

William Spilsbury

Prof. Matthew Umphlet

CYSE 200T

26 November 2025

Analytical Paper – CIA Triad

In this paper, I will discuss the CIA triad and evaluate it to identify and address potential future long-term ramifications. The CIA triad is a simple model that forms the foundation of cybersecurity system development. It consists of three layers: confidentiality, integrity, and availability. Confidentiality refers to the idea that data needs to be kept private. Integrity is meant to keep data trustworthy and free from any sort of tampering. Availability is the assurance that, if needed, data is readily available to any employees or customers who need it. Potential problems that may arise surrounding the triad include: loss of public trust, compromised public records or evidence, long-term damage to the economy, increased vulnerabilities to national security, and many more.

Ramifications

One of the first issues I want to address is potentially compromised public records and digital evidence. Related to the integrity aspect of the triad, digital forensic evidence often lacks scientific validity. According to research by Radina Stoyvoka, she found that legislation does not enforce reliability assessments, which “results in routine admission of digital evidence without meeting digital forensics standards.” One solution Stoyvoka suggests is implementing DF methodology for more complex cases. She states, however, that this would be “redundant, costly,

and burdensome for practitioners.” DF procedures involve steps such as analysis, evaluation, and acquisition of digital evidence in legal and systematic proceedings to investigate incidents related to digital devices (Watson and Jones 2013). Stoyvoka writes that this procedure, along with formal verification by the court, is the most suitable method to address the issue of reliability validation within digital forensics. Returning to the connection to integrity, these findings show that digital evidence currently lacks integrity. It is a difficult problem to fix completely, and probably impossible. However, with proper verifications and assessments, we can begin to admit more reliable evidence into cases.

Next, issues with the availability side of the triad lead to long-term national security vulnerabilities. More specifically, cyber weaknesses within local governments. Governments located within rural areas and smaller counties are more at risk of breaches due to a lack of budget. They have a far lower response capacity and are not as readily available to uphold security as larger/wealthier counties. In an article published by Charles Harry, he researched this exact issue. Harry found that common vulnerability exposure (CVE), which measures attack surface diversity and severity, does not correlate with exploitation likelihood. From his publication, you can also take away that people who rely on these government services may be harmed at a disproportionate rate due to officials not fairly assessing cyber risks. These issues, along with potential DoS attacks or ransomware, directly compromise availability. To combat this problem, Harry suggests an open-data method in order to measure attack surfaces of counties across the U.S. These will allow locals to better understand their risks and allow for governments to plan against potential attacks.

Lastly, repeated cyberattacks and breaches against the government demonstrate a lack of confidentiality, leading to a decline in public trust. In an article published by Ryan Shandler and

Miguel Alberto Gomez, they examine how perceptions and values shift toward the government due to cyberattacks. Their surveys found that cyberattacks cause a “precipitous drop in public trust,” with dread and anger fueling these emotions. Shandler and Gomez also argue that these “societal risks” of declining trust are “more insidious, long-term, psychological,” than physical destruction. This highlights how vital public trust is and how a lack of confidentiality can slowly but profoundly undermine a nation’s foundation. As the need for cybersecurity increases daily, it would be reckless for countries not to allocate nearly as much funding to these security measures as they do to the military. While the article does not suggest a detailed solution, there are some simple ones to consider. The simplest being an increase in funding and education within the field. With more knowledgeable specialists and money to work with, we can try to prevent more breaches and increase public trust.

Conclusion

The ramifications involved around the CIA triad can be as serious as national security risks and a complete loss of public support. While this model is the simplest way to build a cybersecurity system, it is also the easiest one to examine for problems. Integrity failures threaten court cases and public records; weaknesses in availability put small communities at risk, leading to national security issues; and breaches in confidentiality weaken the trust between the public and government institutions. Research articles suggest that issues stemming from local to national governments must all be observed. This may sound simple, but ignorance and an overall lack of urgency surrounding these issues pose a potential threat to every citizen in the country.

Work Cited

- Stoyvoka, Radina. "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence." *Science Direct*, Computer Law & Security Review, Sept. 2021, www.sciencedirect.com/science/article/pii/S0267364921000480.
- Watson, David, and Andrew Jones. "Chapter 9 - Case Processing." *Science Direct*, Digital Forensics Processing and Procedures, 2013, www.sciencedirect.com/science/chapter/monograph/abs/pii/B9781597497428000091.
- Harry, C., Sivan-Sevilla, I., & McDermott, M. (2025, January 17). *Measuring the size and severity of the integrated cyber attack surface across US county governments*. Oxford Academic. <https://academic.oup.com/cybersecurity/article/11/1/tyae032/7959399>
- Shandler, Ryan, and Miguel Alberto Gomez. "The Hidden Threat of Cyber-Attacks – Undermining Public Confidence in Government." *CyberIR@MIT*, MIT Political Science Department, 2022, cyberir.mit.edu/site/hidden-threat-cyber-attacks-undermining-public-confidence-government/.