LEGISLATING CYBERCRIME:

WHY STRONGER LEGISLATION IS REQUIRED CONSIDERING THE PSYCHOLOGY OF COMPUTER USERS

Dani LeBlanc

DECEMBER 12, 2022

HN-300-F

Professor Trudeau & Professor Thomson

Introduction

Crime and punishment are together often a popular topic of debate amongst criminologists, psychologists, and law and policy makers; however, as cybercrime quickly escalates in popularity, computer specialists and cybersecurity professionals are beginning to enter the fray. Emerging cybercrimes are the beginning of a whole new field of crime, leaving investigators and prosecutors scratching their heads, wondering how to investigate and punish cybercriminals while applying the current policies and punishments in place for crime as it stands. It may initially appear that cybercrimes can be jammed into the pre-existing constructs of other methods and classes of crime, yet there are multiple differences distinguishing cybercrime as an entire category of its own. These differences include the uniquely developed psychology of individuals behind a computer screen, the primarily financial motivation of the crimes not dependent on the victim, and the lack of specific legislation regarding cybercrime. Additionally, writing new legislation can be difficult due to differences in public opinion and the incredibly technological aspect of the crimes, as well as the unique nature of the digital environment which presents an entirely new set of challenges. While the crimes that occur within cyberspace are often comparable to crimes seen offline, it is clear that the nature of cybercrimes and psychological state of cybercriminals differs substantially from that of traditional criminals, and therefore an improvement in cybercrime legislation based on these factors is essential.

Cybercrime's Current Impact

While some may question whether cybercrime is really a relevant enough issue to require its own legislation, after contextualizing cybercrime with how it impacts businesses today it is apparent that cybercrime is in fact relevant. Many companies think that they could never be a

victim of cybercrime due to the security of their networks or practices they put in place, however as of mid-2022 hackers had the capability to breach 93% of networks (Brooks). Despite the implications of this being initially obscure, monetizing the impact of these breaches makes the extent of the effects apparent. In 2021, cybercrime cost businesses over $6.9 billion (Brooks). This is obviously a large monetary impact on any business, but it is easy to see how a large financial breech due to cybercrime could be detrimental to small businesses especially.

Another way that businesses often fall vulnerable to cybercriminals is through phishing scams, which target human vulnerabilities rather than technical vacancies. Phishing is when a criminal pretends to be a legitimate source in order to gain information that normally would only be trusted to that source. A common example is a criminal pretends to be a bank employee from a victim's bank and asks for account information or usernames and passwords under the guise that they work at the bank. If the criminal is convincing enough, victims will often hand over their information, allowing criminals to gain access to their accounts, sell the info on the dark web, or even steal their identity. This is often a product of or leads to email compromises, which since 2016 have been responsible for $43 billion being stolen (Brooks). Healthcare and insurance organizations were especially vulnerable to phishing schemes, having a 45-60% chance of being the victim of a phishing attack at the beginning of 2021 (Brooks). This in and of itself is a concerning statistic, showing the prevalence of cybercrime in important industries, however the rate at which this chance is growing is concerning as well, increasing by 10% by the end of the year (Brooks). Evidently, cybercrime is a present and growing threat, and because it is so prominent amongst businesses it needs to be regulated, prevented, and prosecuted in some manner.

Current Legal Context and Challenges

Computer-based entities are increasing in both presence and utility as a part of everyday life, facilitating similar interactions and functions as those performed outside of the digital environment. Many are reluctant to seek regulations for cyberspace, however, viewing it as a potential invasion of privacy. While there is very limited cyber-focused policy around the world, what little there is often comes under heavy fire, making it difficult to both develop current legislation and enact new policies. In March of 2015, Canada instated a bill entitled the Protecting Canadians from Online Crime Act, which criminalized activities such as possession of nonconsensual intimate images and harassment via digital means of communication (Coburn et al.). While the Canadian bill was intended to decrease cyberbullying and other harmful online behaviors, it was met with opposition rooted in concerns over infringing on privacy, as the bill gives police more investigative and enforcement abilities online (Coburn et al.). While the focus of the bill is not investigative privileges of law enforcement, but rather the protection of citizens from dangerous online behaviors, the concerns quickly shifted to privacy violations that are not unique to Canadians.

Americans share similar concerns over privacy, and for this reason it is difficult to instate new laws regulating virtual activities. Despite the challenge, this is essential, due to the fact that the current legislation used to investigate and punish cybercrime is not specific to digital crimes, despite their fundamental differences. Continuing to use old legislation developed before the rise of cybercrime results in a situation where law enforcement must attempt to fit crimes committed online into pre-existing definitions of real-world crimes. Essentially, they are responsible for identifying the cybercrime's closest real-world equivalent, and prosecuting it as such. The directions and definitions outlined within legislation are therefore close, but not entirely

applicable to the cybercrime, as the virtual environment creates a different dynamic between the cybercriminal, the crime they commit, and the victim. This results in an oversimplification of the complex dynamics of cybercrime, forcing these criminal activities to be jammed into imperfect categories, and limiting law enforcements' ability to investigate and prosecute cybercrimes.

Law enforcement observation and regulation of Cyberspace is often viewed as an infringement of privacy, despite the motivations of digital investigations aligning with the interests of citizens, just as traditional criminal law enforcement does (Gray et al.). The difficulty in creating new cyber focused legislation revolves around the public fear of giving up rights and privacy in the interest of security while online. What many citizens don't realize is that some of the current policies in place for the physical world create similar "invasions of privacy" but allow law enforcement to properly carry out their duties with clear direction and boundaries for that privacy. In the landmark court case *Katz vs. United States*, the public observation doctrine and third party doctrine were upheld in the interest of traditional crime (Gray et al.). The public observation doctrine allows law enforcement to monitor public spaces themselves and from public spaces the activities of an individual, or preserve discarded property thrown into trash bins (Gray et al.). The third-party doctrine states that any information shared with another party can no longer be considered completely private and that the information could therefore be shared with others (Gray et al.).

These principles could easily be refined to provide protections for citizens online, both from cybercrime and from invasions of privacy, contrary to what they may think. This is because laws and policies provide distinct and clear boundaries for law enforcement investigations, making it clear what is an invasion of privacy compared to a legal method of investigation. Law enforcement is therefore prevented from unknowingly or unintentionally crossing the line and

breaching an individual's privacy. Considering social media platforms are essentially the public meeting spaces of the internet and emails, texts, and other forms of virtual communication can be considered akin to conversations had in the real world, it is easy to extrapolate these protective, real-world measures long upheld by the justice system to a virtual environment, which would provide citizens with benefits just as it does outside of cyberspace today.

Distinguishing Cybercrime from Real-World Crime

By examining the distinguishing features of cybercrime, it is apparent that a virtual interface may be more conducive to some crimes, and therefore requires additional regulation to dissuade the use of technology for malicious reasons. The nature of the crimes themselves is inherently different from real world crime, because technology creates an entirely new type of environment for crime to occur in. The virtual environment of these crimes presents many uniquely challenging aspects, such as the speed with which it can evolve or the altered perception of reality users experience. Therefore, individualizing legislation against cybercrime is essential to help combat it more successfully. Technological advancements flourish within the blink of an eye, allowing cybercriminals to develop new tactics before their old ones are understood and combated, resulting in a tidal wave of incoming never-before seen cybercrimes (Staniforth and Barrett). This faster-paced development means that cybercrime has begun to and will continue to outpace traditional legislation. Therefore, a more adaptive approach is called for in regulating and disbanding cybercrime, as cybercrime itself is a more adaptive style of crime.

Additionally, compared to traditional crimes, there are exponentially more methods in which crime can potentially be conducted, making it difficult to classify and prosecute crimes. One such evolution into a new territory of crime has occurred with biomedical data. In recent years,

cybercriminals have shifted focus beyond identity theft in the traditional sense to biomedical data and other previously undisturbed categories of personal information, now viewed as infinitely more valuable and private than credit card numbers or bank transactions (Staniforth and Barrett). It is difficult to decide whether to call the theft of biomedical data identity theft or some other variety of crime, when the action of stealing biomedical data is so unique to the digital front. While biomedical data has been stolen in the past, it had never been conducted in the magnitude or with the ease seen today. Previously, as with many real-world versions of cybercrime, it would have involved high-risk actions such as breaking into facilities or homes, and in person exchanges of the data for money. Now, all within a few keystrokes and clicks, biomedical data can be obtained, posted for sale, and sold to the highest bidder for a quick and easy profit obtained by the criminal. This highlights the difference between cybercrimes and real-world crimes, as cybercrime moves at a much faster pace, with incredibly large quantities of money, all without the criminal getting up from their chair. New legislation would be required in order to allow for the proper deterrence, investigation, and prosecution of cybercrime in these previously unexercised regions and in previously unfathomable methods from which no equal comparison can be made to the non-digital world.

Morality and Motives of Cybercriminals

In analyzing crime as a whole, it can be observed that the most prominent motivation as to why people commit crimes is the human nature to aim towards maximization of their own pleasure combined with minimized pain (Hirschi and Gottfredson). The quick receipt of pleasure compounds the satisfaction one derives from it, making instantaneous pleasure the most satisfying of all (Hirschi and Gottfredson). It can be argued that interactions facilitated by digital means create instant gratification, maximizing the speed with which pleasure and satisfaction are

obtained by those using technologies such as video games, social media, and online transaction platforms. Some of the virtual factors that create the instant gratification for cybercriminals, further encouraging cybercrime, are the fact that there is an endless victim pool, infinite resources available, and little risk involved in committing crimes due to the lax regulations on cybercrime and little observation. This illustrates how cybercrime as it stands today maximizes pleasure without much risk for pain, especially when broken down in terms of instant gratification and the increased satisfaction it adds. Imposing stricter regulations and steeper, well-defined punishments would elevate the risk of failure, maximizing the potential pain factor and reducing the pleasure and satisfaction derived from such activates. When the risk of committing cybercrime becomes great enough that the pleasure is minimized, it makes the commission of cybercrimes less attractive for criminals.

Outside of the digital realm, steep punishments are imposed on those who commit egregious crimes; however, the same tenacity is not seen in prosecuting cybercrime, allowing it to grow in popularity. Robbing a bank for millions of dollars is not very attractive when there is a high likelihood that this will be met with in depth investigations leading to a long stay in prison and ultimately no financial gain. Conversely, anonymously stealing millions of dollars in the span of a few minutes from the comfort of home, without the threat of intense investigations and hefty punishments, begins to look very profitable and easily doable. Therefore, stricter legislation would aid in minimizing the attractiveness of cybercrime, helping to dissuade future criminals combined with obviously aiding in the prosecution of current criminals.

In addition to some of the other challenges that distinguish cybercrime from other types of crime, the psychology of individuals while engaging with a virtual environment is altered to accentuate factors that allow them to disengage with reality and leave traditional morals behind.

There are several elements that contribute to an individual's recognition of morality, a large deterrent in the commitment of crime, however some elements of online interactions distill a few of these elements to the point where morality is tossed aside. Traditionally, people do not commit crime because their morality and ability to empathize with the victim create strong feelings of guilt. This is typically agreed upon as an unpleasant emotion that directly results from one's actions when it violates their morals. One key factor in maintaining moral conduct is the recognition by an individual that their actions negatively impact another individual (Bandura). An understanding by the criminal that the crime they committed has caused the person who was the victim to be in a worse condition then they had been in previously is essential for feelings of guilt and remorse.

In cybercrime, the digital separation can obscure the impact that the criminals have on the victims, making guilt scarce. Since guilt is triggered by empathy, one can theorize that empathy is directly impacted by the separation between victim and criminal in a digital environment. This is in fact the case, as one essential component of empathic behavior is the ability to observe and mimic the behavior of others (Ferrari), which obviously is not possible if the criminal never sees or interacts with the victims of their crimes beyond the data displayed on their monitor. The sense of disconnection felt by computer users from each other allows them to forget that they are impacting real people with their interactions, further disconnecting from reality. Therefore, it may seem at times that others on the internet and the information belonging to others are akin to objects in a video game. It lures computer users into a mentality where cybercriminals can rationalize or justify their actions, because they never see these actions negatively impact the victims of their crimes from behind their screen. Because the impact is never fully realized, guilt is mitigated and the negative side effects of committing crime are diminished, meaning that the

"positive" results criminals see are not combated by their morals in the same way they would be in the real world. Therefore, cybercrimes are easier for criminals to commit, and additional regulation would be required to heighten the negative consequences.

It is widely agreed that interacting with others online feels different from interacting with people in the real world, and is more like interacting with fictional components from videogames than interacting with real people and their information. Dehumanization of those who are impacted by the actions of cybercriminals is another psychological disengagement technique, in which those influenced by an individual's actions are viewed as without human qualities, depicting them as without feelings, hopes, and concerns (Bandura). The virtual environment is more conducive for cybercriminals to view victims as digital elements rather than real people, allowing the crimes to seem more moral than they would if committed face-to-face. While many cyber criminals would never consider walking up to an elderly woman and stealing her wallet, they don't think twice when stealing personal information or money from online bank accounts belonging to those same individuals. While it is evident that these are vastly different crimes, it begs the question of why? When stripped down to this simple level, they seem similar. Moreover, why it is possible to feel so comfortable while online, but be abhorred by the real-world version of the exact same crime? The essential difference in this case is that the facilitation of the crime online allows criminals to disengage from the reality of their actions and dehumanize the victims, considering they only see a name and numeric data associated with a victim rather than the person themselves. Empathy relies on the observation and mimicry of others due to the fact that body language and facial expressions are associated with a particular feeling, and when the same body language is observed in another person, the brain of the observer evokes the associated emotion (Ferrari). Because the person themselves is never

observed and data does not share this same interpersonal connection, it is easy to see how empathy remains unstirred and feelings, hopes, and concerns of the victims can go unthought of. This makes it clear that dehumanization that occurs between computer users uniquely strips them of their typical morals, making cybercrime vastly more plausible compared to traditional crime.

While a tendency of cybercriminals to rationalize their actions via dehumanizing victims is a byproduct of the virtual environment, there are also certain practices which perpetuate dehumanizing others online. Videogames and other digital activities make regular practices of encouraging users to do whatever they please to other characters or players while interacting with them within the context of the game. Violent videogames specifically promote dominance over others within the environment and promote the elevation of one's own status through overcoming others, while encouraging the use of anger-related traits (Denson et al.).While the impact of violent videogames in the real world is often heavily disputed, when the difference between a space where you can have no care or empathy towards those around you and a space where you are interacting with others and their real lives is an application window or browser tab away, the lines can easily get blurry. Users may develop a subconscious association between being online and this free dehumanization behavior, resulting in the behavior to continue across platforms, despite the inappropriate applications in some spaces. Dehumanization behaviors encouraged in some spaces on the internet can easily bleed over into other online interactions, therefore resulting in a strengthening of this immoral principle which is normally subdued by morality during in-person interactions.

It has been established that the disassociation and dehumanization cybercriminals feel towards victims are two mental facilitators for moral disengagement that uniquely fuel cybercrime, considering they dismantle an individual's morals and are a direct result of the

digital environment. The physical distance between victim and criminal across the digital universe makes it even easier for criminals to disassociate from the reality of their impact on the victims. One theory of moral inhibition is based off the fact that "It is easier to harm others when their suffering is not visible and when destructive actions are physically and remote from their injurious effects" (Bandura). Technology naturally sets up a disengaged relationship between the perpetrator and the victim, making it more palatable to commit a crime against another person. This is yet another factor that makes the psychology of computer users different from that seen in the real world, and outlines how virtual spaces are more conducive to crime. Because crime is more approachable in this space, stronger legislation is required, as it requires more dissuasion to prevent cybercrime than regular crime. This is because moral decision making normally inhibits crime, however when this inhibition is lost, legislation must step in to dispel crime in place.

While very few studies have focused on this principle within cybercriminals, through examining those who engage in cyberbullying behaviors on the internet, it is easy to see that there is a sense of disassociation that separates the user from reality, altering the behavior of those behind the screen. One could extrapolate that malicious behaviors of cyberbullying are similar to those observed in individuals who commit cybercrimes. The disassociation allows individuals who participate in both to more easily engage in immoral behavior. Not only has it been previously established that digital interactions inhibit moral controls through natural dehumanization and distancing factors, the connection between these factors and cybercrime can be furthered by looking at their relationship with cyberbullying. It has been discovered through studies that "While the moral disengagement mechanisms together predicted cyber aggression perpetration, only dehumanization, advantageous comparison, distortion of consequences, and displacement of responsibility were significant, unique predictors" (Nocera et al.). There are a

wide variety of factors that are often observed in connection with cyberaggression, yet a majority of these factors have to do with distortion of reality to mitigate the perceived wrongfulness of the criminal actor. Essentially, cyberbullying is widely engaged in because of the ease with which individuals can participate without feeling remorse, a typical moral inhibition that is dispelled through the separation and dehumanization of cyberbullying victims. Because many of the behaviors seen in cyberbullying relate to those of cybercrime, the same idea can explain why cybercrime may be easier to commit than real-world crime. These displacement and distortion factors make cybercrime more palatable, as there is less empathy and remorse associated with the act after the victim has been dehumanized in comparison to how someone would engage with others outside of a virtual space.

A study by Perren and Gutzwiller-Helfenfinger also identified that "the […] results suggest pronounced predictive power of remorse on cyberbullying. We may speculate that the absence of direct contact between perpetrator and victim lowers the cyberbully's emotional engagement regarding feelings of remorse" (Perren and Gutzwiller-Helfenfinger). This demonstrates the principle that a lack of face-to-face communication decreases the traditional emotional responses one has when they carry out an action that they know will negatively impact or hurt another person in the context of maleficent cyber-based actions. When cyberbullying is examined as a specific type of malicious action that can take place on the internet, it is clear that environmentally encouraged factors such as dehumanization and disassociation make virtual space a more conducive location for cyberbullying behaviors. This principle could be applied towards other harmful and criminal activities conducted in virtual space, making it even clearer that cybercrime comes more easily to individuals than traditional crime. When the internal emotional discomfort factors are limited in comparison to traditional crimes, strong cybercrime

focused legislation is required in order to deter this type of crime, as there are fewer moral inhibitions to do so.

Legislation Moving Forward

Because cybercrime largely does not involve interacting with or harming the victims themselves, the motivations behind cybercrime are almost purely monetary, meaning that economic punishments would have a larger deterring effect than other punishment methods. While money is often a factor in many types of crime, no other group of crime entirely excludes the victim like cybercrime. Crimes of passion or those in which the effect on another individual is observed are often motivated by the feelings the perpetrator has towards the victim, however as established above, in the case of cybercrime, there is no personal, emotional relationship with the victim. When offenders place high value in the risk of committing crimes, then high monetary value compounds the risk, making crime more attractive (Ehrlich). One could develop this premise to also include those who are deterred by large monetary punishments, which are implied to be the ones who are inclined to engage low risk and high reward crimes, meaning crimes with high expected payouts. It can be argued that cybercrime is one of the lowest risk avenues of crime that often results in larger monetary gains. Cybercrime allows criminals to easily remain anonymous, detached and distant from the victims, and have access to large amounts of money. Psychologically, the criminal does not care about the victim, as they are simply a means to an end, the end which they value being financial gain. Almost every cybercrime ends in some form of transaction, either through directly stealing money or online currencies, or selling stolen information or methods of access on the dark web. Because the draw to cybercrime for criminals is not risk, but rather reward, adding steeper financial punishments would disincentivize the crimes, disbanding the idea of little-risk for high-reward. This identifies

the desire of cybercrime as money, meaning that monetary punishments would be more effective in the deterrence of cybercrime, as the crimes themselves are primarily monetarily motivated.

While economic sanctions, or legal financial obligations, are typically viewed as harmful or unwarranted responses to crime, an exception can be made in the case of cybercrime. It has been identified that the crime itself is mainly monetarily driven, and therefore eliminating this draw to the crime would be the most powerful deterrent. Additionally, the impact on the victims of cybercrime is also primarily monetary. The primary argument against monetary punishments is that it leads to great financial uncertainties and frustrations for those they are imposed upon and can push those already struggling with finances into further peril (Alexes Harris et al.). Restitutions, however, are seen as a better alternative. Separate from fees and fines, they are employed specifically in cases where the crime itself incurred financial loss or damage for the victims, with the payments serving to help reconcile the damage or loss (Beckett and Harris). Monetary punishment specifically identified as restitutions would clearly result in the most well-rounded benefit for both the victim and criminal in terms of justice. This is due to the fact that the economic punishment would function as a deterrent for the financially motivated cybercriminals, while the restitutions would specifically benefit those who were victimized by the highly invasive and financially devastating nature of cybercrime. Therefore, a restitution-based cybercrime punishment would be the best form of legislation for both preventing and atoning for cybercrimes.

In Conclusion

Considering the environmental and psychological factors of cybercrime, a virtual environment is more conducive to crime, and therefore requires additional legislation to protect

computer users. One factor that has been clearly established as a conductor for cybercrime is the disengagement and disassociation computer users feel as a side effect of interacting with others from behind their screen. Moral disengagement is a process that occurs over time, compounding as individuals continue to commit harmful acts while disengaging, resulting in a desensitization to these acts and reinforcing the moral disengagement (Bandura). Legislation should consider the desensitization of computer users for their crimes, as there needs to be further reason to not commit cybercrime due to the lack of dissuasion resulting from dissipating morals. Because of the altered psychology and the desensitizing effects of continued crime in a virtual environment, it can be argued that the retribution for such crimes should include psychological evaluations and assistance to help remedy the user's disengagement. As with any crime, rehabilitation is an important preventative measure against the continued commission of the same crime, and since the previously discussed psychological factors are such a large contributor to justifying the crimes, an effort should be made to reengage moral evaluation factors in order to disable this faulty justification process in the future.

While simply creating more laws seems like a relatively easy task, an inhibitor of creating a successful set of modern legislation for cybercrime would be the general lack of technical knowledge by policy makers. This results in a lack of understanding surrounding both why it is important and how to accomplish creating successful legislation. While it is not reasonable to expect policy makers to gain a full understanding of cybercrime and the technology behind it, there are ways in which they can be assisted with understanding this information so that they are better equipped to propose more effective laws and policies. In an attempt to assist their legislative body, the European Union has instituted a group of interdisciplinary experts who focus on remaining up to date with essential cyberspace information, which allows them to better

analyze what is occurring virtually and how to best protect computer users through legislation (Redford). This remedies the issue of legislators being left unaware of progressions in technology and how that technology may be used to violate an individual's rights and safety. Appointing groups such as these have obvious and endless informational benefits, allowing the laws and policies created to be both relevant and accurate in assisting in the prevention of cybercrime.

Initially it may appear that cybercrime can be investigated and prosecuted within the confines of current legislation designed for traditional methods of crime, however upon further investigation it becomes clear that new legislation is essential to combat this distinct and uniquely challenging field of crime. New legislation clearly targeting cybercrime may be viewed as a potential invasion of privacy or otherwise problematic, however after looking at laws for traditional crime, it is clear that specific policy provides definite operational guidelines and boundaries for investigators that actually protects the privacies in question. Additionally, the economic promise of these crimes combined with the anonymity of cyberspace creates a low-risk and high-reward situation, making it particularly attractive to criminals. As a deterrent and prevention mechanism, both psychological treatments to reverse the dissipation of morals and financial restitutions to both make the crime less attractive and help relieve the impact of the crimes on victims should be instated against cybercrime. Additionally, a more informed legal body could help prioritize relevant and accurate anti-cybercrime legislation, helping to make the policies more impactful. Because of the unique challenges of a digital landscape, including the quickly evolving environment itself as well as criminal methods observed to be employed by cybercriminals, cybercrime is vastly different from traditional crime and therefore requires its own set of legislation in order to properly deter and prosecute it.

Acknowledgements

Thank you to everyone who assisted in the making of this paper:

Professor Trudeau & Professor Thomson, and Nicholas Lebanca.

Works Cited

Alexes Harris, et al. “Studying the System of Monetary Sanctions.” *RSF: The Russell Sage Foundation Journal of the Social Sciences*, vol. 8, no. 2, Jan. 2022, pp. 1–33. *EBSCOhost*, https://doi.org/10.7758/RSF.2022.8.2.01.

Bandura, Albert. “Selective Moral Disengagement in the Exercise of Moral Agency: Journal of Moral Education.” *Journal of Moral Education*, vol. 31, no. 2, June 2002, pp. 101–19. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=phl&AN=PHL1703540&site=eds-live&scope=site.

Beckett, Katherine, and Alexes Harris. “On Cash and Conviction: Monetary Sanctions as Misguided Policy.” *Criminology and Public Policy*, vol. 10, no. 3, Aug. 2011, pp. 509–38. *EBSCOhost*, https://sacredheart.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.crpp10.56&site=eds-live&scope=site.

Brooks, Chuck. “Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know.” *Forbes*, https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/. Accessed 20 Nov. 2022.

Coburn, Patricia I., et al. "Cyberbullying: Is Federal Criminal Legislation the Solution." *Canadian Journal of Criminology and Criminal Justice*, vol. 57, no. 4, Oct. 2015, pp. 566–79. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.cjccj57.32&site=eds-live&scope=site.

Denson, Thomas F., et al. "Understanding the Desire to Play Violent Video Games: An Integrative Motivational Theory." *Motivation Science*, vol. 8, no. 2, June 2022, pp. 161–73. 2022-66267-007, *EBSCOhost*, https://doi.org/10.1037/mot0000246.

Ehrlich, Isaac. "Crime, Punishment, and the Market for Offenses." *The Journal of Economic Perspectives*, vol. 10, no. 1, Jan. 1996, pp. 43–67. *EBSCOhost*, https://sacredheart.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edsjsr&AN=edsjsr.2138283&site=eds-live&scope=site.

Ferrari, Pier F. "The Neuroscience of Social Relations. A Comparative-Based Approach to Empathy and to the Capacity of Evaluating Others' Action Value." *Behaviour*, vol. 151, no. 2/3, Jan. 2014, pp. 297–313. *EBSCOhost*, https://sacredheart.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edsjsr&AN=edsjsr.24526010&site=eds-live&scope=site.

Gray, David, et al. "Fighting Cybercrime after United States v. Jones." *Journal of Criminal Law and Criminology*, vol. 103, no. 3, June 2013, pp. 745–802. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.jclc103.25&site=eds-live&scope=site.

Hirschi, Travis, and Michael Gottfredson. “Causes of White-Collar Crime*.” *Criminology*, vol. 25, no. 4, Nov. 1987, pp. 949–74. *EBSCOhost*, https://doi.org/10.1111/j.1745-9125.1987.tb00827.x.

Nocera, Taylor R., et al. “Moral Disengagement Mechanisms Predict Cyber Aggression Among Emerging Adults.” *Cyberpsychology*, vol. 16, no. 1, Mar. 2022, pp. 82–99. *EBSCOhost*, https://doi.org/10.5817/CP2022-1-6.

Perren, Sonja, and Eveline Gutzwiller-Helfenfinger. “Cyberbullying and Traditional Bullying in Adolescence: Differential Roles of Moral Disengagement, Moral Emotions, and Moral Values.” *European Journal of Developmental Psychology*, vol. 9, no. 2, Mar. 2012, pp. 195–209. *EBSCOhost*, https://doi.org/10.1080/17405629.2011.643168.

Redford, Mike. “U.S. and EU Legislation on Cybercrime.” *2011 European Intelligence and Security Informatics Conference*, 2011, pp. 34–37. *IEEE Xplore*, https://doi.org/10.1109/EISIC.2011.38.

Staniforth, Detective Inspector Andrew, and Francesca Barrett. “Securing Cyberspace - Combatting Cyber Fraud and Online Identity Theft.” *International Scientific Conference on Security & Euroatlantic Perspectives of the Balkans Police Science & Police Profession*, Sept. 2017, pp. 62–71. *EBSCOhost*, https://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=155413510&site=eds-live&scope=site.