Rossow Law & Adjunct Professor, UD Law School & W. David Salisbury, Professor of Information Systems & Director, UD Center for Cybersecurity & Data Intelligence

Given the daily drumbeat of news regarding online data breaches, some may wonder why cybercriminals are not often found and arrested. It would seem that, when enough people and organizations are victimized, and enough money is stolen, that this would certainly be a focus for law enforcement.

Humorist P. J. O’Rourke once wrote: “*Evil is an outreach program. A solitary bad person sitting alone, harboring genocidal thoughts, and wishing he ruled the world is not a problem unless he lives next to us in the trailer park. In the big geopolitical trailer park that is the world today, he does.”*

The problem is that on the Internet, everybody lives next to us in the trailer park. It’s also currently harder to catch this person when they do something bad. In today’s digital age, the sophistication of a crime has grown immensely, making it almost impossible, if not financially

impracticable to utilize resources in bringing the perpetrator to justice.

As a cybersecurity researcher and a millennial lawyer with a strong concentration on cyberspace law, blockchain technology, and digital monies, we discuss the three main challenges law enforcement currently faces when attempting to bring cybercriminals to justice.

When You're Online, Jurisdiction is Unlimited

The beauty of our digital age is the (almost) unlimited power and freedom we have when browsing the internet. Cyberspace, as we call it, provides another world where each of us has the ability to re-create who we are.

But, is it really that hard to believe? Online, you are different—your name and image, dialect and personality—all repurposed to give the online community a perception you want them to see. Your online appearance is what lawyers call "residual self-image," the mental projection of your digital self.

Unlike the physical nature of the world we live in where laws and physical borders help shape the ways in which we interact and engage with one another, online, there are no boundaries or borders. It's a free-flowing network of computer code and users.

Given the distributed nature of the Internet, and given that the internet wasn't designed with bad actors in mind, this shouldn't be a surprise. Cyber-criminals, categorized as either *black-hatters, gray-hatters,* and/or *white-hatters* utilize the networks for different purposes.

Physical Jurisdiction vs. Digital Jurisdiction

Individuals who wish to launch a cyberattack can do so from anywhere in the world. There is no longer this constraint on physical presence, which in the legal community, often is a major factor. Online, the meaning of "jurisdiction" is different, as physical presence isn't the deciding factor—a targeted attack can be enough to warrant jurisdiction if its determined that the attack was almost as if the attacker was physically present in/on the victimized location.

From a national security standpoint, state actors can readily launch attacks against people and systems in other countries, such as the recent Capital One data breach, where a former Amazon Web Services employee was able to penetrate the system through the back-end.

Hiding One's Identity Online

With the internet, we have the ability to mask our identity by re-routing our IP address (our computer's driver's license) and making it look like activities are coming from another location/IP address. This is often done through the use of virtual private networks, or VPN's.

By masking the servers from which one is working, or indeed routing the attacks through other countries, individuals and nation-states engaging in cyber-attacks can, with relative ease, mask their locations. This makes it difficult for law enforcement and governments to identify the source of attacks, which obviously means that pursuing the attackers is difficult as well.

There is a Low Motivation to Capture and Extradite Cybercriminals

Because of the virtual nature of online interaction, the resources needed to first recognize an attack has occurred, then identify where it originated from, then identify the culprit behind it is at times, impracticable and financially unfeasible.

Assuming one can even find the attackers, many of them come from countries not well integrated into the global community, and as such the laws in those countries are not as robust. Further, many of these countries don't have extradition treaties with western nations, so even if they can be found they may not be readily caught. Finally, in some cases, the attackers are working for the nation state directly, or are at least doing things that benefit the country where they reside, so motivation to help catch them and extradite them is low.

So What's Next?

While the good news here may not be readily visible, determination and drive is everything, and the means for attack can also be the means for surveillance and identification of the attacker.

Vigilance is of utmost importance for those who have sensitive and important information available to them. The problem is that the cyber environment tends to move fast, and laws and governments tend to be slow.

In the law, we are still catching up. Legislators for the longest of times have attempted to plug in these new forms of crimes into existing laws and statutes, hoping it fits like a puzzle piece. Unfortunately, it's a not a one size fits all analysis. For example, not all instances of stalking, bullying, or harassment can be addressed by existing harassment statutes. Each case is different because of the manner in which it was carried out and the technology utilized to help facilitate its damage.

It is for this reason that many states simply don't have the laws that readily address these problems we face on the regular. Legal experts are taking up the discussion of cybercrime and international law, which will eventually lead to norms for behavior in cyberspace.

Further, even smart people make mistakes, and find themselves in a country where there are strong extradition agreements, and where intelligence services can find them. As an example, in 2018 a suspected Russian hacker has been extradited to the US after his capture in the Czech Republic.

Clearly there are and will continue to be challenges with respect to capturing cyber-criminals due to the nature of geography, laws, international relations and the reach of the technology itself. However, progress is being made, and will continue.