RAIS Journal for Social Sciences | Vol. 10, No. 2, 2026
ISSN 2574-0245 (Print) | ISSN 2574-1179 (Online) | DOI:10.5281/zenodo.24489802

Espionage or War Preparation? Assessing the Intent Behind State-Sponsored Cyber Activity That Threatens National Security

Sharon L. Burton

College of Aviation, Embry-Riddle Aeronautical University, Daytona Beach, FL, USA
burtons6@erau.edu

Abstract: Between February 2024 and October 2026, agencies in the United States and allied countries faced cyber intrusions by foreign governments, and the digital evidence could point either to spying or to preparation for war. In February 2024, three agencies of the United States assessed with high confidence that the Volt Typhoon group was pre-positioning inside critical infrastructure networks to disrupt them in a future crisis. The government of China called the same group an international ransomware gang. In August 2025, 23 agencies from 13 countries warned that related intrusions into telecommunications networks could let Chinese intelligence services track targets worldwide. This qualitative document analysis examines how investigators inferred the intent behind such activity, using the Diamond Model of Intrusion Analysis and the Analysis of Competing Hypotheses. Six findings emerged. Identical access served different purposes, and victim selection supplied the strongest evidence of intent. Declared motives required corroboration, and adversaries contested attributions in public. Confidence language guarded against cognitive bias, and coalition judgments depended on shared knowledge. This article argues that intent assessment is a human judgment that national security leaders should strengthen through attention to analyst performance, structured training, and knowledge sharing.

Keywords: Attribution, Cyber Intent, Cyber Law, Human Factors, Intelligence Analysis, Knowledge Management, National Security, Pre-Positioning

Introduction

National security in cyberspace often turns on a question that technical evidence cannot answer alone: what an intruder intends to do with the access it has gained. Ferazza (2026) argues that the same technical features can fit espionage, coercion, or sabotage. The Congressional Research Service (CRS) reports that investigators combine evidence about tradecraft, malware, and infrastructure with analysis of an attacker's intent before stating a level of confidence (Jaikaran, 2026). That judgment determines whether a government treats an intrusion as routine collection or as a threat that demands a national response.

Public intent assessments issued between 2024 and 2026 give this inquiry its urgency. On February 7, 2024, three agencies issued the first assessment in a joint advisory (Cybersecurity and Infrastructure Security Agency [CISA] et al., 2024). The agencies were the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI). They assessed with high confidence that the Volt Typhoon group was pre-positioning for disruptive attacks rather than conducting traditional espionage (CISA et al., 2024). China's Ministry of Foreign Affairs described the group as an international ransomware gang (Ministry of Foreign Affairs of the People's Republic of China, 2024). Rob Joyce, a former NSA Director of Cybersecurity, argued instead that its targeting revealed war preparation (Joyce, 2026). One body of evidence supported three competing accounts of intent, and this article addresses that problem.

This article examines how investigators judge the intent behind state-sponsored cyber activity and which human conditions influence that judgment, a concern Heuer (1999) raised for intelligence analysis. The research question asks: How did investigators in the United States and allied countries infer intent from cyber activity affecting national security between February 2024 and October 2026? A second question asks what roles analyst performance, preparation, and the exchange of knowledge play in the reliability of those inferences. Supporting scholarship spans analyst performance (Nobles, 2022; Nobles & McAndrew, 2023), workforce preparation (Burton, 2021, 2025), and organizational knowledge (Burton, 2022; Dodla & Jones, 2023a, 2023b). Studies of attribution and intelligence analysis (Broeders, 2024; Rid & Buchanan, 2015) complete that foundation.

Background

Pre-Positioning Inside Critical Infrastructure

The Volt Typhoon case turned intent assessment into a public national security issue. In February 2024, CISA, NSA, and FBI assessed that actors sponsored by the People's Republic of China (PRC) were seeking access to information technology (IT) networks. Their purpose, the agencies judged, was to enable disruptive or destructive attacks on critical infrastructure in the United States during a major crisis or conflict (CISA et al., 2024). Target choice and the pattern of behavior formed the basis of that judgment. They also assessed with high confidence that the actors were preparing to move toward operational technology (OT) assets (CISA et al., 2024). In 2023, the Department of Defense (DoD) had already judged that, in a conflict, the PRC likely intends to launch destructive cyberattacks against the United States homeland to hinder military mobilization (U.S. Department of Defense, 2023).

A former official now outside the United States government reached a stronger conclusion. Joyce (2026) read the reach of the campaign into port logistics, Guam communications, transportation command centers, and military fiber links as war preparation. The Office of the Director of National Intelligence (ODNI) reported in 2026 that China and Russia were continuing pre-positioning efforts against the United States (Office of the Director of National Intelligence [ODNI], 2026). Targeting choices became the evidence through which investigators read intent.

Espionage at Global Scale

Telecommunications intrusions illustrate how intent can be stated more narrowly. In August 2025, 23 agencies from 13 countries attributed a global campaign against telecommunications and internet service providers and against the lodging and transportation sectors to PRC state-sponsored actors (National Security Agency [NSA], 2025). The advisory stated that stolen data could allow Chinese intelligence services to identify and track the communications and movements of their targets worldwide, a purpose consistent with espionage (NSA, 2025). Broeders (2024) observes that intelligence agencies are the leading security actors in cyberspace and that their operations increasingly resemble covert action, blurring collection and attack.

Declared and Contested Intent

Some actors announce their intent, while others deny it. ODNI (2026) reported that on March 11, 2026, an Iran-linked group claimed an attack on a medical technology company in the United States as retaliation for strikes by the United States against Iran. The same assessment noted that Russia often hides and denies its role in gray-zone activity (ODNI, 2026). China's Ministry of Foreign Affairs cited a report by China's National Computer Virus Emergency Response Center to argue that Volt Typhoon was a ransomware group. The ministry also claimed that agencies of the United States had made false allegations (Ministry of Foreign Affairs of the People's Republic of China, 2024). Claims and denials became evidence that investigators had to weigh rather than accept.

Legal Authorities That Turn on Intent

Intent also carries legal weight in the United States response. The Computer Fraud and Abuse Act makes unauthorized access a crime when done knowingly or intentionally. It adds offenses for intent to defraud and for intentional damage (Computer Fraud and Abuse Act, 2026). Federal Rule of Criminal Procedure 41 (2023) allows a judge to authorize remote searches when the location of computers has been concealed through technological means. It also allows such searches when protected computers in five or more districts have been damaged. In January 2024, federal prosecutors announced a court-authorized operation that deleted malware from hundreds of routers in the United States that Volt Typhoon had used to conceal its PRC origin (U.S. Attorney's Office, Southern District of Texas, 2024). A similar operation in 2021 had removed malicious web shells from Microsoft Exchange servers (U.S. Department of Justice, 2021). Military law authorizes the Secretary of Defense to conduct cyber operations, including clandestine ones, in response to malicious cyber activity by a foreign power (Authorities Concerning Military Cyber Operations, 2026). Each authority depends on a prior judgment about who acted and why.

Why Intent Assessment Is Difficult

Scholars disagree on how much public evidence can reveal about intent. Rid and Buchanan (2015) argued that attribution "is what states make of it" (p. 4), a judgment that joins technical, operational, and strategic analysis. Ferazza (2026) contends that intent usually stays hidden because actors filter what reaches the public. Intent assessment is a human analytic act performed under uncertainty, and that view frames the method of this article.

Research Method and Design

This article used qualitative document analysis, which Bowen (2009) describes as a systematic procedure for reviewing and evaluating documents in print and electronic form. Its sources were joint cybersecurity advisories, the 2026 ODNI threat assessment, a CRS report, an official statement by the government of China, and peer-reviewed studies of attribution, analytic reasoning, and the analytic workforce. Cases were included if a government agency or a former senior official published an assessment of state-linked cyber intent between February 2024 and October 2026. Material available only in blogs or social media was excluded, because Bowen (2009) advises researchers to assess the authenticity and credibility of each document.

Each case was coded against the four features of the Diamond Model, the competing intent hypotheses in the public record, and the stated confidence (Caltagirone et al., 2013; Heuer, 1999). The final corpus comprised 33 sources, including eight government records. They included three joint or agency advisories and assessments, a CRS report, and a DoD strategy summary. Two Department of Justice releases and a statement by China's foreign ministry completed that set (CISA et al., 2024; Jaikaran, 2026; NSA, 2025; ODNI, 2026). Three statutes and court rules, two government standards, and 20 scholarly works made up the rest of the corpus. The coding results were recorded in a case-by-hypothesis matrix, presented as Table 1 (Caltagirone et al., 2013).

Assumptions, Limitations, and Delimitations

Assumptions

This article rests on six assumptions. First, it assumes that public advisories accurately represent the judgments the issuing agencies reached, even though the classified evidence behind them is withheld (CISA et al., 2024; NSA, 2025). Second, it assumes that confidence labels carry the meanings the CRS describes, in which high confidence signals no viable alternative and low confidence signals significant information gaps (Jaikaran, 2026). Third, it assumes that the intent of a state actor can be inferred, at least in part, from observable

choices of targets and techniques, the premise of the Diamond Model (Caltagirone et al., 2013). These assumptions allow public documents to serve as evidence of official reasoning.

The remaining assumptions concern analysts. Fourth, it assumes that intelligence analysts face the same cognitive limitations as other people when they judge incomplete and ambiguous information, a premise Heuer (1999) drew from cognitive psychology. Fifth, it assumes that stress, burnout, and security fatigue affect analytic performance, consistent with the human factors account of Nobles (2022). Sixth, it assumes that preparation and the exchange of knowledge can sharpen judgments made under uncertainty, consistent with the link Burton (2021) draws between knowledge and the growth of human capital among cybersecurity leaders. If these assumptions failed, the findings would describe official reasoning without explaining its reliability.

Limitations

Six limitations bound the findings. First, this article relied on unclassified documents, so it cannot test whether withheld evidence supported the stated confidence (CISA et al., 2024). Second, Ferazza (2026) warns that the public record is filtered by actors who decide what to reveal. Publicly attributed cases may not represent all state intrusions. Third, the position of the government of China rests on reports this article could not evaluate technically. That position is treated as a competing claim rather than as established fact (Ministry of Foreign Affairs of the People's Republic of China, 2024). These constraints limit how far the findings can be generalized.

Further limitations arise from timing, verification, and perspective. Fourth, assessments published between February 2024 and October 2026 may be revised by later disclosures (ODNI, 2026). Fifth, attacker claims, including the claim by the Iran-linked group to have erased 200,000 systems, remain unverified in the sources examined (ODNI, 2026). Sixth, this article did not draw on interviews with analysts. Its human dimensions rest on documents and on laboratory experiments whose results may not transfer to live cases (Dhami et al., 2024). Because the experience of the author could color interpretation, every claim is tied to a cited source.

Delimitations

The author narrowed the scope through six choices. First, this article is limited to state-sponsored or state-linked activity against the United States and its allies. The PRC claim that Volt Typhoon was criminal is still examined as a competing hypothesis (Ministry of Foreign Affairs of the People's Republic of China, 2024). Second, the period runs from February 2024 to October 2026 (CISA et al., 2024; ODNI, 2026). Third, this article examines intent rather than identity, so technical attribution methods appear only where they inform judgments about purpose (Jaikaran, 2026). These choices keep the analysis on the reasoning behind national security judgments.

The final choices concern theory, law, and sources. Fourth, this article applies the Diamond Model and the Analysis of Competing Hypotheses (ACH); the Q Model of Rid and Buchanan (2015) informs the background only. Fifth, this article describes the legal authorities of the United States without ruling on whether any intrusion broke international law or amounted to war. Libicki (2026) contends that labeling a cyber operation as war is ultimately a political decision. Sixth, the review was restricted to sources published in English, and the human conditions examined were confined to analyst performance, preparation, and organizational knowledge (Dodla & Jones, 2023a; Nobles, 2022). This scope supports actionable guidance across adversaries.

Theoretical Framework

Framework One: The Diamond Model of Intrusion Analysis

The Diamond Model describes every intrusion event through four core features: an adversary, a capability, the infrastructure that delivers it, and a victim (Caltagirone et al., 2013). Its first axiom holds that each event involves an adversary taking a step toward an intended goal. The authors locate intent in a social-political relationship, defined by the needs of the adversary and the ability of the victim to satisfy them (Caltagirone et al., 2013). Intent, in this model, is an inference drawn from relationships among observable features rather than a direct observation.

The model was selected because the 2024–2026 assessments inferred intent mainly from the victim feature. CISA et al. (2024) judged Volt Typhoon by its targets and behavior, and Joyce (2026) read intent from the specific infrastructure the campaign reached. Weak protection of critical infrastructure leaves nations open to harm (Dawson et al., 2021), so the pool of possible victims that intent analysis must weigh is broad. These sources make the victim feature the natural entry point for the analysis.

In this article, the model organizes each case into its four features and then asks which adversary need would explain the pairing of capability and victim. A telecommunications victim paired with data theft suggests collection, whereas a transportation or water victim paired with a path toward control systems suggests disruption (CISA et al., 2024; NSA, 2025). The model structures the evidence, and the second framework explains how analysts weigh it.

Framework Two: Heuer's Analysis of Competing Hypotheses

Heuer (1999) drew on cognitive psychology to explain how analysts judge incomplete and ambiguous information. He observed that much analysis resembles satisficing, the selection of the first alternative that appears good enough. In his account, analysts choose an intuitively likely answer and then dismiss evidence that does not support it as misleading (Heuer, 1999). He proposed ACH, an eight-step procedure that requires analysts to weigh evidence against every reasonable explanation rather than against a favored one (Heuer, 1999). The framework shifts attention from the evidence itself to the reasoning applied to it.

The framework was selected because the Volt Typhoon record contains three public hypotheses about one body of activity. These hypotheses are espionage, pre-positioning for conflict, and criminal ransomware (CISA et al., 2024; Joyce, 2026; Ministry of Foreign Affairs of the People's Republic of China, 2024). It also matches the CRS account that investigators entertain competing theories and seek to minimize human error (Jaikaran, 2026). Nobles (2022) links stress, burnout, and security fatigue to human performance problems in cybersecurity, conditions that can push analysts toward satisficing.

In this article, ACH serves as the standard for judging whether public assessments considered alternatives and how they expressed uncertainty. Burton (2025) calls for simulation built on realistic scenarios. Ohu and Jones (2025) design an artificial intelligence framework that flags insider risk from cognitive and psychological signals, and each approach could carry structured reasoning into judgments about intent. The Diamond Model identifies what evidence exists, while ACH explains how analysts can test it (Caltagirone et al., 2013; Heuer, 1999).

Critique of the Theoretical Framework

Drawbacks of the Diamond Model

The Diamond Model carries limitations for the analysis of intent. First, its authors chose not to treat intent as a top-level feature and placed it in a social-political sub-tuple, which leaves intent as a secondary inference (Caltagirone et al., 2013). Second, the model depends on observable features, yet Ferazza (2026) argues that the variables that carry the greatest weight

for strategy, including intent and cost-risk calculations, usually remain hidden. Third, the model was built for intrusion analysis and does not address public attribution, which Rid and Buchanan (2015) treat as a strategic as well as a technical judgment. These gaps limit what the model can say about national decisions. Further drawbacks concern ambiguity and change over time. Fourth, Ferazza (2026) notes that a target may be unable to distinguish a deliberate signal from careless tradecraft, and the model offers no rule for resolving that ambiguity. Fifth, Ferazza (2026) also observes that access consistent with espionage can create options for later sabotage, a shift that analysis of a single event cannot capture. Here, the model serves to arrange the evidence rather than to decide intent.

Drawbacks of the Analysis of Competing Hypotheses

ACH has drawn empirical criticism. First, Dhami et al. (2024) found that participants given the ACH-style matrix, with hypotheses in columns and evidence in rows, were not less likely to show confirmation bias. Participants given hypotheses in rows and evidence in columns were less likely to show it (Dhami et al., 2024). Second, the same study found that the majority of 62 Dutch military analysts did not show confirmation bias (Dhami et al., 2024). That result suggests that the bias ACH targets may be less common among trained analysts than Heuer (1999) assumed. Third, the procedure can test only the hypotheses that analysts generate, so an explanation no one proposes never enters the matrix. These findings question whether the tool, rather than training, produces better judgments.

Further drawbacks concern time and evidence. Fourth, analysts working under the stress and fatigue that Nobles (2022) describes may lack the time to complete all eight steps during a fast-moving crisis. Fifth, ACH weighs the evidence that analysts can see, yet Ferazza (2026) argues that public evidence is filtered by actors with reasons to reveal or conceal. A well-structured matrix can still rest on a biased record. This article uses ACH as a standard for judging public reasoning, not as proof that any assessment was correct.

Results and Data Findings

Table 1 maps the principal cases to the observed activity, the competing intent hypotheses, and the stated judgments. In each case, intent was inferred from relationships among features rather than observed directly, which is the central result. National security judgments about cyber activity rested on human interpretation of victims and behavior (Caltagirone et al., 2013; Jaikaran, 2026). Six findings emerged.

Table 1. Intent Assessments of State-Linked Cyber Activity, February 2024–October 2026

Case (date)	Observed activity and victims	Intent hypothesis or stated judgment
Volt Typhoon advisory (Feb. 2024)	Persistent access to IT networks in critical infrastructure of the United States, with paths toward OT	Pre-positioning for disruption; high confidence
PRC government response (Apr. 2024)	Same Volt Typhoon activity	International ransomware group; allegations by the United States called false
Global telecommunications advisory (Aug. 2025)	Telecommunications and internet providers, lodging, and transportation; 23 agencies from 13 countries	Espionage: tracking the communications and movements of targets
Iran-linked attack claim (Mar. 11, 2026)	Medical technology company in the United States; claimed erasure of 200,000 systems	Declared retaliation; claims unverified in the sources examined
Joyce analysis (2026)	Port logistics, Guam communications, transportation command centers, military fiber links	War preparation, not espionage

Note. Compiled by the author from CISA et al. (2024); Joyce (2026); Ministry of Foreign Affairs of the People's Republic of China (2024); NSA (2025); and ODNI (2026).

Finding 1: Identical access can serve different purposes. The government of China attributed Volt Typhoon to criminals (Ministry of Foreign Affairs of the People's Republic of China, 2024). Agencies of the United States attributed it to pre-positioning (CISA et al., 2024), and Joyce (2026) attributed it to war preparation. Ferazza (2026) explains why such disagreement persists: technical evidence does not uniquely reveal purpose. The same foothold cannot settle intent without contextual evidence.

Finding 2: Victim selection supplies the strongest evidence of intent. CISA et al. (2024) cited target choice and behavior, Joyce (2026) cited logistics and communications nodes, and NSA (2025) linked telecommunications and lodging victims to the tracking of individuals. In Diamond Model terms, the victim feature carried the weight of the inference (Caltagirone et al., 2013). Victims, who often hold the evidence, become partners in national intent assessment.

Finding 3: Declared motives require corroboration. The Iran-linked group announced retaliation and claimed sweeping damage, while Russia often hides and denies its role (ODNI, 2026). Ferazza (2026) argues that actors decide what to reveal or conceal, which suggests that declared motives can themselves serve as instruments of influence. Analysts must treat claims and denials as hypotheses to test.

Finding 4: Adversaries contest attributions in public. The counter-narrative of the government of China placed a third hypothesis into public debate (Ministry of Foreign Affairs of the People's Republic of China, 2024). Broeders (2024) urges states to end their legal and diplomatic silence about intelligence operations so that limits can be agreed, and Willers and Gjesvik (2026) trace how early great-power framing shaped later cyber diplomacy. Intent assessment extends from the analytic cell into diplomacy.

Finding 5: Confidence language guards against cognitive bias. The CRS confidence scale requires investigators to state whether viable alternatives remain (Jaikaran, 2026), a discipline that counters the satisficing Heuer (1999) described. Dhami et al. (2024) found that matrix format alone did not reduce confirmation bias, which suggests that training matters more than tools. Burrell (2024) found that more cyber instruction alone has not kept attackers from exploiting weak points, and Burton (2025) favors simulation. Together, these sources point toward repeated practice with ambiguous cases.

Finding 6: Coalition judgments depend on shared knowledge. The 2025 advisory carried the seals of 23 agencies from 13 countries, a joint judgment that required agencies to share evidence and reasoning (NSA, 2025). Dodla and Jones (2023b) sort knowledge risks into human, technological, and organizational categories, and Burton (2022) frames the movement of knowledge inside an organization as part of its security posture. Intent assessment at national scale is a knowledge management task as much as a technical one. The discussion that follows interprets these six findings.

Discussion

The six findings answer the research question by showing that investigators inferred intent from context rather than from the intrusion itself. Victim selection, declared motives, and public denials carried more weight than malware or infrastructure (CISA et al., 2024; NSA, 2025; ODNI, 2026). This pattern supports the argument by Rid and Buchanan (2015) that attribution joins technical, operational, and strategic judgment. It also confirms the warning by Ferazza (2026) that public evidence reflects what actors choose to reveal. The two theoretical frameworks explain this pattern in different ways.

The Diamond Model organized each case, yet it could not decide between espionage and pre-positioning on its own (Caltagirone et al., 2013). ACH supplied that missing discipline, because the public record contained three rival hypotheses about Volt Typhoon (Heuer, 1999; Ministry of Foreign Affairs of the People's Republic of China, 2024). Dhami et al. (2024), however, found that the matrix format did not by itself reduce confirmation bias.

Read together, these frameworks suggest that the quality of an intent judgment depends on the analyst more than on the tool.

The human dimensions of the findings align with earlier leadership and human factors research. Nobles (2022) linked stress, burnout, and security fatigue to weaker performance, conditions that can push analysts toward the satisficing Heuer (1999) described. Burton (2021) tied cybersecurity leadership to the growth of knowledge, which suggests that leaders shape whether analysts share reasoning across agencies and allies. Dodla and Jones (2023a) examined strategies for knowledge management systems, and the 2025 coalition advisory applied such strategy at international scale (NSA, 2025). These implications inform the recommendations in the conclusion.

Conclusion

Cyber activity affects national security less through what intruders have done than through what investigators judge they intend to do. Between February 2024 and October 2026, agencies assessed pre-positioning, global espionage, declared retaliation, and denial (CISA et al., 2024; NSA, 2025; ODNI, 2026). China, meanwhile, contested the account of Volt Typhoon (Ministry of Foreign Affairs of the People's Republic of China, 2024). In each case, the decisive step was a human inference drawn from victims, behavior, and context.

Four recommendations follow. First, agencies should train analysts in structured techniques using realistic, ambiguous scenarios rather than relying on matrix formats alone (Burton, 2025; Dhami et al., 2024; Merritt et al., 2024). Second, leaders should monitor analyst stress, workload, and fatigue as threats to the quality of judgment (Nobles, 2022; Nobles & McAndrew, 2023). Third, agencies and allies should build shared repositories for intent indicators and for the reasoning behind confidence levels (Dodla & Jones, 2023a; NSA, 2025). Fourth, governments should publish the basis of their confidence judgments where security permits, because courts, allies, and publics now weigh those judgments (Broeders, 2024; Federal Rule of Criminal Procedure 41, 2023; Jaikaran, 2026).

A promising next step is dissertation-level qualitative work on how cyber threat analysts weigh rival explanations of intent under time pressure, building on the experiments of Dhami et al. (2024). Studies of behavioral indicators of state-actor intent would extend the insider-focused framework of Ohu and Jones (2025) to national security analysis. The task ahead is to make judgments about intent as disciplined as the technical forensics that support them (Heuer, 1999; Jaikaran, 2026).

Key Terms and Definitions

Attribution: The process of identifying the party responsible for a cyber incident by corroborating technical and intent evidence from multiple sources (Jaikaran, 2026).

Confidence Level: The degree of certainty investigators assign to an assessment, expressed as high, moderate, or low (Jaikaran, 2026).

Cyberspace: "The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information systems, industrial control systems, networks, and embedded processors and controllers" (Committee on National Security Systems, 2022, "Cyberspace").

Intent: In the Diamond Model, the adversary need that a victim can satisfy, such as espionage or fraud (Caltagirone et al., 2013).

Pre-Positioning: Gaining and maintaining access to networks in advance so that disruptive or destructive attacks can be launched during a future crisis or conflict (CISA et al., 2024).

References

Authorities concerning military cyber operations, 10 U.S.C. § 394 (2026). https://uscode.house.gov/us/usc/119-118/t10/s394/

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Broeders, D. (2024). Cyber intelligence and international security: Breaking the legal and diplomatic silence? *Intelligence and National Security, 39*(7), 1213–1229. https://doi.org/10.1080/02684527.2024.2398077

Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. *Land Forces Academy Review, 29*(1), 38–49. https://doi.org/10.2478/raft-2024-0004

Burton, S. L. (2021). Cybersecurity leaders: Knowledge driving human capital development. *Scientific Bulletin, 26*(2), 109–120. https://doi.org/10.2478/bsaft-2021-0013

Burton, S. L. (2022). *Cybersecurity leadership from a telemedicine/telehealth knowledge and organizational development examination* (Publication No. 29066056) [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations and Theses Global. https://www.proquest.com/dissertations-theses/cybersecurity-leadership-telemedicine-telehealth/docview/2662752457/se-2

Burton, S. L. (2025). Digital saboteurs: Unmasking insider cybersecurity threats in aviation and aerospace. *Law, Economics and Society, 1*(2), 1–20. https://doi.org/10.30560/les.v1n2p1

Caltagirone, S., Pendergast, A., & Betz, C. (2013). The diamond model of intrusion analysis (Technical Report ADA586960). *Center for Cyber Intelligence Analysis and Threat Research*. https://apps.dtic.mil/sti/citations/ADA586960

Committee on National Security Systems. (2022). *Committee on National Security Systems (CNSS) glossary (CNSSI No. 4009)*. https://csrc.nist.gov/glossary/term/cyberspace

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2026). https://uscode.house.gov/us/usc/119-121/t18/s1030/

Cybersecurity and Infrastructure Security Agency, National Security Agency, & Federal Bureau of Investigation. (2024, February 7). *PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure* (Cybersecurity Advisory AA24-038A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review, 26*(1), 69–75. https://doi.org/10.2478/raft-2021-0011

Dhami, M. K., Belton, I. K., De Werd, P., Hadzhieva, V., & Wicke, L. (2024). Effects of task structure and confirmation bias in alternative hypotheses evaluation. *Cognitive Research: Principles and Implications, 9,* Article 37. https://doi.org/10.1186/s41235-024-00560-y

Dodla, T. R., & Jones, L. A. (2023a). Identifying knowledge management strategies for knowledge management systems. *ACCESS: Access to Science, Business, Innovation in Digital Economy, 4*(2), 261–277. https://doi.org/10.46656/access.2023.4.2(8)

Dodla, T. R., & Jones, L. A. (2023b). Mitigating knowledge management internal and external risk factors: A literature review of best practices. *Scientific Bulletin, 28*(1), 44–54. https://doi.org/10.2478/bsaft-2023-0005

Federal Rule of Criminal Procedure 41, 18 U.S.C. app. (2023). https://www.uscourts.gov/sites/default/files/document/criminal_federal_rules_pamphlet_dec_1_2023.pdf

Ferazza, F. (2026). Seeing only what we can see: Why cyber strategy may be built on illusion. *International Journal of Information Security, 25*(5), Article 156. https://doi.org/10.1007/s10207-026-01325-y

Heuer, R. J., Jr. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence, Central Intelligence Agency. https://www.cia.gov/resources/csi/books-monographs/psychology-of-intelligence-analysis-2/

Jaikaran, C. (2026). *Cybersecurity: Selected cyberattacks, 2012–2025 (CRS Report No. R46974*). Congressional Research Service. https://www.congress.gov/crs-product/R46974

Joyce, R. (2026). China's cyber explosives are in place. Where's our response? *The Cyber Defense Review, 11*(2), 221–227. https://doi.org/10.55682/cdr/y0f7-s7pf

Libicki, M. (2026). Is cyberwar war – and why might it matter? *The Cyber Defense Review, 11*(2), 81–88. https://doi.org/10.55682/cdr/ahs0-k0pg

Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder, J. N., & Walden, D. (2024). *Building a cybersecurity and privacy learning program* (NIST Special Publication 800-50r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50r1

Ministry of Foreign Affairs of the People's Republic of China. (2024, April 15). *MFA coordinator for cyber affairs Wang Lei takes an exclusive interview with CCTV*. https://www.fmprc.gov.cn/mfa_eng/gjhdq_665435/3376_665447/3432_664920/3435_664926/202404/t20240418_11283884.html

National Security Agency. (2025, August 27). Countering Chinese state-sponsored actors compromise of networks worldwide to feed global espionage system [Joint cybersecurity advisory with 22 partner agencies from 13 countries]. https://www.ic3.gov/CSA/2025/250827.pdf

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA – Journal of Business and Public Administration, 13*(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

Nobles, C., & McAndrew, I. (2023). The intersectionality of offensive cybersecurity and human factors: A position paper. *Scientific Bulletin, 28*(2), 215–233. https://doi.org/10.2478/bsaft-2023-0022

Office of the Director of National Intelligence. (2026). Annual threat assessment of the U.S. intelligence community. https://www.odni.gov/wp-content/uploads/dlm_uploads/ATA-2026-Unclassified-Report.pdf

Ohu, F. C., & Jones, L. A. (2025). Predictive behavioral risk intelligence: An AI framework for insider threat detection based on cognitive and psychological indicators. *RAIS Journal for Social Sciences, 9*(2), 108–132. https://doi.org/10.5281/zenodo.17468887

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

U.S. Attorney's Office, Southern District of Texas. (2024, January 31). *U.S. government disrupts botnet People's Republic of China used to conceal hacking of critical infrastructure* [Press release]. https://www.justice.gov/usao-sdtx/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

U.S. Department of Defense. (2023). *2023 DOD cyber strategy summary*. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

U.S. Department of Justice. (2021, April 13). *Justice Department announces court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities* [Press release]. https://www.justice.gov/archives/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-exchange

Willers, J. O., & Gjesvik, L. (2026). Diplomacy in the age of expertise: The case of cyber diplomacy. *International Affairs, 102*(2), 513–534. https://doi.org/10.1093/ia/iiaf271