8-2023

Applying Normal Accident Theory to Ideological and Nation-State-Sponsored Cybercrimes

Thomas J. Holt

National Counterterrorism Innovation, Technology, and Education Center

Applying Normal Accident Theory to Ideological and Nation-State-Sponsored Cybercrimes

August 2023

Research Team
Thomas J. Holt *Michigan State University*

NCITE
A DHS CENTER OF EXCELLENCE

About the Report. This project aims to explore a new perspective on cyberattacks by applying normal accident theory, typically used to analyze complex system failures, to the realm of cybersecurity. The goal is to gain insights into the factors contributing to cyberattacks and identify potential strategies to prevent and mitigate them. Applying normal accident theory to cyberattacks reveals that while complete prevention is challenging, focusing on human and organizational aspects of cybersecurity can significantly reduce risks. Encouraging adherence to best practices and establishing cybersecurity audit and compliance entities are critical steps toward a more resilient cybersecurity landscape.

Questions about this report should be directed to Thomas Holt at holtt@msu.edu.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 20STTPC00001-03. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

About the Authors.

Thomas J. Holt is a professor in the School of Criminal Justice at Michigan State University. His research focuses on computer hacking, malware, and the role of the Internet in facilitating all manner of crime and deviance. His work has been published in various journals including *Crime and Delinquency*, *Deviant Behavior*, the *Journal of Criminal Justice*, and *Youth and Society*.

About NCITE. The National Counterterrorism Innovation, Technology, and Education (NCITE) Center was established in 2020 as the Department of Homeland Security Center of Excellence for counterterrorism and terrorism prevention research. Sponsored by the DHS Science & Technology Office of University Programs, NCITE is the trusted DHS academic consortium of over 50 researchers across partner institutions in the U.S. and Europe. Headquartered at the University of Nebraska at Omaha, NCITE is a leading U.S. academic partner for counterterrorism research, technology, and workforce development.

Table of Contents

EXECUTIVE SUMMARY

Introduction. Cyberattacks are a pervasive threat in industrialized nations, impacting various sectors, including retail, government, and critical infrastructure. While existing research primarily focuses on technical solutions to detect and prevent cyberattacks, this paper explores a novel approach by applying normal accident theory to cyberattacks. normal accident theory, developed by Charles Perrow, helps us understand catastrophic failures in complex systems due to technological failures and human errors. The study aims to identify insights from this theory that can inform strategies for preventing cyberattacks.

Normal Accident Theory. Normal accident theory asserts that complex systems with high levels of complexity and coupling are prone to catastrophic failures. Complexity refers to how system components interact, while coupling indicates the interdependence of these components. Complex, tightly coupled systems are more likely to experience accidents that cascade and result in severe consequences. The theory has been applied to various contexts, including chemical plants, nuclear facilities, and financial markets.

Application to Cyberattacks. This paper extends normal accident theory to cyberattacks, recognizing that these attacks can have significant societal and economic impacts, despite not causing physical harm like nuclear meltdowns. Cyberattacks can lead to cascading failures, affecting various components and services within a network. For instance, a ransomware attack targeting one part of a network can disrupt unrelated services, leading to economic and personal harm.

Data and Methods. The study analyzes cyberattack incidents from the Extremist CyberCrime Database (ECCD) between 1998 and 2018, involving both nation-state and non-nation-state actors. Four diverse incidents were selected for analysis based on their complexity and impact.

Key Findings

1. **Complexity and Coupling:** Complex, tightly coupled systems are more susceptible to cyberattacks, often resulting in cascading failures that lead to significant harm.
2. **Vulnerabilities in Cybersecurity:** Tight coupling and linear processes in some incidents made them vulnerable to attack, highlighting the importance of robust security measures.
3. **Human Error and Organizational Dynamics:** Human errors and organizational factors played a role in some incidents, emphasizing the need for a cultural shift toward cybersecurity awareness and compliance.

Findings. The analysis of these incidents highlights common vulnerabilities and contributing factors to cyberattacks. Tight coupling of systems and linear processes in some incidents made them susceptible to attack. Some attacks were relatively simple and required minimal intrusion, while others involved more complex methods. Additionally, security tools sometimes failed to detect and mitigate attacks, and human error and organizational dynamics played a role in several incidents.

Discussion and Conclusions. The application of normal accident theory to cyberattacks underscores the importance of cybersecurity practices and protocols. While it is challenging to reduce the complexity and coupling of network systems, focusing on human and organizational aspects can significantly mitigate risks. Cultural shifts toward recognizing cybersecurity threats and adhering to best practices are necessary. Encouraging compliance with cybersecurity standards, increasing visibility of best practices, and establishing cybersecurity audit and compliance entities can help strengthen cybersecurity across public and private sectors, reducing the likelihood of successful cyberattacks and minimizing their impact. Ultimately, this approach can contribute to a more resilient cybersecurity landscape.

BACKGROUND

Cyberattacks are exceedingly common in industrialized nations, whether they result from economically motivated criminals, extremist actors, or nation-states. The scope of attacks has also increased, affecting retailers, government agencies, and critical infrastructure like hospitals and agricultural concerns (Holt, 2023). Computer science research on cyberattacks often focuses on technical solutions to better detect and reduce the likelihood of future attacks (Leukfeldt & Holt, 2019). While helpful, attackers frequently identify workarounds to defeat cybersecurity tools to ensure they can persist in compromising targets. Similarly, criminological studies on cybercrime largely focus on the characteristics of individual victims rather than the organizations and entities that are affected in major attacks (Leukfeldt & Holt, 2019).

There is a need to identify frameworks that may improve our understanding of cyberattacks and how they may be prevented, incorporating both technical and social risk factors. A potential model that holds promise involves normal accident theory, which assesses the likelihood of catastrophic failures in complex systems on the basis of technological failure and human error (Perrow, 1999). This study attempts to apply normal accident theory to cyberattacks performed by ideological and nation-state-sponsored actors in order to identify solutions that may reduce the risk of future compromise.

Normal Accident Theory

Most industrialized nations depend on complex systems that generate and maintain critical services and infrastructure, such as nuclear power plants and hydroelectric dams. A failure in one part of these systems can produce systemic, catastrophic failures if not detected and mitigated in time. For instance, the Three Mile Island nuclear power plant disaster in the U.S. was an excellent example of a catastrophic system failure (Perrow, 1999). In 1979, the Three Mile Island reactor in Pennsylvania experienced a partial meltdown that led to the release of radioactive materials into the environment. This incident occurred due to mechanical failures in a non-nuclear part of the plant, which led to a failure in reactor components which enabled the meltdown. The equipment failures were also compounded by flaws in information and control systems which left operators with little time to make critical decisions (Perrow, 1999)

Large-scale system failures can result from basic accidents in parts of a system and may be compounded by human decision-making by operators and system owners. As an example, the space shuttle Challenger was set to launch on January 28, 1986, despite the weather being slightly below potential tolerances for various parts of the shuttle infrastructure (Perrow, 1999). The decision to launch was made by NASA in conjunction with various parts and system manufacturers to more fully understand the potential risks posed by the temperature. During the launch, a series of small O-rings on a component of the launch system were too brittle from the ambient temperatures to handle the rapid changes in temperature and pressure upon takeoff (Perrow, 1999). The failure of this component caused an eventual cataclysmic explosion shortly after launch, destroying the shuttle and killing the crew. Sociologist Charles Perrow (1999) devised the normal accident theory as a way to understand when systemic failures occur in complex systems. The main argument of this theory is that accidents are common and should be expected. In any sort of system, the more complexity that is introduced, the more likely it is that any small accident that occurs will likely produce a catastrophic outcome.

There are two key factors that influence the complexity of a system: its complexity and coupling (Perrow, 1999). Complexity is related to the ways that system components interact in expected, unexpected, and unknown ways. Interactive complexity is used to describe a system in which multiple functions interact in unexpected and even unknown ways.

Regarding coupling, systems are tight or loose, depending on the degree to which they contain interdependent parts with time sensitive demands on one another (Perrow, 1999). The more systems are interdependent, and depend on sequential and timely operations to succeed, the more likely they are to be considered tightly coupled. These couplings can be loosened on the basis of substitutions and independence within the system to ensure continued functionality. Systems can also be linear and procedurally predictable, or nonlinear which involves complexity in order to complete their processes.

Researchers using normal accident theory have examined chemical plants and nuclear facility accidents, as well as other systems. These studies generally note that normal accidents occur when complex systems experience errors that compound one another or interact in unexpected ways. In addition, user error can play a role as system operators may be unable to observe or intervene when components fail (Perrow, 1999). In a broader context, the characteristics of an organization and its culture can also increase the risk of accidents by virtue of the ways they require employees to respond in the event of an error or system failure.

For instance, researchers noted that the introduction of additional safety features in chemical plants and nuclear facilities may actually increase the risk of normal accidents. By adding in additional redundancies, it appears that this increases the overall complexity of systems (Pidgeon, 2011; Yankun, 2021). In addition, an analysis of a market crash occurring in 2010 argued that some financial markets have reached high interactive complexity and tight coupling, leaving them prone to normal accidents (Min & Borch, 2021). The degree to which financial systems and trading platforms are now enabled by computers and automated analyses rather than humans creates significant interactive complexity and tight coupling on the basis of the speed at which transactions can occur. In an absence of stopgaps and redundancies, the presence of these tools can substantially increase volatility in markets and were attributed to the market value drop of over $1 trillion in less than 30 minutes for no apparent reason.

Limited scholarship applies normal accident theory to computer systems and networks in general (Maas, 2018; Nunan & Domenico, 2015). For example, Nunan and Domenico (2015) argued that a crash in the streaming service Netflix in 2014 was a function of the deletion of code by an Amazon Web Services engineer who did not validate their work with another colleague. Netflix was unable to diagnose this problem on their own and had to wait for Amazon to detect and resolve this problem (Nunan & Domenico, 2015). The lack of transparency, the complexity, and coupling of systems severely increases the risk of accidents.

This application of normal accident theory to computer networks and online activity in general suggests it may also be used to understand cyberattacks and their impact. Since virtually all aspects of modern life in western nations are dependent on the Internet, an attack that affects its operation could have dramatic effects on society. Though a cyberattack is unlikely to cause the same physical harm as a nuclear meltdown or chemical spill, the presence of Internet-enabled infrastructure to manage critical infrastructure creates the potential for a cyberattack to produce harm in physical space.

In addition, an attack that leads to the failure of systems, such as websites or online services, can be thought of in similar terms to a normal accident. Specifically, an attack affecting one component of a network can cause unintended consequences for other components and services. For instance, a ransomware attack that is designed to encrypt data on computers within a network can cause unaffected users to be unable to access sensitive data or services that are linked to those affected devices. It is also possible for a cyberattack to lead to the loss of sensitive data that could generate economic or personal harm to governments, businesses, and individuals. The failure of systems and services fits within Perrow's (1999) framework and could produce various policy recommendations to reduce future incidents.

DATA & METHODS

Thus, this study attempted to apply normal accident theory to a series of incidents captured in the Extremist CyberCrime Database (ECCD), an open-source data set utilizing definitional frameworks that mirror other open-source databases for off-line terror, violence, and extremist-related crime, especially the U.S. Extremist Crime Data Base (Freilich et al., 2014). The database includes a purposive set of incidents occurring between January 1, 1998, and December 31, 2018. An open-source search protocol was developed that covered over 80 different sources, including media reporting, cybersecurity vendor reports, law enforcement and government materials, academic research, blog sites, and watch group reports (see Holt et al., 2022 for more detail). All incidents included must have targeted either Internet infrastructure or target(s) operating within the United States. Additionally, all ideological frameworks are included in this data, along with incidents that were performed by nation-state sponsored attackers such as Russian or Chinese military actors.

The ECCD also captures cyberattacks as "schemes," which can involve a single incident or series of attacks motivated by the same ideological cause or purpose performed against any number of targets over time (Freilich et al., 2014). This enables all incidents within a larger attack to be captured and coded to reflect the variations in attacker behavior, target preferences, and success rates. This methodology provided a final sample of 246 incidents occurring between 1998 and 2018.

For this analysis, a purposive yet convenient sample of cases were selected to provide a sample of attacks that involve both nation-state and non-state sponsored ideological actors. Though it is expected that these actors will differ in their motives, training, and resources, the outcome of their attacks may be similar. This analysis will not focus on comparing these incidents, but rather on assessing the impact of the attacks and identifying how they may be mitigated in the future.

Two nation-state sponsored and two non-nation-state sponsored attacks were selected, and an attempt was made to select incidents with varied complexity and negative outcomes to the target. In addition, incidents were selected on the basis of information about the incident and their overall severity so as to best assess the utility of normal accidents as a framework to understand cyberattack outcomes. The events are described below, followed by an overall assessment of the degree to which normal accident theory can inform our understanding of these incidents, and identify solutions to minimize the risk of future incidents.

Nation-State Sponsored Cyberattacks

The first nation-state sponsored incident occurred in June 2013 when Iranian hackers were able to compromise a cellular modem used in the small town of Rye Brook, New York which maintains a small dam. The Bowman Avenue Dam is approximately 15 feet long and 2.5 feet high, making it relatively small and able to manage overflow from the nearby Blind Brook in the event of flooding. The affected modem was used to remotely manage aspects of the dam's operation via its supervisory control and data acquisition (SCADA) system. The modem itself was apparently was housed in city hall for the town. Though the attackers were able to gain access to the SCADA system, they were only able to monitor systems due to an error. No functional control was possible as a component of the system controlling the sluice gate was disconnected due to routine maintenance. Since this component was not reconnected, either in error or because maintenance was ongoing, the attackers were limited in their capacity for harm.

The second incident occurred on or around April 15, 2015, the Office of Personnel Management (OPM) noted that there had been suspicious activities occurring within their network, and that data had been accessed and exfiltrated by unknown parties. This incident actually began in November 2013, when attackers were able to obtain access to manuals and information about the network structure. Beginning in December 2013, attackers

then attempted to breach two contractors (USIS and KeyPoint) who facilitate background checks for OPM and had access to their servers.

In March 2014, OPM identified the initial hack, but did not publicly notify anyone as they determined that the compromise did not allow the attacker access to personnel data. OPM instead chose to monitor the attackers in order to understand their efforts and identify a mitigation strategy. While OPM was aware of these activities, on May 7, 2014, attackers utilized stolen login credentials from the contractor KeyPoint and used this path to install backdoors into the network. OPM chose to implement a system-wide purge on May 27, 2014, in the hopes of expelling the attackers that were initially identified in March. This was a response to attackers' attempts to load keystroke logging software onto database administrators' systems in order to gain credentials and information that could enable access to sensitive data.

The system purge did not remove the backdoors installed by the attackers, and they were able to continue unabated through the network. The attackers began to exfiltrate background investigation data from OPM systems in July and August 2014. BY October, the attackers moved from OPM to the Department of Interior in order to obtain additional personnel records. They were able to steal 4.2 million records in December 2014, and then access and remove fingerprint data in March 2015. These activities were finally observed in April, leading OPM to begin to report the breach. Tens of millions of personnel records were lost as a result of these breaches, including SF-86 security clearance data, and fingerprint records.

Non-Nation-State Sponsored Cyberattacks

The first incident examined began in November 2014 following the November 19, 2014, shooting death of a 12-year-old boy named Tamir Rice by a rookie police officer named Timothy Loehmann. The incident occurred in the Cudell Recreation Center park in Cleveland, Ohio, when two officers responded to a call for service regarding a male pointing a pistol at people. The officers arrived on the scene in their patrol car and told Rice to show them his hands. Loehmann indicated he thought Rice was reaching for something and shot him twice. Upon examining what Rice was carrying, it was determined to be an airsoft replica bb gun without an orange safety tip indicating it was not an actual firearm.

In response, on November 21, 2014, the hacker group Anonymous indicated they planned to launch a DDoS attack against the city of Cleveland's website. They argued the attack was a necessary response to the use of force against Rice. The attack was successful in keeping the site from being accessed by the public until approximately November 26, 2014. During the attack, it appears the city was able to continue to offer services, though residents had to call the City Hall phone line directly.

The second incident occurred during the week of March 21, 2016, an actor identified an estimated 5,000 publicly accessible, WIFI enabled printers located across the US, including dozens of printers located on college campuses. He then had them print out fliers featuring swastikas, white supremacist propaganda, and a link to a then-prominent Neo-Nazi website. The actor claimed responsibility publicly, including in interviews with major media outlets. They noted that the "hack" itself did not require any real intrusion on the part of the actor, as the printers were configured to allow remote access printing. This is a feature that constitutes a potential vulnerability as they could be accessed by anyone and used to complete print requests.

FINDINGS

Flaws in Technical Systems and Coupling

Assessing the overall characteristics of these incidents enables the identification of common problems that may have engendered the attacks. In all but the anonymous attack, the coupling of the systems used may have created opportunities for failure. For instance, the OPM network appeared to involve a tightly coupled series of networks and databases that allowed attackers to transition across the infrastructure and acquire data. This is particularly evident in the fact that the attackers utilized DHS contractors in order to gain access to the organization's network.

The printer hack incident and Bowman Avenue Dam hack also involved tight coupling and relatively linear processes. For example, the Bowman Avenue Dam infrastructure appears relatively simplistic in construction, but compromising the modem enabled access to the SCADA system that managed the dam's processing. The same can be said for the printer hack, as printers constitute a peripheral, but linear component of any networks. While printers are not a critical service within any institution or home proper, they typically do not have redundancies that can be used by others.

There were, however, substantive differences in the complexity of the attacks required in order to negatively affect the infrastructure involved. The OPM hack was the most complex, as the attackers utilized unique malicious software and tools to facilitate the compromise and had to move slowly in order to avoid identification.

The dam hack and printer incident appeared to involve the use of open-source research on the part of the attackers in order to identify the vulnerable systems. For example, the dam attacker was able to identify the target system through the use of Google dorking, which involves engaging in manipulation of search terms within Google to identify publicly accessible data and infrastructure. The same is true for the printer incident, as the attacker identified publicly accessible printers and then utilized a five-line script of code to make the print request work.

In the case of the anonymous attack, it is unclear if the attackers utilized the commonly known anonymous tool called the Low Orbit Ion Cannon (LOIC), or a series of remotely commanded computers managed by malicious software called botnet malware. An analysis of the attack by Binary Defense Systems indicated that approximately 9,000 computers were involved in the operation of the attack, so it is likely a botnet was involved. In this case, the attackers needed only to identify the IP address of their target (the website for the City of Cleveland) and direct malformed packet traffic to the site that mimicked legitimate user requests. Distributed denial of service attacks is extremely common, and do not require much complexity in order to be effective.

There was also some degree of failure evident in the security tools that would identify and mitigate cyberattacks. For instance, the federal government's EINSTEIN intrusion detection system did not identify the breaches performed in this incident. The first breach was reported to DHS by a third party, while the second was identified by either DHS employees utilizing Cylance software tools or a third-party software provider to detect the breach. There also appeared to be no infrastructure in place to identify attacks in the dam hack incident. This may be a function of the limited nature of the dam's operation and the size of the town as a whole. The same can be said for the lack of security observed to protect the printers affected by the remote printer hack. As these systems were publicly accessible, they were easily compromised.

Human and Organizational Errors

There is also evidence that human error and organizational dynamics played a role in at least two of these hacks. In the OPM hack, the agency received multiple warnings related to its cyber security practices. The limitations and vulnerabilities presented by their operational practices enabled hackers to gain access with greater ease then

would otherwise be possible in a more secured environment. In particular, data was thought to be stored in an unencrypted fashion with limited internal intrusion detection systems to identify external penetrators. In addition, the then CIO claimed that resources to better secure their infrastructure could not be implemented due to their use of legacy systems within the agency. Such claims were invalid based on general open reporting at the time.

The same is true for the dam hack, as the fact that the dam equipment was disconnected limited the attacker's capacity to cause harm. At the same time, this would have limited the city's capacity to correctly manage the dam infrastructure properly. It is less clear how actor decision-making may have increased the risk of error in the printer incident and Anonymous attack. The only observed issue with the Anonymous DDoS attack was that city officials reported that the website was operational when it was only usable for those within City Hall. The issue was eventually corrected, though this did not appear to be a serious problem.

Assessing the post-incident responses also highlights potential for future harms for three of the organizations affected. An OIG report on the investigation noted that the OPM CIO, Donna Seymour, was effectively slowing their work which led to calls as to whether she was acting appropriately. Both the OPM Director and CIO resigned after the incident, which created a leadership vacuum which may have exacerbated existing flaws in cybersecurity and operational practice. A series of reviews performed by the Government Accountability Office (GAO) on OPM infrastructure after the incident recommended 80 changes that could be made to improve the state of security. It appears that not all the recommendations had been implemented, especially basic ideas like requiring users to change passwords that may have been affected by the breach and eliminating shared administrative accounts. The absence of such simple security protocols suggests that OPM is still vulnerable to attack, which may be due to managerial or institutional resistance to change.

The city of Rye Brook reportedly disconnected the Bowman Avenue Dam SCADA and other systems from the Internet. Such a move is strategically sensible as it makes their infrastructure inaccessible to online threads, but only because of the size and operational function of their equipment. Larger cities and more complex critical infrastructure are not always able to be taken offline.

In much the same way, some institutions affected by the wireless printer incident reported that they blocked external print requests. This would provide a fix for this specific issue, though it does not eliminate the overall vulnerabilities presented by the use of publicly accessible (i.e., non-password protected) printers in any network. Finally, it is unclear what, if any steps were taken by the City of Cleveland to minimize their risk of a loss of services due to DDoS attacks. There are a number of service providers who offer attack-proof hosting, so it is possible they may have migrated their services to such infrastructure.

Discussion and Conclusions

Taken as a whole, normal accident theory recognizes that the likelihood of a catastrophic error is more likely in complex, tightly coupled systems where there is minimal time to identify or correct a problem before it causes cascading harm to other parts of the system (Perrow, 1999). Though this framework has been applied to traditional complex systems, few have utilized it to account for harms stemming from cyberattacks. This analysis demonstrates the substantive potential of normal accident theory to assess cyberattacks, particularly those associated with nation-state sponsored attackers.

It is clear that virtually any system can be hacked, no matter how much security is in place. At the same time, the degree of harms resulting from an incident can be mitigated through the use of adequate security protocols and practices. One of the key implications of this analysis is the need to ensure all entities make the best effort possible to be in compliance with best practices for cybersecurity relative to the size and characteristics of the entity. The OPM example is illustrative as simple cybersecurity strategies could and should have been implemented after the breaches. It is unclear why there was resistance to the adoption of solid security measures, and there may have

been managerial resistance to such efforts given reporting.

It is similarly unclear as to the factors at play in the Bowman Avenue Dam hack, as having a piece of critical infrastructure indexed and noted for the public to observe online presents a risk for compromise. Similarly, having equipment disconnected during the attack was a seemingly lucky coincidence that minimized the potential harm that could be caused. It is unclear if these factors were a function of lax cybersecurity or other factors given the size of the city and its overall infrastructure operations.

These examples demonstrate a need to transform the risk of systemic failures stemming from cyberattacks in various ways. At present, there appear to be few ways to consistently minimize the complexity and coupling of network architecture, databases, and Internet functionality. There is too much variability in the resources of organizations relative to the demands placed on their infrastructure to effectively minimize these concerns.

Instead, it is imperative that cybersecurity policy makers focus on areas where the greatest impacts may be generated through human and organizational practices. In particular, a cultural shift is needed regarding the risks of cybersecurity threats and the importance of compliance with best security practices at all levels of employment and organizational types. One possible way to increase the likelihood that public and private entities adopt appropriate cybersecurity protocols is through increased visibility of best practices documentation and services from agencies like DHS CISA, NIST, and the FTC.

In addition to guidance, there may be value in the creation of cybersecurity audit and compliance entities across the whole of federal and state governments. For example, the FTC has a responsibility to monitor and enforce compliance with the Standards for Safeguarding Customer Information Rule for private entities that operate as financial institutions. The rule requires basic cybersecurity protocols and does not extend to entities outside of the financial services arena.

As a result, there may be substantive benefits to the creation of a more efficient and robust model of cybersecurity compliance for all public and private entities. Empowering federal and state agencies to engage in regular audits and penalize non-compliance may be a way to help ensure greater alignment to national cybersecurity strategies and policies than what is currently used. Such an entity could also help to reduce the likelihood of compromise among those contracting entities that work directly with federal agencies. In turn this could reduce the potential for nation state attackers to find inroads into various entities in the public and private sector.

REFERENCES

Boustras, G., & Waring, A. (2020). Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context. Safety Science.

Brown, H. (2018, June). Keeping the Lights On: a comparison of normal accidents and high reliability organizations. IEEE Technology and Society Magazine, pp. 63-70.

Galligan, T. C. (2012). A Sad Tale of the Deepwater Horizon Disaster, Normal Accidents, and Our Appetite for Risk. Roger Williams University Law Review, pp. 264-294.

Holt, T. J. (2023). Understanding the state of criminological scholarship on cybercrimes. Computers in Human Behavior, 39, 107493.

King, W. R. (2009). Police officer misconduct as normal accidents. Criminology & Public Policy, 771-776.

Leukfeldt, R. & Holt, T. J. (2019). The Human Factor of Cybercrime. London: Routledge.

Maas, M. (2018). Regulating for 'normal AI accidents' - Operational lessons for the responsible governance of AI deployment. Association for the Advancement of Artificial Intelligence.

Min, B. H., & Borch, C. (2021). Systemic failures and organizational risk management in algorithmic trading: Normal accidents and high reliability in financial markets. Social Studies of Science, 1-26.

Nunan, D., & Domenico, M. (2015). Big Data: A Normal Accident Waiting to Happen. Business Ethics, 481-491.

Perrow, C. (1999). Normal Accidents: Living With High Risk Technologies, 2nd Edition.

Princeton, NJ: Princeton University Press.

Pidgeon, N. (2011, September 22). In Retrospect: Normal Accidents. Retrieved from Nature: https://www.nature.com/articles/477404a

Yankun, Z. (2021). Normal accidents in risk supervision: an analysis of a basic government chemical supervision system model. 2nd International Conference on Urban Engineering and Management Science (ICUEMS), (pp. 250-253). Zhuhai, China.