**A Critical Review of the Literature: Cybersecurity in Criminal Justice**

Robert Chapa

Doctor of Criminal Justice Department, Saint Leo University

DJC 705: Transformational Leadership

Dr. Eloy Nuñez

10/1/2021

**Critical Review of the Literature Course Project**

***Critical Review of (Teaching Cybersecurity to Criminal Justice Majors)***

Brook Nodeland, Scott Belshaw, and Mark Saber, 2019

**Summary**

The authors identified an area of weakness in criminal justice programs at the college level. They evaluated several colleges and universities throughout the United States and found that most were lacking in teaching cybersecurity in their criminal justice programs. Because cyber-crimes are continuing to grow, it has become a top concern for criminal justice professionals. The lack of cybersecurity education has hampered their ability to handle these crimes (Nodeland et al., 2019).

It is the opinion of the researchers that institutions of higher learning must develop, implement, and promote cybersecurity courses. Researchers have developed a cybersecurity course recommendation complete with a suggested syllabus for incorporation into criminal justice programs (Nodeland et al., 2019).

**Article Analysis**

This study discussed the history of cybersecurity in education and addressed many of the issues that current criminal justice students face. For example, a student who desires a focus on cybersecurity will have to go outside the criminal justice department. They may have to look at courses in computer science, engineering, or business. The problem is that the courses from these departments aren't geared toward criminal justice. The student won't find material for developing skills in evidence collection, preservation, and legal, environmental factors (Nodeland et al., 2019).

I somewhat disagree with this assessment. In my MS program in information assurance and cybersecurity, we covered evidence collection and preservation. The program also had a section on how not to contaminate data by using copies or sandboxes. My point is that some college cybersecurity programs do consider evidence preservation and other criminal justice concerns. Also, a colleague of mine received her MS in cybersecurity at the University of Southern Florida. Her program had a whole section on forensics.

Additionally, where I teach (Pasco Hernando State College), we also have courses in forensics. The courses are at the AS and BS levels. I do believe that many programs have started to consider cybersecurity from a criminal justice perspective.

Another area of concern regarding the research methodology was the source material that the authors used to come to some questionable statements. For example, they state that cybersecurity has not been taken seriously because students are uninterested. The uninterest was due to a perception of low monetary reward (Nodeland et al., 2019). The sources cited were published in 2002 and 2000. I would argue that this is no longer correct. The researchers should've known since it had been almost twenty years ago.

Areas, where the research shined were in the area of recommendations for new cybersecurity programs in criminal justice. They said that programs should offer experiential learning (Nodeland et al., 2019). In my opinion, only through hands-on practice will a cybersecurity student learn how to perform a task. It is a combination of knowledge and muscle memory.

Another observation they made was noticing that there is a gap between law enforcement and cyber threat responses. They recommend that criminal justice experts bridge this gap (Nodeland et al., 2019). Criminal justice programs have to educate students with the latest knowledge and methodology to bridge the gap.

**Practical Applications**

The research clarified that criminal justice programs must create and promote a cybersecurity component to the security branch. This applies to any college or university that has a criminal justice department.

Graduates with this background will close the gap between criminal justice agencies and cybersecurity professionals with technical skills. Departments must develop an appropriate cybersecurity curriculum to teach these skill sets.

The curriculum should include; cyberspace, cybercrime, cybersecurity laws, policies, cyberterrorism, harassment, and stalking (Nodeland et al., 2019). If colleges and universities do not implement cybersecurity courses into their programs, criminal justice students will be ill-fitted for the future. The gap between law enforcement and technology experts will only continue to widen.

Barriers to implementation are cost and knowledgeable personnel. All new programs have a price. Due to budget tightening, it is challenging to convince the administration to create new courses and curriculum material. However, these costs are justifiable and necessary.

It is critical to start hiring persons with strong cybersecurity technical backgrounds to teach the new curriculums in the department of criminal justice.

A possible unintended consequence to consider when implementing cybersecurity into the program is that it may drive some students away because of the technical nature of the cybersecurity course. For this reason, I recommend the cybersecurity courses be a concentration or a focus rather than a requirement.

***Critical Review of (Why digital forensics is not a profession and how it can become one)***

Michael Losavio, Kathryn C. Seigfried-Spellar, and John J. Sloan III, 2016

**Summary**

The researchers argued that digital forensics (DF) is not yet a profession. They identified several reasons that impede the advancement of DF to this status. Primarily a perception of the low social status of the clients and the uniqueness of this field with the division of labor has held back the advancement of DF (Losavio et al., 2016). The researchers argued suggestions for promoting DF.

**Article Analysis**

The authors did an excellent job of defining DF's objective. It is the search for truth. I especially liked the explanation of the DF process. It begins with interconnected systems in computer science, engineering, information systems, and communications. The process will ultimately end up in the judicial system, concluding in the courts (Losavio et al., 2016).

Additionally, they explained that public trust in the DF experts is paramount. The DF experts are expected to contain competency in their discipline and practice ethical behavior (Losavio et al., 2016). I feel that this is particularly challenging with the current distrust of science by the public.

In the paper of DF, the researchers stated some court cases had been dismissed due to a lack of standardized tools and forensics procedures. There are some standardized government tools, but more are needed (Losavio et al., 2016).

The researchers also claimed DF lacks in tools and procedures. They might have expanded a bit more on exactly which areas in DF are lacking.

An area of DF that was detrimental to its becoming an occupation was the claim of a high burnout rate due to practitioners working on data of a sexual nature (Losavio et al., 2016). The possibility of working on the suspect's hard drives that contain sexual content is something that I have considered. In the future, I would like to assist law enforcement in the area of forensics or cybersecurity. However, I wouldn't help in the area of sexual crimes. Some things cannot be unseen. I do not want any images of that nature burned into my mind.

A surprising statement was the claim that there are no DF codes of ethics enforced through civil and criminal law. There are also no regulatory practices (Losavio et al., 2016). A discrepancy like this will have to be addressed for DF to be considered an occupation.

**Practical Applications**

A concern from this research was the possibility of misuse of the tools. Because the tools for DF are so technical, it is difficult to have public or private scrutiny. There is also a possibility of specific devices having proprietary technologies that a jury or the public would not be able to test. Reliability becomes an issue as it may not be possible to test or confirm results (Losavio et al., 2016).

The strength of DF may favor the prosecution because the tools may only be available to the prosecution and government officials who can afford them.

An ethical code must be developed and then accepted by the public and industry. Ethics will limit the possibility of misidentifying or possibly leading to incorrect conclusions about a suspect.

Barriers to implementation are cost and time. Many of these tools will be too expensive for either particular defense to purchase and could lean towards anyone who has the means to afford them. Thus, money may sway the balance of justice.

Furthermore, suspects convicted of crimes based on a forensics analysis that is biased or unreliable is a possible unintended consequence.

***Critical Review of (A principlist framework for cybersecurity ethics)***

Paul Formosa, Michael Wilson, Deborah Richards, 2021

**Summary**

The study posits that there is no agreed-upon cybersecurity ethical framework. The researchers in this study seek to address this shortcoming.

Researchers examined ethical issues that arise from four common cybersecurity attacks; penetration testing (pen), distributed denial of service (DDoS), ransomware, and system administration (Formosa et al., 2021). Responses to the attacks by victims and the cybersecurity community were examined using five ethical principles—the principles of beneficence, non-maleficence, autonomy, justice, and explicability (Formosa et al., 2021).

Finally, the study proposes the principlist ethical framework for cybersecurity.

**Article Analysis**

Authors examined cybersecurity attacks on civil cybersecurity infrastructure. Attacks on user financial, medical, or other sensitive information were the focus. These data breaches may cause psychological and social harm (Formosa et al., 2021).

Another area studied was system administrators' and programmers' role in making ethical decisions to control hate speech or misinformation. This type of ethical decision-making impedes freedom and the right to ethical privacy concerns (Formosa et al., 2021).

I found this fascinating because of our political environment. For example, Facebook system administrators examine user posts and determine what to post and what not to post, even flagging certain statements as inflammatory or racist, or untrue. The ethics of these types of decisions by the system administrators are questionable.

One limitation of the study was limiting the scope to civil. I find the broader context of state-sponsored cyber surveillance or cyber warfare more interesting. I feel that limiting the discussion to only civil cases was disappointing. How can we examine ethics without examining the vulnerability of the threats posed by foreign governments? Attacks on our election processes and results come to mind.

The researchers identified several ethical principles based on the five cybersecurity ethics categories: non-maleficence, justice, explicability, maleficence, and autonomy (Formosa et al., 2021). The moral principles and their sub-categories were effectively displayed in a helpful chart for cybersecurity professionals to consider.

The research demonstrated the danger of moral disengagement from purely technological decision-makers, and ignoring ethics increases security problems. Results showed system administrators engage in trade-offs to solve problems.

I feel that developing an ethical principle framework was accomplished with this research. There is a need for more ethical training and logical decision-making in the field of cybersecurity.

**Practical Applications**

A lesson learned from this study was the need for an ethical framework for cybersecurity. I was unaware that this was an issue. The recommendation of using the principlist ethical framework was a solid suggestion. This framework borrowed heavily from applied ethics, bioethics, AI, ethics which made definite sense.

The weakness of the study was that those with means would have access to more robust cybersecurity tools. The results might be biased without an ethical framework.

Another weakness of not having an ethical framework was that programmers and system administrators might bias the results, unbeknownst to the general public. Today this is visible via Facebook and Twitter canceling policies.

The most significant opportunity from the study is that of instilling an ethical framework in cybersecurity. This study and other studies that support the conclusions should promote cybersecurity policy changes in all organizations.

Another opportunity is to educate the public on the potential biases of system administrators in large technology domains. A more informed public could help to influence positive change.

A barrier to implementation might be resistance to change by organizations, especially system administrators who are reluctant to give up power.

Acceptance is also a barrier to implementation. For the principlist ethical framework for cybersecurity to be implemented, public and private organizations would have to be broadly accepted.

An unintended consequence for the principlist ethical framework for cybersecurity could be a new layer of bureaucracy that slows down progress. The cost might also be an unintended consequence that has to be burdened by organizations.

***Critical Review of (Criminal law protection of cybersecurity considering AI-based cybercrime)***

XiaoLing Wang, 2020

**Summary**

The study by Dr. Wang argues that artificial intelligence is invading cybersecurity at an alarming rate. This type of cybersecurity is a much more severe threat to national security and other public interest (XiaoLing, 2020).

He asserts that there must be a new strategy within the judicial system to address artificial intelligence cybercrime. In China, there is a high threshold for the conviction of those accused of cybercrime. The study proposes to adjust the threshold due to the substantially more dangerous AI cybercrime (XiaoLing, 2020).

The study also suggests a balance between justice and legislation. Objective interpretation is the methodology suggested for addressing the balance. Accurate interpretation emphasizes fairness and justice by looking at the circumstances of the crime (XiaoLing, 2020).

Finally, Dr. Wang argues that other cybersecurity and criminal law studies must address the rapid advancement of AI-based cybercrimes (XiaoLing, 2020).

**Article Analysis**

The article made a solid point about the rapid advancement of artificial intelligence in cybersecurity. It did an excellent job of defining the areas in which cybersecurity impacts our national security and infrastructure. The article explained that cybercrime is not a single legal issue but a compound issue (XiaoLing, 2020).

I felt that Dr. Wang did not expand on what a compound legal issue meant. He could have expanded on the compound legal statement with some concrete examples.

The study also presented that society is moving on to the network where nearly everything we do is in the network to the point that it reflects actual reality. Because of this, we are much more sensitive to cyberattacks than ever before. AI also exaggerates these attacks.

His use of the term network was a little bit confusing to me because the network in the United States has a meaning that involves a series of computer systems, usually inside of an organization that is inter-connected. When Dr. Wang says the network, he is talking about what most people consider "cyberspace." The use of the term cyberspace would remove confusion and ambiguity from the article.

The article made an interesting assertion stating that the legal rules of the natural world will need to enter the virtual world, or what the paper calls network space (XiaoLing, 2020).

I believe it required a broader explanation. Although Dr. Wang explained that most of our lives are conducted in network space, he doesn't sufficiently explain how legal rules would enter this virtual world.

He also proposed that we must criminalize even the act of preparing for cyber crimes and create a new crime that he called "helping cybercrime" (XiaoLing, 2020). He does not explain or expand upon what preparing entails. I feel that he might be arguing for criminalizing the act of preparing to commit a crime. I believe this would be unconstitutional in the United States.

Dr. Wang stated concern with the potential for expanded charges and possible aggressive enforcement of the law. He addressed this by leaning on objective interpretation theory.

This theory involved a legal interpretation that explored the law within social development from the legal norms. He described it as a fair interpretation that seeks fairness and justice. The law should look at the essence of the crime rather than just the reality. In other words, the spirit of the law and not just the letter of the law.

He also argued that the objective interpretation would pay closer attention to the circumstances of the crime, particularly the severe circumstances. How this would remain objective was unclear.

**Practical Applications**

The study shed light on the need to review AI cybercrime judicial processes. Cybercrime is a multifaceted type of crime. The Judicial system must prepare itself for this new threat.

Objective interpretation theory may be the methodology for the judicial system. I should provide a fair and balanced punishment.

We risk not handing out the appropriate punishment for AI-based severe cybercrimes without an objective review of how the judicial system handles cybercrime. It is essential to understand AI-based cybercrimes are a much more potent threat to national security and infrastructure than basic cybercrime.

This study presents an opportunity to reflect carefully on how the US handles cybercrime. We must determine if implementing a new methodology is needed. The study also provided a chance to reflect on the need for further research in the area of AI cybercrime's

A barrier to implementation might be the lack of understanding of cybercrimes in general, but especially AI-based cyber crimes.

Furthermore, the judicial system's slow speed and reaction time versus the lightspeed movement of AI-based cybercrimes could also be a barrier.

One possible unintended consequence is over the sentencing of AI-based cybercrime partners.

***Critical Review of (Survey of intrusion detection systems: techniques, datasets and challenges)***

Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman, 2019

**Summary**

In this study, the authors carefully reviewed signature-based intrusion detection systems (SIDS). They also looked at anomaly-based intrusion detection systems (AIDS).

Additionally, the researchers examined the taxonomy of contemporary IDS and took a careful look at the data sets used for detection. The authors presented a few evasion techniques used by malicious actors to avoid detection(Khraisat et al., 2019).

Lastly, the authors discussed the future challenges computer systems will face becoming more secure (Khraisat et al., 2019).

**Article Analysis**

The article cited other articles heavily. The citations were probably due to the number of complex definitions and processes that needed defining. In any case, I didn't find much in the way of original research.

I found that their collections or aggregate data from previously published research could benefit someone interested in intrusion detection systems. In particular, I liked their table that compared the IDS datasets with accompanying results and observations.

The researchers also did an excellent job in explaining the advancements in cybercriminal intrusions. They made a strong argument for creating new or advanced intrusion detection systems due to the sophistication of attacks. I also appreciated the in-depth discussion on the advantages and limitations of each intrusion detection system.

Unlike most sources for intrusion detection systems, this research emphasized the limitations of each one, such as AIDS being excellent at catching zero-day attacks while simultaneously producing false positives (Khraisat et al., 2019).

A limitation of the research was that all of their studies examined public data sets. For an accurate evaluation, private datasets from the industry are necessary.

Furthermore, although the researchers briefly discussed polymorphic attacks, I would have liked a more in-depth discussion because, from my studies, polymorphic malware is significantly more powerful, difficult to detect, and also more highly utilized by malware designers.

**Practical Applications**

The lessons learned from this research are that a much better method for collecting datasets for IDS comparisons is necessary. It also revealed that updated documentation on IDS and AIDS along with testing results is needed.

Opportunities for testing IDS and AIDS while tracking malware are present. More research in these areas is required.

As usual, barriers to implementation include funding, public support, or buy-in along with political champions.

An unintended consequence of implementation might be an over-locked down system that becomes slow and classifies everything as a threat.

***Critical Review of (Regulating Cybercrime through Law Enforcement and Industry Mechanisms)***

Thomas Holt, 2018

**Summary**

This research examined cybercrime issues within the judicial and social context. It did an excellent job of defining cybercrime and its sub-categories. Where the study shined, however, was in the discussion of efforts by industry to combat cybercrime. I also found the section on challenges law enforcement and the criminal justice system valuable (Holt, 2018).

The ability of cybercriminals to hide both their location and identity with computer tools has greatly hampered investigations. Another issue that causes problems for law enforcement is that many of the criminals reside and commit crimes from foreign countries where no extradition treaties exist.

Researchers also revealed that a psychological component occurs where the victim becomes compliant. Victims are either embarrassed to report their case or do not believe law enforcement will look seriously at it. Victimization statistics are undercounted as a result. Studies have shown that police officers do not feel motivated nor prepared to investigate cybercrime in most cases (Holt, 2018).

Another gem in the study was the assertion that the private sector has taken on a law enforcement component to deter cybercrimes in some areas. They have been very successful, such as minimizing the rates of piracy. They have also collaborated with ISP providers to send out cease-and-desist letters to those whose IP address matches attempts to pirate media.

Another action by industry was the creation of corrupted files, also known as junk information that they distribute on filesharing services to help confuse anyone who tries to download illegal content (Holt, 2018).

In an extreme case, Indian film studios engaged in denial of service attacks against known piracy sites after they did not respond to requests to remove their content. Denial of service attacks are illegal (Holt, 2018).

Concerns about the industry's role in law enforcement have raised some problems because the industry has no obligation to the general public, and their motives might be suspect. There are also questions regarding what the industry will do with certain private information obtained during law enforcement (Holt, 2018).

**Article Analysis**

This research did an excellent job explaining many types of cybercrime, such as cyber trespass, piracy, and fraud. However, I found the discussion about the role of industry to be most interesting. The article states that the efforts by industry to limit cybercrime have been most influential in slowing crimes but not in stopping them.

The article also expressed concern about the industry overstepping the legal system in its efforts. It would have been good if this article had discussed lawsuits or retribution from citizens or hacker groups against the drive for overstepping some of these bounds.

Researchers also mentioned the collection of personal and private data by industry to enforce legal media piracy protections. Again, I would've liked to have read the information regarding retribution against the industry because of these actions.

It is hard to argue that the industry does not have a place in enforcement. According to the article, it is more agile and has much larger budgets, and, therefore, is in a better position to respond to offenses. The industry owns almost all the platforms and technology used for these crimes.

The section of the research that focused on the phenomenon of victim compliance was fascinating. I would have liked to have read a lot more discussion about this phenomenon. The researchers did not go into very much depth on this topic. Victimization is probably undercounted because of the lack of reporting by the victims. I feel that this entire section could be a vast research area.

Another limitation of the research was the lack of state-sponsored cyber warfare and cyber-surveillance. I acknowledge that these areas are vast; however, they should be briefly addressed.

**Practical Applications**

The most vital lesson learned from this research was the need for knowledge and training of all stakeholders. Law enforcement is not adequately trained in cybercrime. Organizations need to make a robust inquiry about the police's qualifications and consider contacting the federal authorities. Federal law enforcement is better suited for cybercrime (Holt, 2018).

Organizations should be aware that the prosecution of cybercriminals is challenging and may not result in any convictions due to the geographical location of the cybercriminals. (Holt, 2018)

Weakness in an organization may be the lack of cyber attack insurance. It will help to offset the cost of an attack on a business. If a company holds sensitive client data on its databases, it must have this insurance (Holt, 2018).

Barriers to implementation are funding, acceptance, and the awareness that cybercriminals may not see justice. Unfortunately, the prosecution rates are low (Holt, 2018).

An unintended consequence is the continued merging of the industry as law enforcement to stem cybercrime. Ethical questions arise due to the unregulated access to personal data due as industry responses to cybercrime (Holt, 2018).

***Critical Review of ( Zero-day responsibility: The benefits of a safe harbor for cybersecurity research)***

Charles Alek, Emery (2017)

**Summary**

The paper by Mr. Emery focused on the problem of regulating zero-day exploits. (Emery, 2017). He argued that the market for zero-day exploits is unregulated. He also claimed that although some exploits go to malicious actors, most are sold to intelligence agencies of the United States (Emery, 2017).

The main point of this research was to argue that regulation of the zero-day exploits market is critical for national security. However, this regulation must not take the form of enhanced criminalization or the expansion of the computer fraud and abuse act (CFAA). Instead, he makes a compelling argument for shifting the burden of regulation to tort law. He believes that tort law will be a much more effective model for enforcing the regulation. Tort law has more flexibility, is easy to administer, and may have high stakeholders' acceptance *(Emery, 2017).*

Another point the author makes is that, unlike criminal law, tort law will not make malicious actors go further underground and anonymous, thus making the prosecution more difficult (Emery, 2017).

**Article Analysis**

the research begins with a background discussion on computer networks and vulnerabilities. Within this discussion, two statements stood out. The first one was that computer networks are by their very nature vulnerable to attack. The second statement that stood out was that the timeline for vulnerability starts as soon as a developer releases the product. If that product contains a vulnerability, the computer security professional may find it and exploit it (Emery, 2017).

I agreed with both statements. I feel that there is a perception in the public consciousness that computer networks can be completely secured. If a vulnerability is exploited, then it is the fault of the security technicians. After investigation, it may be the case that the security technicians did not do everything they needed to protect the sensitive material. However, the exploit often happens because of an unknown vulnerability or vector.

The second statement is also true. Once the software is released, malicious actors will immediately begin to examine for weaknesses or vulnerabilities. Unless a software developer is trained to think like a hacker and secures their software as they write it, vulnerabilities will exist.

Probably the most compelling argument that the author made was that zero-day vulnerabilities perform a potential benefit to society (Emery, 2017). As a cybersecurity expert, I have only ever looked at zero-day vulnerabilities as malicious and, therefore, undesirable. So, this statement of its beneficial use was interesting to me.

He argues that the benefit is that a zero-day vulnerability provides society the opportunity to prepare computer networks against attacks. The hardening that strengthens a network against attack will result. He goes further and includes the example of the Stuxnet virus used by the government to attack the infrastructure of an enemy country. Without vulnerabilities, this benefit would not have existed (Emery, 2017).

Regarding the use of tort law to regulate zero-day attacks, tort law would protect researchers who research vulnerabilities and zero-day attacks while also helping to guide malicious actors into compliance. His point was that if we continue to criminalize and expand upon the computer laws, malicious actors will only go deeper into the dark web and become even more anonymous, thus making the prosecution even more challenging (Emery, 2017).

I am also glad that he mentioned the safe harbor laws protecting researchers because it's something that I had not considered. He stated that the researchers in this field are likely to continue their work if they do not fear criminal liabilities. Fewer researchers will result in our country being less secure. For this reason, it is crucial not to broaden criminal law but rather to turn to tort law (Emery, 2017)

I found his arguments compelling. Consider that as things are today, there are few researchers in this field. If new talent is turned off, then it will be to the detriment of our national security.

**Practical Applications**

Organizations should consider that regardless of safeguards, technicians cannot wholly secure their networks. Now that doesn't mean they should give up, or the system administrator should be allowed to become complacent. Instead, it means to face and exploit with an open mind and then come to the conclusions that the data indicates.

The driving message in this research is our society must shift regulation to tort law rather than criminal law for the benefit of researchers and, inadvertently, our national security (Emery, 2017).

Organizations must have motivated and enthusiastic IT security personnel who tirelessly work on the networks. If this person becomes complacent or lazy, then the company's security is at risk. Vulnerabilities are ever-growing and often unknown.

As usual, the barrier to implementation is wide acceptance. There must be a paradigm shift in the thinking that we must criminalize all computer acts. This over-broadening concept will criminalize even researchers and academics. Therefore, a safe harbor law must protect both the researcher and entry-level cybersecurity experts (Emery, 2017).

***Critical Review of (The use of specialized cybercrime policing units: an organizational analysis)***

Dale Willits and Jeffery Nowacki (2016)

**Summary**

This paper examined the use of cybercrime units in policing from 3097 law enforcement agencies. Its primary concern was with an organizational analysis. The researchers reviewed 5324 observations over 2000, 2003, 2007, and 2013 from the law enforcement management and administration statistics (Willits & Nowacki, 2016).

Researchers examined the data through the lens of contingency theory, institutional theory, and Maguire's theory of police organizational structure. The study focused on a descriptive analysis using organizational correlates, environmental pressures, and the role of time (Willits & Nowacki, 2016).

The study revealed that public perceptions about police departments being unprepared for cybersecurity attacks might be incorrect. As time passes, cybercrime units continue to grow and become normal within police agencies. This is most likely the case for larger agencies and agencies with a much greater task scope to adopt broader technologies (Willits & Nowacki, 2016).

The paper demonstrated a correlation between cybercrime complaints and cybercrime units established by police departments. As expected, the larger agencies typically form the cybercrime units due to the larger volume of crimes and the greater access to resources and technical personnel (Willits & Nowacki, 2016).

The study also showed that police agencies had increased their cybercrime investigations over the years. In 2000, 51% of agencies did not investigate cybercrime, but by 2013, only 15.5% of agencies did not investigate cybercrime. This trend is expected to continue as cybercrime becomes more prevalent (Willits & Nowacki, 2016).

Another result from the study was that if an agency has more routine tasks, they are less likely to form a cybercrime unit(Willits & Nowacki, 2016).

Furthermore, the researchers conclude that cybercrime units will continue to become more common in the future. Still, the state-level agencies will have the most substantial need for cybercrime units due to the geographical nature of cybercrime being challenging to prosecute (Willits & Nowacki, 2016)

Lastly, this study did not examine whether the cybercrime units effectively combat cybercrime (Willits & Nowacki, 2016).

**Article Analysis**

Research results support the hypothesis that police agencies are becoming more technologically savvy and prepared to handle cyber cybercrime. The study qualified this statement by saying that the larger agencies are most likely to have these departments. The smaller agencies are still in a struggle with this.

In this study, the dependent variable was whether or not an agency had a crime unit or did not. Thus, all the data was specific towards those with a crime unit cybercrime

The law enforcement management and administrative statistics surveys (LEMAS) provided the survey data. The surveys show items that regard the organizational characteristic, and this would include cyber policing units.

A significant weakness in the LEMAS surveys is not including sufficient cybersecurity questions. Furthermore, many departments do not fully complete the surveys; thus, surveys often miss questions or answers (Willits & Nowacki, 2016). Sometimes there is not a standardized way that agencies will answer a question. Confusion or bias in the reported information in this design is likely.

And another hurdle that continues to rear its head is the jurisdictional question of who has the authority to investigate and prosecute offenders over large geographical distances—the effect results in limiting agency cybercrime decision making (Willits & Nowacki, 2016).

The researchers also acknowledge that the inconsistency in the survey questions formats and variables make it impossible to look at a time series investigation into the police organizational structure.

In conclusion, the study demonstrates that organizational factors such as the size, agency type, whether or not they have the technology savviness, and ability will determine if a cybercrime unit is established or increases in size.

**Practical Applications**

lessons learned from this research were that the public perception of law-enforcement agencies as not adequately prepared for cybercrime might be incorrect. Also, Organizations may need to recognize that the pressure to create a cybercrime unit may come from institutional establishments pushing normative policing practices and not necessarily an environmental demand for more cybercrime investigations.

With the public interest in cybercrime, the pressure will likely continue to mount for specialized cybercrime units in more organizations. However, it is essential to remember that these cybercrime units have not demonstrated measurable effectiveness (Willits & Nowacki, 2016). Issues such as the jurisdiction and geographical distance between offenders and victims will hinder investigation and prosecution.

Administrators should edit the LEMAS to include more cyber security-specific questions. Organizations should make every effort to answer questions on the survey, leaving no blanks on the responses.

Analytical and technical expertise will continue to drive state and federal cybercrime unit growth and viability due to their ability to handle broad geographical areas (Willits & Nowacki, 2016).

Barriers to implementing more robust policies and organizational structure to support cybercrime are a lack of funds: administration buy-in, and the perception of police technological ability and efficacy (Willits & Nowacki, 2016).

***Critical Review of (Threats to privacy in the forensic analysis of database systems)***

Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine (20)

**Summary**

Researchers demonstrated the persistence of unwanted data in databases (Stahlberg et al., 2007). The authors performed experiments that resulted in confirming the unsecured data. Databases preserved data in table storage, transaction logs, indexes, and other database structures (Stahlberg et al., 2007).

To address the problem of persistent data, the researchers created a set of system transparency criteria. The criteria handled the issue of data retention by bounding the data in time. They also increased the database transparency by developing techniques to ensure record and log deletion (Stahlberg et al., 2007).

**Article Analysis**

This paper was significant because it examined privacy and confidentiality threats in commonly used database systems. The paper mentions that deleted Enron team member emails were discovered on hard drives and then used against them in court (Stahlberg et al., 2007).

Even financial and medical records were quickly found on decommissioned hard drives. Persistent data is a threat to privacy and even violates some laws (Stahlberg et al., 2007).

Forensics analysis is the process of recovering data. The problem arises when an unauthorized party or malicious actor uses forensic analysis to recover sensitive materials from decommissioned hard drives (Stahlberg et al., 2007).

The objective of the research was to design a database system that would resist unwanted forensic analysis. The main goal here was to establish forensically transparent procedures. The method and accessibility should retain data through a legitimate interface. However, hidden data should never be recovered or available to unauthorized actors (Stahlberg et al., 2007).

The research centered on how data is preserved in database tables, transaction logs, etc. After examining the results of their experiments, the researchers proposed internal design changes that would protect databases and remove persistent data (Stahlberg et al., 2007).

I found this to be fascinating due to no one studying unintended retention of the sensitive data before. The researchers introduced the term "forensic transparency" to satisfy this objective. A database system must have three desiderata to achieve forensic transparency; clarity, purposeful retention, and complete removal. Forensic transparency would be challenging for malicious actors to access data (Stahlberg et al., 2007).

The researchers did a significant amount of work testing their theories on different databases. The databases consisted of MySQL, DB2, SQLite, InnoDB. I found this of great interest because I have used all but one of these databases. AS a senior database administrator, I have written extensive queries across many databases (Stahlberg et al., 2007).

Their research showed me a deeper layer of database systems. For example, temporary tables are created inside the system during the delete update and insert queries, and data is written into the FS–slack file. Within this file, data will remain persistent for quite some time.

Additionally, all the database systems run a vacuum command that reorganizes the table storage. The process of overwriting tuples and reorganizing the system pages creates another file called FS–slack. It contains persistent data for an extensive amount of time (Stahlberg et al., 2007).

The researchers describe DB-slack as unmanaged work that expired and is inaccessible to legitimate users. FS-slack is an unmanaged storage file. However, it is considerably more significant than the DB-slack. Both of these retain persistent data (Stahlberg et al., 2007).

The researchers note that many software systems designed to secure the databases will use encryption. The problem is encryption increases expense significantly. It expenses the amount of load on the processor and memory and impacts system performance; thus, it is not ideal for securing persistent data (Stahlberg et al., 2007).

A recommendation from the researchers is to delete the whole transaction log. The process will not impact system performance. I would have liked them to discuss this issue in more detail because the transaction logs are required for restoration, especially after a system failure. A more detailed explanation of the process to determine when transaction logs are not needed would be good (Stahlberg et al., 2007).

In my own experience, I would often delete the transaction log after one month because the transaction log grows considerably over time and takes too much backup storage. It also increases the amount of time to back up the database significantly (Stahlberg et al., 2007).

Another recommendation researchers made was securing the B – tree operations. This is a modification to the code. This code will overwrite by modifying this code and allow different SQL commands such as insert, update, and delete to run without creating a persistent data set in the slack files. I believe this is an excellent recommendation. However, it requires work from the manufacturers of the database systems (Stahlberg et al., 2007).

In my opinion, the researchers did an excellent job in their evaluation of the different database systems. Their primary focus for achieving forensic transparency was to address the slack data in the table storage and the persistent data in the transaction logs (Stahlberg et al., 2007).

Their conclusions were sound. They gave a compelling demonstration of major database systems commonly used that fail to remove data after deletion and leave remnants of operations and data allocation and storage. They also demonstrated that these mainstream databases make unnecessary, redundant copies of the data items, and they will persist in the system for a significant amount of time. I was also impressed with their addressing the performance issues of the system while implemented solutions. Typically, performance is not addressed when discussing database security is usually considered just the cost of securing the database.

**Practical Applications**

This research taught critical lessons for organizations that use databases. Entities should be aware that their data is not as secure as they think it is. Part of this is the fault of the database vendors. The vendors often sell their products with broad statements about security protection, encryption, etc. No mention is made whatsoever about persistent data. If not for sensational cases that make the mainstream media, most of us would not even be aware that data is easily retrievable from databases.

Research revealed the technical process by which forensic investigations retrieve persistent data. This unveiling of the forensic process made the potential for continuous data accurate. The average administrator can now view and understand the process.

Organizational administrators must secure databases to protect against threats by deleting the transaction log. Additionally, vendors must make the recommended modifications to their database products.

Barriers to implementation are as follows. First, as is almost always the case, funding is a significant impediment. The cost to make any of these changes would most likely be high.

Secondly, buy-in by the business organizations would not be difficult once the vulnerabilities. I believe buy-in may be achievable; however, buy-in by the database vendors would be considerably more challenging.

Criminal activity may be challenging to uncover and prosecute as an unintended consequence. And, of course, it could lead to additional crimes.

***Critical Review of (Digital forensic analysis of hard disk for evidence collection)***

Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine (20)

**Summary**

After examining multiple open-source forensic tools and the literature regarding digital forensics, the authors identified weaknesses in the current processes. They then wrote a more robust algorithm for performing digital forensics on a hard disk. The objective was to recover documents and files (B. Meshram et al., 2018).

The authors' application had a simple three-step process for the recovery of deleted files from NTFS; acquisition, analysis, and reporting. The tool could find hidden files and documents in the ADS free spaces, such as file slack and volume slack. Additionally, the researchers were able to identify who deleted, accessed, or altered any files (B. Meshram et al., 2018).

Lastly, their system generated a report with all the collected evidence, metadata, and the recovered files (B. Meshram et al., 2018).

**Article Analysis**

The research was very informative. The authors did an outstanding job of reviewing the literature. They also did an excellent job of identifying the weaknesses in the current forensics analysis tools—the most substantial contribution. The authors suggested a new methodology along with proof of concept for the recovery and analysis of deleted files (B. Meshram et al., 2018).

Instructions on their algorithm were very useful and easy to follow. I'm confident that if I wanted to replicate this algorithm I could do so in any number of languages.

In my opinion, this research only handles information that has been deleted or purposefully hidden in allocated sectors of the hard drive. The study does not answer how to recover heavily encrypted data or data hidden in plain sight using Steganography methodology. I am confident that with little effort I could defeat their system.

The authors would've written a more substantial paper had they identified these two main areas or areas of weakness and the need for further research in this area.

**Practical Applications**

Although this application was written to capture malicious activity on a system, the authors might have pointed out that legitimate reasons for hiding data could use this research. Organizations that handle sensitive material should be aware that simply deleting their data or moving it to unallocated sectors on the drive will not sufficiently hide or delete the data.

An opportunity from this research is for law enforcement to have another tool that simplifies the process of forensic analysis and data recovery. Additionally, legitimate businesses and organizations can harden their data deletion and hiding techniques.

A barrier to implementing this algorithm is simply ignorance of how secure administrators might believe their data already is. A lack of education on the security of data on databases for organizations is the most substantial barrier to this application.

The only unintended consequence that I can think of regarding this research is that malicious actors also read current research on data analysis and retrieval. Any new study that reveals new techniques or algorithms will be analyzed. Afterwards counter measures will be programmed by malicious actors. As I already stated, because of their laid-out step-by-step algorithm, I am confident that with little effort, I could easily defeat this proposed methodology.

References

B. Meshram, B., The Society of Digital, I., & Wireless, C. (2018). Digital forensic analysis of hard disk for evidence collection. *International Journal of Cyber-Security and Digital Forensics*, *7*(2), 100-110. <https://doi.org/10.17781/P002372>

Emery, A. C. (2017). Zero-day responsibilty: The benefits of a safe harbor for cybersecurity research. *Jurimetrics*, *57*(4), 483-503.

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, *109*. <https://doi.org/10.1016/j.cose.2021.102382>

Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science*, *679*(1), 140-157. <https://doi.org/10.1177/0002716218783679>

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1-22. <https://doi.org/10.1186/s42400-019-0038-7>

Losavio, M., Seigfried-Spellar, K. C., & Sloan Iii, J. J. (2016). Why digital forensics is not a profession and how it can become one [Article]. *Criminal Justice Studies*, *29*(2), 143-162. <https://doi.org/10.1080/1478601X.2016.1170281>

Nodeland, B., Belshaw, S., & Saber, M. (2019). Teaching cybersecurity to criminal justice majors. *Journal of Criminal Justice Education*, *30*(1), 71-90. <https://doi.org/10.1080/10511253.2018.1439513>

Stahlberg, P., Miklau, G., & Levine, B. (2007, 2007). Threats to privacy in the forensic analysis of database systems. SIGMOD/PODS07: International Conference on Management of Data, Beijing china.

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: an organizational analysis [Article]. *Criminal Justice Studies*, *29*(2), 105-124. <https://doi.org/10.1080/1478601X.2016.1170282>

XiaoLing, W. (2020). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, *1533*(3). <https://doi.org/10.1088/1742-6596/1533/3/032014>