Moestopo International Review on Societies, Humanities, and Sciences (MIRSHuS)
Vol. 6, No. 2 (2026) pp. 436-455
ISSN: 2775-9601

Cyber Coercion in Healthcare: Evidence from the 2024 Synnovis Ransomware Attack

Bintang Corvi Diphda*
Universitas Brawijaya, Malang, Indonesia
Fahdina Camela Farcha
Universitas Brawijaya, Malang, Indonesia
Nayottama Aryaputra
Universitas Brawijaya, Malang, Indonesia
Sarah Marwah Azzahra
Universitas Brawijaya, Malang, Indonesia
Siti Ni'mah Milly Otolomo
Universitas Brawijaya, Malang, Indonesia

*Correspondence: bintangcorvi058@gmail.com

ARTICLE INFO

Article History:
received: 15/05/2026
revised: 30/06/2026
accepted: 24/08/2026

Keywords:
Cybersecurity; Cyber Coercion; Ransomware; NHS

DOI:
10.32509/mirshus.v6i2.191

ABSTRACT

This article examines the 2024 Synnovis ransomware attack on the United Kingdom's National Health Service. The study employs a qualitative single-case design based on a structured desk review. The evidence was analysed through Borghard and Lonergan's framework of cyber coercion. The findings show that Qilin clearly communicated a financial demand and imposed substantial operational, clinical, financial, reputational and informational costs through various disruption measures. However, these consequences demonstrate successful cost imposition rather than successful alteration of the target's cost-benefit calculus. The ransom remained unpaid, indicating that the coercive pressure was insufficient to produce compliance. Qilin's credibility was demonstrated through actual disruption and the publication of stolen data, while reassurance remained weak because payment could not guarantee system restoration, permanent data deletion, or protection from further exploitation. The article contributes to cyber-coercion research by extending its application to criminal ransomware and showing that coercive effectiveness depends partly on the relationship among service dependency, cost distribution, decision authority, and behavioural outcome.

INTRODUCTION

The digital transformation of healthcare has reshaped how states provide essential public services (Komariah et al., 2025; Mauro et al., 2024; Neubauer et al., 2026; Stoumpos et al., 2023). For example, in the United Kingdom, the National Health Service (NHS) has increasingly relied on digital infrastructure to build a connection between patients, hospitals

Moestopo International Review on Societies, Humanities, and Sciences (MIRSHuS)
Vol. 6, No. 2 (2026) pp. 436-455
ISSN: 2775-9601

and the health administrative systems (Cresswell & Williams, 2026). This dependence can be seen in the daily routine of healthcare practices in the UK. According to Kello et al. (2026), the NHS digital channels are used for around 94.3% of appointment bookings, 98.9% of repeat prescription requests and 84.1% of health test result checks (see Figure 1). These numbers, hence, indicate that healthcare digital systems in the UK have become essential to the accessibility and continuity of healthcare services.

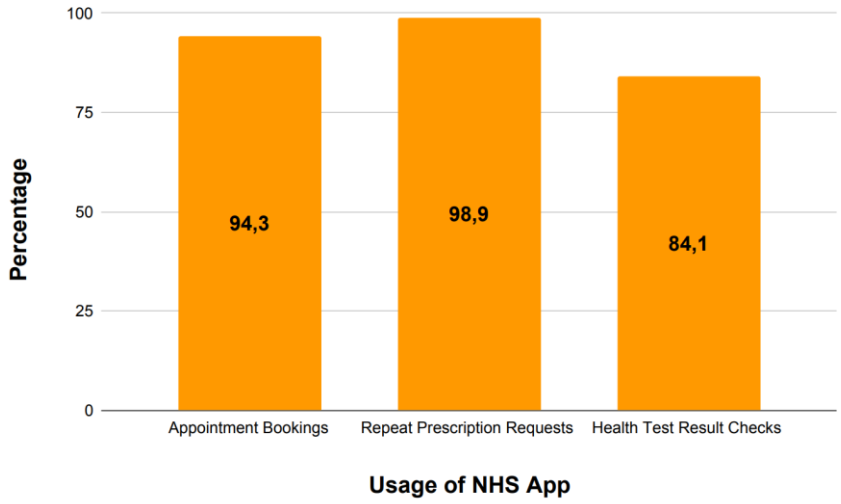

Figure 1. Data of NHS App Usage
Source: Kello et al., 2026

However, greater digital integration has also increased the NHS's exposure to cyber risks. Healthcare services now depend on cloud infrastructure, information systems technology, digital or electronic health records and networked medical devices. Consequently, when there is a cyberattack, the concurrent impact thus could affect clinical and organizational activities beyond the information technology environment itself (Aldosari, 2025; Damar et al., 2024; Sinha, 2024). Elgabry (2023), for example, makes a point to explain that the expansion of the NHS digital environment has created additional security vulnerabilities. This is because when these systems are disrupted, the consequences may affect access to patient data, clinical functions, service continuity and patient safety across the wider healthcare system.

These vulnerabilities, unfortunately, became visible during the 2024 ransomware attack against Synnovis. On June 3, 2024, Synnovis, a pathology partnership involving SYNLAB, Guy's and St Thomas' NHS Foundation Trust, and King's College Hospital NHS Foundation Trust, experienced a ransomware attack that caused a major information technology incident and substantially reduced its capacity to process patient samples (Aash, 2025; Alder, 2024; NHS England, 2024). The attack was attributed to Qilin, a ransomware group reportedly associated with the Russian cybercrime ecosystem (Warren, 2025). The disruption from this attack, thus, affected Guy's and St Thomas' NHS Foundation Trust, King's College Hospital NHS Foundation Trust, and around 194 general practices in South East London that depended on Synnovis services (Rajput et al., 2025; Warren, 2025).

Henceforth, noting the scale of impact created by this attack, the Synnovis incident raises an important problem to be considered and examined. At the immediate level, the

operation was a financially motivated cybercrime. Qilin reportedly demanded a ransom of US$50 million and used the threat of data exposure to pressure the victim into making a payment (Sollof, 2025). At the broader level, the consequences affected critical healthcare infrastructure. The attack constrained diagnostic services, disrupted medical procedures, created risks to patient safety and weakened public confidence in the protection of sensitive health information (Tytler, 2025). This case, therefore, exemplifies an important example of an operation conducted by a non-state criminal group that affected the capacity of institutions connected to the British government to maintain essential healthcare services.

On the other hand, based on the existing research on this scope of study, it provides only a partial explanation of this problem. Healthcare cybersecurity studies have examined some areas such as the digital vulnerabilities, operational disruption, patient safety and organizational resilience (Aldosari, 2025; Damar et al., 2024; Elgabry, 2023; Sinha, 2024). Meanwhile, International Relations scholarship has also tried to analyse cyber incidents in the context of cyber espionage, sabotage, disruption, deterrence and coercion (Brantly, 2020; Hung, 2025; Whyte & Etudo, 2025). Furthermore, another strand from cyber-coercion research has primarily examined relations between states and the ability of governments to use cyber capabilities to influence the behaviour of foreign adversaries (Manantan, 2020; Sharp, 2017; Whyte, 2016).

Despite the growth of various research toward a rigorous examination of this phenomenon, these three bodies of literature still leave a specific research gap. Such healthcare cybersecurity research has explained how digital attacks can disrupt essential services and endanger patient care. Meanwhile, cyber-coercion research has examined how actors use threats and limited harm to influence the behaviour of adversaries. However, less attention has been given to how financially motivated ransomware groups (such as Qilin) generate coercive pressure in cyberspace through the disruption of critical healthcare services and why its severe disruption may still fail to produce the behaviour demanded by the attacker.

Growing out from that missing puzzle piece, an examination of the Synnovis case thus provides an opportunity to address this gap because this case lies at the intersection of cybercoercion and healthcare cybersecurity. In this context, Qilin was a transnational criminal actor whose objective was financial payment. Its leverage, however, depended partly on Synnovis's position within a wider healthcare service network in the UK. Synnovis was the direct organizational target, while the consequences of the attack extended to NHS's healthcare system, patients and the wider public. The case, therefore, raises an important analytical question concerning the relationship between the location of disruption that happens in cyberspace, the distribution of costs, and the decision from the authority. An important puzzle exists: severe system-wide consequences may increase coercive pressure, yet they do not necessarily translate into equivalent leverage over the actor capable of authorizing compliance.

Against this background, the article asks: How can the 2024 Synnovis ransomware attack on the United Kingdom's National Health Service be understood as a form of coercion in cyberspace? To resonate with that question, hence, the study implies three objectives. First,

it identifies the coercer, the direct organizational target, the demanded behaviour and the principal forms of pressure used during the attack. Second, it examines the case through the four elements of cyber coercion developed by Borghard and Lonergan (2017): communication, cost-benefit calculus, credibility and reassurance. Third, it distinguishes the costs imposed by the attack from evidence that those costs altered the target's decision calculus, unveiling the links on why substantial operational, financial, reputational and clinical consequences did not result in ransom payment.

The article, therefore, argues that the Synnovis attack constituted an unsuccessful ransomware-based attempt at coercion. Qilin communicated a financial demand and imposed substantial operational, clinical, financial, reputational and informational costs intended to increase pressure for payment. The group also demonstrated its capability and willingness to inflict further harm through service disruption and the publication of stolen data. However, the available evidence does not establish that these costs changed the relevant decision-maker's preferences sufficiently to make payment preferable to continued resistance. The ransom remained unpaid. Reassurance was also weak because payment could not provide a dependable guarantee of complete system restoration. The case, therefore, demonstrates a situation of cyber coercion where there are substantial cost imposition and credible punishment but without successful coercive conversion.

To unpack that question and line of argumentation, at the general theoretical level, the study draws on Schelling's (1956) understanding of coercion as an attempt to influence behaviour by shaping the relative costs associated with resistance and compliance. At the operational level, it applies Borghard and Lonergan's (2017) framework of coercion in cyberspace. Their framework identifies four connected elements. First, the coercer must communicate the demanded behaviour and the consequences associated with refusal. Second, the coercer attempts to alter the target's cost-benefit calculus by making continued resistance increasingly costly relative to compliance. Third, the threat must be credible, requiring the target to believe that the coercer possesses both the capability and willingness to impose the threatened harm. Fourth, the coercer must provide some reassurance that compliance will result in the termination or withholding of further punishment.

Table 1. Analytical Elements of Coercion in Cyberspace

Analytical element	Theoretical meaning	Application to the Synnovis case
Communication	The coercer communicates the demanded behaviour and the consequences associated with refusal.	Ransom demand, threats of data publication, communication attributed to Qilin, and subsequent publication of stolen data.

Cost-benefit calculus	The coercer attempts to change the relative attractiveness of resistance and compliance by increasing the expected costs of continued refusal.	Evidence of operational, clinical, financial, reputational, and informational costs; assessment of whether these costs changed behaviour; and the observed outcome of non-payment.
Credibility	The target believes that the coercer possesses the capability and willingness to impose the threatened consequences.	Demonstrated access to Synnovis systems, operational disruption, possession of sensitive information, and publication of stolen data.
Reassurance	The target has reason to believe that compliance will reduce or terminate the threatened harm.	Reliability of promises concerning decryption, system restoration, cessation of data publication, deletion of stolen information, and prevention of further exploitation.

Source: Authors' operationalization based on Borghard and Lonergan (2017)

Because Borghard and Lonergan's (2017) framework was developed primarily to examine coercion among states, its application to ransomware requires conceptual adaptation. In this study, Qilin is treated as the coercer, Synnovis as the direct organizational target, and ransom payment as the demanded behaviour. The analysis also distinguishes the direct target from the broader actors experiencing the consequences of the attack. Hospitals, general practices, clinicians and patients absorbed substantial operational and clinical costs even though they were not necessarily responsible for deciding whether the ransom would be paid. This distinction matters because the distribution of harm across an interconnected service network may differ from the distribution of authority over the decision demanded by the coercer.

Accordingly, the four elements are treated as analytical categories rather than indicators that automatically establish coercive success. Communication is assessed through the clarity of the demanded behaviour and the threatened consequences of refusal. Within the cost-benefit dimension, the analysis distinguishes cost imposition, decision pressure and behavioural outcome. Operational disruption, delayed procedures, recovery expenditures, patient-safety risks, data exposure, and reputational consequences establish that costs were imposed. They do not independently establish that those costs altered the target's preferences. Evidence of successful manipulation would require stronger indications that the target moved toward compliance, such as payment, documented changes in negotiation behaviour, or reliable evidence of internal decision-making. Credibility is assessed through Qilin's demonstrated capability and willingness to impose harm, while reassurance concerns whether compliance could credibly be expected to terminate or reduce that harm.

This approach is aimed at making two related contributions. First, it tries to extend cyber-coercion analysis beyond state actors by showing how criminal ransomware can

reproduce several features of coercive bargaining through conditional demands, cost imposition, credible punishment and promises of restraint. Second, it demonstrates that the strategic significance of ransomware depends partly on the relationship between service dependency, cost distribution and decision authority. Synnovis's position within the healthcare service network amplified the consequences of the attack across dependent organizations and patients. Yet the case also demonstrates that widespread systemic harm does not automatically translate into sufficient bargaining leverage over the actor controlling compliance. The analytical significance of the case, therefore, lies in exploring how disruption and unsuccessful coercion can coexist within the cyberspace.

The remainder of the article proceeds as follows. The next section explains the qualitative case-study design, document-selection procedure and theory-guided thematic analysis. The results and discussion section then reconstructs the Synnovis incident and evaluates it through communication, cost-benefit calculus, credibility and reassurance, with particular attention to the distinction between cost imposition and successful behavioural influence. The final section considers the implications of the case for cyber-coercion research, healthcare resilience, critical-supplier governance and the study of ransomware against essential public services.

METHOD

This article utilizes the qualitative research approach in order to observe and examine the 2024 Synnovis ransomware cyberattack on the UK National Health Service (NHS) (Yin, 2016). Reflecting to the research question, qualitative approach is therefore appropriate because the paper seeks to analyze and explore how a cybersecurity attack can be understood from the understanding of coercion in the cyberspace framework. Moving on, the research design uses a case study design (Yin, 2018). A case study was selected because the article will focus on a single event which is the ransomware attack on Synnovis in 2024 and also the following subsequent responses from relevant institutions. In this context, case study design allows the researcher to conduct an in-depth analysis of the relationship between the cyber incident and broader questions of cyber coercion, healthcare infrastructure and international security.

Data were collected through desk review. This technique was used because the available evidence is primarily contained in relevant documentary sources, including government documents, policy documents, official institutional reports, credible news coverage and peer-reviewed journal articles. Barbieri et al. (2025) explain that desk review involves the identification, selection and analysis of documents that may not always be indexed in conventional academic databases, including gray literature, legal texts, institutional reports, and government documents.

The desk review was conducted in three stages. First, a broad search was carried out to identify sources related to Synnovis, the NHS, ransomware, healthcare cybersecurity and coercion in cyberspace. Second, the search was narrowed to institutional and academic sources, including publications from NHS England, the National Cyber Security Centre, UK government policy documents, research reports on ransomware in the healthcare sector, and

journal articles on cybersecurity and International Relations. Third, the collected documents were selected based on their relevance to the research question, the credibility of the source and their analytical value for explaining the Synnovis case as a form of coercion in cyberspace.

For more detail, the documentary search focused primarily on publications produced between 2016 and 2026, covering the development of UK cybersecurity regulation, healthcare cybersecurity, ransomware and the policy environment surrounding the Synnovis attack. Earlier publications were retained when they provided foundational theoretical or methodological concepts required for the study, particularly literature on coercion and reassurance. Academic literature was identified through scholarly databases and search platforms, while official materials were collected from GOV.UK, NHS England, the National Cyber Security Centre, Synnovis and relevant UK government and parliamentary publications. Additional institutional and research reports were included where they provided evidence concerning NHS resilience, critical infrastructure, ransomware or the UK regulatory response.

The search strategy combined incident-specific, sector-specific, theoretical and policy-related terms. These included “Synnovis ransomware,” “Synnovis cyber attack,” “Qilin Synnovis,” “NHS ransomware,” “healthcare ransomware UK,” “healthcare cybersecurity,” “cyber coercion,” “coercion in cyberspace,” “ransomware coercion,” “Cyber Security and Resilience Bill,” “NIS Regulations,” and “critical suppliers cyber security.” A retrospective audit identified 47 unique documents in the final analytical corpus, consisting of peer-reviewed research, theoretical and methodological publications, government and institutional documents, organizational materials, research reports and established journalistic sources.

For the inclusion and exclusion corpus, documents were included when they provided verifiable evidence concerning the Synnovis incident, addressed ransomware or cybersecurity in healthcare and critical infrastructure, contributed theoretical or methodological material relevant to cyber coercion or documented the development of UK cybersecurity policy and institutional responses. Sources were excluded when they duplicated information available from more authoritative material, contained claims that could not be independently traced, addressed unrelated cyber incidents or provided limited empirical or theoretical relevance to the research question. Unverifiable social media material, unattributed online commentary and repetitive news reports were also excluded. Where several sources described the same event, priority was given to official and primary institutional documents, followed by peer-reviewed research and established journalistic reporting.

Moestopo International Review on Societies, Humanities, and Sciences (MIRSHuS)
Vol. 6, No. 2 (2026) pp. 436-455
ISSN: 2775-9601

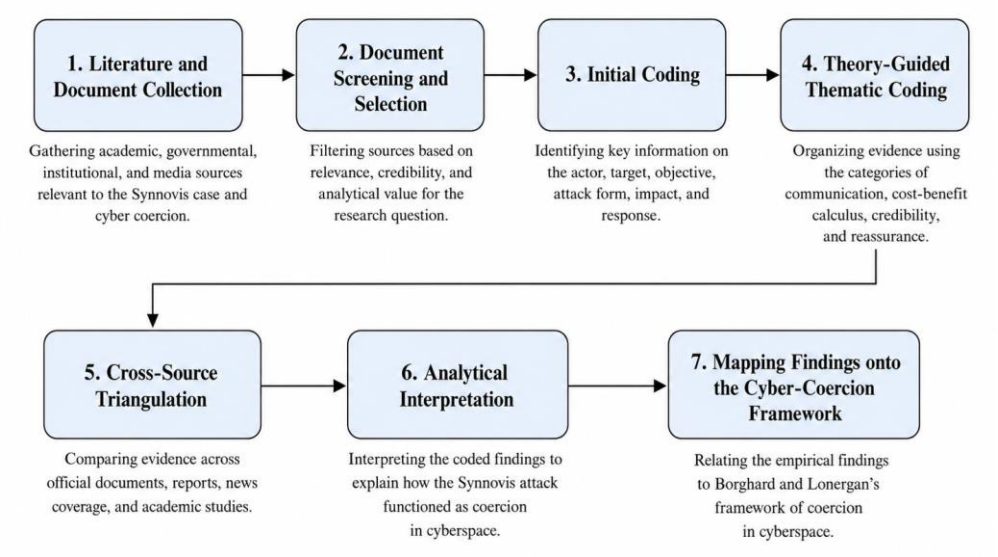

Figure 2. The Research Method and Analytical Process
Soruce: Author's Creation

The collected data were analyzed using thematic analysis developed by Braun and Clarke (2006), as adopted through Byrne's (2021) explanation. The research thus selects thematic analysis because it provides the researcher with the opportunity to identify, analyze and interpret patterns of meaning among all of the qualitative data. The thematic analysis in this article was conducted in a theory-guided manner. This means that the coding process and theme development were informed by Borghard and Lonergan's framework of coercion in cyberspace, particularly its four main elements: communication, cost-benefit calculus, credibility and reassurance. At the same time, the analysis remained open to empirical themes that emerged from the data, including healthcare digital dependency, third-party vulnerability, patient safety, ransomware governance, institutional response and international enforcement limitations (Ahmed et al., 2025).

Operationally, the thematic analysis followed six stages. First, the researcher became familiar with the data by repeatedly reading the collected documents. Second, initial codes were developed based on information related to the actor, target, strategic objective, form of attack, impact, response and elements of coercion. Third, these codes were grouped into preliminary themes, such as ransom communication, cost pressure on the victim, credibility of threats through actual disruption and weak reassurance in ransomware negotiations. Fourth, the themes were reviewed to ensure their consistency with the research question and the empirical evidence. Fifth, each theme was defined and named more precisely. Sixth, the findings will be presented as analytical description or explanation which then connects the evidence with the analytical framework of coercion in cyberspace. Last but not least, the paper has also applied triangulation by comparing information from government documents, institutional reports, credible news coverage and academic articles to prevent an over reliance toward a single source of data while also preserving the credibility of the research findings.

RESULT AND DISCUSSION

The 2024 Ransomware Cyber Attack on Synnovis

The 2024 ransomware attack against Synnovis demonstrates how such disruption to a single healthcare service provider can generate system-wide consequences within a highly digitalized public health system (Grass et al., 2024; Turel, 2025). Synnovis is a pathology partnership established by SYNLAB, Guy's and St Thomas' NHS Foundation Trust, and King's College Hospitals NHS Trust (Synnovis, 2022, 2024). Its role is strategically important because it provides pathology and diagnostic services that support core clinical processes, including blood testing, diagnostics, transfusion processing, sample processing and result reporting. This is why, Synnovis is known as a critical health service because it connects various entities in the NHS healthcare system such as laboratories, hospitals, general practices, clinicians and patients.

To give a sense on how the incident happened, the chronology will be outlined, starting on where the incident began on 3 June 2024, this is where Synnovis got attacked with a ransomware cyberattack with ransom demand of US$50 million (Toparti et al., 2026). The attack thus caused a lockdown of Synnovis systems, restricted access to pathology services, and sharply reduced sample-processing capacity. Noting from Rajput et al. (2025) where it is outlined that the disruption had put an effect on around 194 general practice surgeries in South East London. Preserving consequences include such disruption to patient diagnostics, blood transfusion processing and result reporting. These effects indicate that the attack has thus interrupted the clinical workflow through which NHS providers diagnose, monitor and treat patients.

The actor attributed to the attack was Qilin, a ransomware group commonly associated with the Russian cybercrime ecosystem (Warren, 2025). In this context, Qilin should be understood as a transnational criminal actor. Its motive was financial extortion, yet the effects of its operation reached the level of national healthcare delivery. This distinction is important because the strategic significance of the attack did not derive from the formal status of the perpetrator. It derived from the location of the target within the United Kingdom's critical health infrastructure.

Qilin's association with the incident illustrates the complexity of attribution and communication in contemporary ransomware operations in the cyberspace. In June 2024, Qilin reportedly spoke to the BBC through the encrypted messaging service qTox and attempted to frame the attack as a political protest against the actions of the British government (Warren, 2025). However, the clearest operational logic of the attack remained financial extortion, since the central demand was the payment of a US$50 million ransom.

The direct target of the attack was Synnovis as a pathology provider. The affected population, however, was much broader. The damage which caused by this attack extends also to Guy's and St Thomas' NHS Foundation Trust, King's College Hospital NHS Foundation Trust, primary care services in South East London, 194 general practice surgeries, healthcare workers, patients and the wider public that uses the NHS services (Rajput et al., 2025; Toparti et al., 2026). This evidence thus exemplify in which in a digitally integrated healthcare

ecosystem thus a technical target can become a strategic pressure point when it occupies a central position in the service network.

To give a broader sense, the Synnovis attack perpetuates several severe impacts that were visible in the scale of cancelled and delayed care. Noting from Rajput et al. (2025), it is shown that the disruption has led to cancellation of around 10,152 outpatient appointments which also led to the effect of the postponement of 1,710 elective procedures at Guy's and St Thomas' NHS Foundation Trust and King's College Hospital. This impact derive into a prolonged recovery timeline, it is noted that the recovery to near-normal operating levels can be done after 16 weeks after the initial shutdown. Therefore, it shows in which ransomware attack can produce a sustained operational crisis.

The impact on primary care was also severe. Resources had to be redirected to prioritize hospital-based services due to the impacted blood test processing capacity. Consequently, primary care services in South East London faced hard times in order to obtain timely test results for new diagnoses and urgent medical needs. Rajput et al. (2025) also add a point whereas the impact on primary care is often less visible in public reporting although delays in cancer diagnosis, referrals to secondary care and chronic disease monitoring can generate long-term consequences for patient outcomes.

In addition to clinical disruption, the attack has thus developed into a data breach. Moving on to 20 June 2024, the Qilin group began publishing the stolen data online. This evidence thus indicates that the Synnovis case exemplifies a broader pattern in modern ransomware operations in which encryption, data theft, public exposure are combined to increase pressure on the victim. Noting down from the Synnovis Cyberattack Information Centre, the published data consisted of partial copies from administrative working drives and may have included names, NHS numbers and medical test codes (Synnovis, 2024). Moreover, moving on to the financial impact of the attack. According to Kello et al. (2026) estimation, it is projected that the economic cost of the attack on Synnovis reached around £32.7 million in 2024. These numbers also count the immediate response costs and longer-term recovery efforts.

Based on these dynamics, the strategic objective of the Synnovis attack can be understood as financial extortion through health service disruption. The immediate aim of the perpetrators was to obtain ransom payment. Yet the pressure used to pursue that aim was built through disruption to healthcare services, the risk of patient data exposure, recovery costs and reputational harm to Synnovis and the NHS. The attackers exploited the sensitivity of the healthcare sector as leverage. Because healthcare services have a very low tolerance for downtime, ransomware against this sector can generate stronger pressure than attacks against ordinary commercial organizations.

Ransomware Attack on Synnovis as Coercion in Cyberspace

Borghard and Lonergan (2017) conceptualize coercion as an attempt to influence a target's behaviour by shaping the relative costs of resistance and compliance. Their framework identifies four connected elements: communication, cost-benefit calculus, credibility, and reassurance. Applied to ransomware, these elements provide a useful way to

examine how a criminal actor attempts to transform technical disruption into behavioural pressure. However, their presence should not be merely treated as evidence that coercion has succeeded. This distinction is particularly important in the Synnovis case because Qilin clearly imposed substantial costs, while the demanded ransom payment did not occur. The analysis, therefore, will distinguish between the production of coercive pressure and the successful conversion of that pressure into compliance.

Moving to the first element is communication. For Borghard and Lonergan (2017), coercion requires the target to understand the behaviour being demanded and the consequences associated with refusal. Communication can be difficult in cyberspace because attribution, intention and signaling are often ambiguous. Ransomware partially reduces this problem because the attacker normally communicates a conditional demand directly: payment is requested in exchange for some combination of decryption, restoration or restraint from publishing stolen information.

In the Synnovis case, Qilin's principal demand was relatively clear. The group reportedly demanded approximately US$50 million (Rajput et al., 2025; Toparti et al., 2026). Qilin also communicated through the encrypted messaging service qTox and later spoke to the BBC, where it attempted to frame the attack as a political protest connected to British government actions in an unspecified conflict (Warren, 2025). However, the available evidence does not identify a corresponding political concession demanded from the British government. The financial demand therefore provides the clearest indication of the operation's immediate objective.

Communication was subsequently reinforced through the publication of stolen data on 20 June 2024 after the ransom was not paid (Warren, 2025). Data publication communicated Qilin's willingness to impose an additional consequence following refusal. It also demonstrated that the threat of exposure was actionable rather than merely rhetorical. Accordingly, communication in the Synnovis case was strongest at the level of financial extortion. Qilin communicated the demanded behaviour and demonstrated consequences associated with non-payment, while its broader political claims remained less clearly connected to a specific behavioural demand.

The second element is cost-benefit calculus. In Borghard and Lonergan's (2017) framework, the relevant question is whether the coercer can make compliance sufficiently attractive, or continued resistance sufficiently costly, to change the target's behaviour. To set the stage for this part, evidence that an operation produced damage therefore establishes cost imposition, while successful manipulation of the target's cost-benefit calculus requires stronger evidence that those costs changed the relative attractiveness of resistance and compliance. This distinction matters to underline the condition where severe costs can somehow exist without producing the demanded behaviour, as what will be discussed in the Qilin case afterwards.

Qilin case clearly demonstrated a substantial capacity for cost imposition. First, the attack disrupted pathology systems supporting healthcare services across parts of London. The disruption constrained blood testing, diagnostic services, transfusion processing, sample processing and result reporting. These operational effects subsequently affected clinical

activity. Again, noting Rajput et al. (2025) report, around 10,152 outpatient appointments were cancelled and 1,710 elective procedures were postponed, while 194 general practices in South East London were also affected. These consequences show that compromising Synnovis allowed disruption to extend beyond the directly targeted organization into healthcare providers that depended on its services.

Second, Qilin increased the costs of continued resistance through data exposure. The publication of stolen information created additional privacy, reputational and data-protection consequences because the compromised material involved sensitive health-related information. Third, the interruption of pathology services created potential patient-safety consequences. Delayed diagnostic results, disrupted transfusion processes, postponed procedures and interruptions to routine monitoring transformed the incident from an information-security problem into a healthcare-service disruption. Finally, the financial consequences were substantial. As the estimated cost associated with the incident reached approximately £32.7 million in 2024, including response and recovery expenditures (Kello et al., 2026).

Taken together, these consequences provide strong evidence that Qilin made resistance costly. They do not, however, demonstrate that Qilin successfully changed the target's underlying cost-benefit calculation. As a limitation of this research, the available documentary evidence does not provide sufficient access to Synnovis's internal deliberations, negotiation records, or decision-making process to determine whether decision-makers came to regard payment as preferable to continued resistance. Accordingly, the analysis thus establishes that Qilin attempted to alter the calculus by increasing the costs associated with non-payment.

The behavioural outcome provides an important boundary for this interpretation. The reported US$50 million ransom was not paid. Non-payment does not reveal every consideration that informed the decision and the available evidence does not permit a complete reconstruction of the internal reasoning behind it. Nevertheless, the outcome establishes that the pressure generated by Qilin was insufficient to produce the demanded behaviour. The Synnovis case, therefore, demonstrates substantial cost imposition without evidence of successful cost-benefit manipulation sufficient to secure compliance.

This distinction becomes even more important when considering how the costs were distributed. Synnovis was the direct organizational target, while a significant proportion of the consequences were experienced by NHS trusts, general practices, clinicians and patients. The actors bearing the operational and clinical costs were, therefore, broader than the actor or actors capable of deciding whether the ransom should be paid. In such an interconnected service network, the aggregate severity of harm may exceed the decision pressure experienced by the authority controlling compliance. The case consequently suggests that the coercive value of disruption depends partly on the relationship between where costs are imposed and where decision authority is located.

Moving on, the third element is credibility. A coercive threat becomes credible when the target believes that the coercer possesses both the capability and willingness to impose the threatened consequences. Borghard and Lonergan (2017) emphasize that credibility is

particularly difficult to establish in cyberspace because capabilities are often concealed and intentions are difficult to interpret. In ransomware, however, attackers can establish credibility through observable actions that demonstrate access to systems, possession of data and willingness to escalate harm.

Qilin established considerable credibility through the operational effects of the Synnovis attack. The group demonstrated that it had obtained sufficient access to disrupt pathology services, reduce sample-processing capacity and generate consequences for healthcare providers dependent on Synnovis (Kello et al., 2026). These effects provided observable evidence of capability. The subsequent publication of stolen information further demonstrated willingness to carry out threatened consequences following non-payment.

Data publication strengthened credibility in two respects. First, it demonstrated possession of information that could create further reputational and privacy-related costs for the victim. Second, it showed that Qilin was prepared to impose additional harm after its demand had not been satisfied. Credibility, therefore, arose from demonstrated capability and implemented consequences rather than from Qilin's political statements.

However, credibility of punishment should remain analytically separate from coercive effectiveness. Qilin demonstrated that it could impose harm and follow through on threats, yet this credibility did not produce ransom payment. The case therefore illustrates that credible punishment is an important component of coercive pressure without being sufficient by itself to generate compliance.

The fourth element is reassurance. In coercive bargaining, the target must have some reason to believe that compliance will reduce or terminate the threatened punishment. Borghard and Lonergan (2017) identify this as a persistent difficulty in cyberspace because the target may be unable to verify whether malicious access has been removed, copied information has actually been deleted, or an attacker will refrain from returning. The same difficulty is pronounced in ransomware because the relationship between perpetrator and victim lacks institutional mechanisms for enforcing promises after payment.

Reassurance was, therefore, particularly weak in the Synnovis case. Even if Qilin offered decryption or restraint from further data publication, Synnovis could not independently ensure that compliance would fully terminate the consequences of the attack. Exfiltrated information can be copied, transferred, sold, or reused after payment (Riggs et al., 2023). Moreover, criminal ransomware groups operate outside enforceable contractual relationships, leaving victims without a reliable mechanism to compel them to honor promises concerning deletion or system restoration (Teichmann, 2026). Payment also cannot guarantee that systems will recover quickly or completely.

Weak reassurance changes the cost-benefit problem itself. Payment creates an immediate financial cost while offering uncertain benefits. If the target cannot reliably expect system recovery, permanent deletion of stolen information, or protection against subsequent exploitation, compliance becomes less predictable as a means of reducing harm. In this respect, Qilin's ability to impose substantial punishment was stronger than its ability to provide a credible assurance that payment would terminate that punishment.

The reported non-payment is consistent with this uncertainty, although the documentary evidence does not allow the study to attribute the decision to reassurance alone. Other institutional, financial, legal, reputational or strategic considerations may also have influenced the decision. For this reason, the analysis does not infer the internal reasoning of Synnovis or other relevant decision-makers where direct evidence is unavailable. It instead identifies weak reassurance as a structural limitation of ransomware-based coercion: the perpetrator can demonstrate its ability to cause harm more easily than it can guarantee that compliance will securely terminate that harm.

Taken together, the four elements show that the Synnovis attack possessed a clear coercive structure while producing an unsuccessful coercive outcome. Communication was evident in the ransom demand and threatened consequences of refusal. Cost imposition was substantial, as disruption generated operational, clinical, financial, reputational and informational consequences across the healthcare service network. Credibility was demonstrated through actual disruption and the subsequent publication of stolen data. Reassurance remained comparatively weak because payment offered no dependable guarantee of complete recovery, permanent data deletion or protection from further exploitation.

Most importantly, the case refines how the cost-benefit element should be interpreted in ransomware-based cybercoercion. The magnitude of harm cannot be used as a proxy for successful manipulation of the target's cost-benefit calculus. Qilin demonstrated the capacity to impose severe costs and appears to have designed those costs to increase pressure for payment. The available evidence does not establish that this pressure changed the relevant decision-maker's preferences sufficiently to produce compliance. The ransom remained unpaid. The Synnovis case should, therefore, be understood as an instance of successful cost imposition combined with unsuccessful coercive conversion. It also indicates that cyber coercion against interconnected essential services depends on how disruption, costs and decision authority are distributed across the affected network.

Strategic Implications for International Relations and Cyber Coercion Studies

The Synnovis incident demonstrates that ransomware attacks against healthcare can generate consequences extending well beyond the technical disruption of information systems. By compromising a pathology provider embedded within the NHS service network, Qilin disrupted clinical processes across hospitals and general practices and exposed patients to delayed diagnostic and treatment services (Rajput et al., 2025). The strategic significance of the incident, therefore, arose partly from the relationship between the directly compromised organization and the essential services that depended on it. This suggests that a non-state criminal actor can generate consequences relevant to state capacity when it targets an organization occupying an important position within critical public-service infrastructure.

This finding has implications for how actors and capabilities are understood in International Relations. Strategic threats have traditionally been associated with states, militaries, and politically motivated organizations possessing identifiable political objectives

(Tu et al., 2024). Cyberspace broadens this landscape because actors pursuing predominantly financial objectives can nevertheless produce political and social consequences. Qilin was a transnational ransomware group associated with the Russian cybercrime ecosystem, while its immediate observable objective in the Synnovis operation was financial extortion. Yet the effects of the attack reached NHS pathology services, primary and secondary healthcare providers, patient data, and clinical activity. The case, therefore, indicates that strategic consequences in cyberspace can result from the interaction between an attacker's disruptive capability and the institutional position of its target.

This point also strengthens the connection between cybersecurity and health security. Healthcare systems provide time-sensitive services in which prolonged disruption can affect diagnosis, chronic-disease monitoring, referrals, transfusion services and patient treatment (Bernard et al., 2020; Muthuppalaniappan & Stevenson, 2020; Rajput et al., 2025). Consequently, cybersecurity failures in healthcare can acquire public-safety and national-resilience implications. The Synnovis case is particularly instructive because the immediate technical compromise occurred within one service provider, while the consequences were transmitted through organizations that depended on its pathology capabilities. This pattern demonstrates why the security of healthcare suppliers cannot be separated easily from the resilience of the wider health system.

The United Kingdom's immediate response illustrates the multi-institutional character of cyber incident management. NHS England coordinated measures to maintain urgent healthcare services and redirect parts of pathology processing, while the National Cyber Security Centre, National Crime Agency, Information Commissioner's Office and Synnovis became involved in different technical, investigative, regulatory, and data-protection dimensions of the response (Kello et al., 2026). These actions indicate that ransomware against essential services requires coordination across healthcare administration, cybersecurity, criminal investigation, and data governance. At the same time, the prolonged disruption demonstrates the limitations of response measures once a highly dependent service provider has already been compromised.

Furthermore, the longer-term regulatory implications, such as the emergence of Cyber Security and Resilience Bill, require greater caution. The United Kingdom had already established the Network and Information Systems Regulations in 2018 to improve the security and resilience of essential services, including health. More importantly, the Second Post-Implementation Review published in 2022 had already identified several weaknesses requiring further attention. These included insufficient protection of supply chains where suppliers were critical to essential-service provision, weaknesses in incident reporting, limited regulatory resources, underused enforcement mechanisms and inconsistent implementation across sectors.

The June 2024 attack, hence, subsequently provided a highly visible demonstration of the type of supply-chain vulnerability that earlier reviews had identified. When the government set out its Cyber Security and Resilience Policy Statement in April 2025, it explicitly referred to the ransomware attack on a supplier to NHS hospitals and the postponement of more than 11,000 outpatient appointments and procedures. At the same

time, the policy statement acknowledged that the legislative proposals were also informed by consultations undertaken by the previous government in 2022 and 2023. The interpretation is, therefore, that Synnovis would reinforced the contemporary relevance and urgency of an existing regulatory reform agenda, particularly concerning supply-chain dependency and the resilience of essential services.

The attack also reveals limits to domestic cyber governance when ransomware operations are transnational. The United Kingdom could coordinate service recovery, investigate the incident, address data-protection consequences, and strengthen domestic regulation. Its ability to impose direct consequences on perpetrators operating through transnational criminal networks was more constrained. Attribution remains difficult because ransomware actors can obscure infrastructure, identity and organizational relationships, while investigation and enforcement can require cooperation across jurisdictions (Borghard & Lonergan, 2017). These difficulties become greater where perpetrators operate from jurisdictions in which cooperation with victim states is limited.

Cross-border enforcement, therefore, remains a significant challenge. Investigating ransomware may require information exchange, infrastructure disruption, financial tracing, asset seizure, and coordinated criminal proceedings across several jurisdictions (Akyesilmen & Akdag, 2025). Such coordination can proceed more slowly than ransomware operations themselves. In addition, the Synnovis incident cuts across several governance domains, including cybercrime, healthcare security, data protection, critical infrastructure, and national resilience. Existing international institutions address parts of these problems, while authority and enforcement remain distributed among different legal and institutional arrangements (Li, 2025). The result is a governance environment in which states may possess considerable capacity to mitigate domestic consequences while retaining more limited capacity to suppress the transnational ecosystem producing those attacks.

Furthermore, for cyber-coercion scholarship, the case offers a related theoretical implication. Borghard and Lonergan's (2017) framework was developed primarily in relation to strategic interaction among states, yet Synnovis shows that criminal ransomware can reproduce several components of coercive bargaining. Qilin communicated a demand, imposed costs, demonstrated its capacity and willingness to inflict additional harm, and implicitly offered restraint in exchange for compliance. However, as the preceding analysis demonstrates, these elements did not produce successful coercion. Severe disruption and credible punishment remained insufficient to secure ransom payment.

The case, therefore, extends cyber-coercion research in two related directions. First, it shows that coercive capacity and coercive success should be analysed separately when studying ransomware or other related cybercoercion events. Non-state criminal actors can generate substantial pressure through disruption and data exposure without successfully changing the behaviour of the target. Second, it shows that the strategic consequences of cyber coercion depend partly on the target's position within an interconnected service network. Synnovis was the direct organizational target, while significant costs were distributed across hospitals, general practices, clinicians and patients. The actors experiencing those consequences were not necessarily the actors controlling the payment decision.

Consequently, widespread disruption does not translate automatically into equivalent bargaining leverage.

Taken together, the Synnovis case suggests that ransomware-based coercion should be analysed through the relationship among service dependency, cost distribution, decision authority and behavioural outcome. A criminal actor may exploit an organization whose network position enables disruption to spread across essential public services. Yet the effectiveness of that strategy depends on whether the resulting costs reach the relevant decision-maker in a form sufficient to produce compliance. This distinction explains how an attack can generate substantial national-resilience consequences while remaining unsuccessful in achieving the coercer's immediate demand.

CONCLUSION

This article examined the 2024 Synnovis ransomware attack from the lens of coercion in cyberspace framework. The findings show that Qilin communicated a financial demand and used system disruption and the subsequent publication of stolen information to generate pressure for payment. These actions imposed substantial operational, clinical, financial and reputational costs on Synnovis and the wider NHS service network. However, the available evidence does not establish that these costs altered the relevant decision-maker's preferences sufficiently to make payment preferable to continued resistance. The ransom remained unpaid. The Synnovis incident is, therefore, best understood as an unsuccessful ransomware-based coercive attempt characterized by substantial cost imposition without successful coercive conversion.

The Synnovis case further contributes to cyber-coercion research by showing how the distribution of harm can differ from the distribution of decision authority. Synnovis was the direct organizational target, yet the consequences extended across NHS trusts, general practices, clinicians, patients and other actors dependent on its pathology services. This network position amplified the social and clinical consequences of the attack. At the same time, the actors experiencing those consequences were not necessarily the actors capable of authorizing ransom payment. The case, therefore, suggests that the coercive significance of ransomware depends on the relationship among service dependency, cost distribution, decision authority and behavioural outcome. Severe system-wide disruption can coexist with unsuccessful coercion when the costs generated across a service network do not translate into sufficient pressure on the actor controlling compliance.

The policy implications follow from this distinction. Healthcare resilience cannot be assessed solely at the level of individual organizations because essential services increasingly depend on interconnected suppliers and digital service relationships. The Synnovis incident demonstrates the importance of identifying critical dependencies, strengthening supplier oversight, improving incident reporting and clarifying decision authority during ransomware incidents. It also illustrates vulnerabilities that were already recognized within the United Kingdom's broader cyber-resilience reform agenda. The later development of the regulatory framework should therefore be understood within this longer regulatory trajectory, with Synnovis providing a prominent empirical demonstration of the supply-chain and critical-

supplier risks that the evolving framework seeks to address. International cooperation remains equally important because ransomware groups operate across jurisdictions where attribution, investigation, asset recovery, and enforcement depend on coordination among multiple authorities.

Future research should examine whether these relationships hold across other ransomware incidents involving essential public services. Comparative studies could investigate how organizational ownership, payment policies, supplier concentration and institutional decision structures affect the conversion of imposed costs into compliance. Further research should also examine how reassurance operates in criminal ransomware negotiations and whether the expected benefits of payment differ systematically between public and private organizations. Most importantly, comparative evidence could test whether the separation between the direct target, the actors bearing the consequences and the authority controlling compliance systematically reduces coercive leverage. Such research would clarify when ransomware-generated disruption becomes effective coercion and when severe harm remains insufficient to produce the behaviour demanded by the attacker.

REFERENCE

Aash, P. (2025). Synnovis Data Breach. In *FireCompass*. https://firecompass.com/synnovis-data-breach/

Ahmed, S. K., Mohammed, R. A., Nashwan, A. J., Ibrahim, R. H., Abdalla, A. Q., Ameen, B. M. M., & Khidhir, R. M. (2025). Using Thematic Analysis in Qualitative Research. *Journal of Medicine, Surgery, and Public Health*, *6*(6), 100198. https://doi.org/https://doi.org/10.1016/j.glmedi.2025.100198

Akyesilmen, N., & Akdag, Y. (2025). Norms, Institutions, and Challenges of Multilateral Cooperation. *Insight Turkey*, *27*(2), 313–336. https://doi.org/10.2307/48829617

Alder, S. (2024). Ransomware Group Leaks Data from 300 Million Patient Interactions with NHS. In *The HIPAA Journal*. https://www.hipaajournal.com/care-disrupted-at-london-hospitals-due-to-ransomware-attack-on-pathology-vendor/

Aldosari, B. (2025). Cybersecurity in Healthcare: New Threat to Patient Safety. *Cureus*, *17*(5). https://doi.org/10.7759/cureus.83614

Barbieri, M., Catania, G., Hayter, M., Aleo, G., Zanini, M., Sasso, L., & Bagnasco, A. (2025). Desk review as a methodological approach for identifying policies and gray literature: A case study. *Nursing Outlook*, *73*(6), 102547. https://doi.org/10.1016/j.outlook.2025.102547

Bernard, R., Bowsher, G., & Sullivan, R. (2020). Cyber security and the unexplored threat to global health: a call for global norms. *Global Security: Health, Science and Policy*, *5*(1), 134–141. https://doi.org/10.1080/23779497.2020.1865182

Borghard, E. D., & Lonergan, S. W. (2017). The Logic of Coercion in Cyberspace. *Security Studies*, *26*(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396

Brantly, A. F. (2020). The Evolving Subdiscipline of Cyber Conflict Studies. *The Cyber Defense Review*, *5*(3), 99–120. https://doi.org/10.2307/26954875

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Byrne, D. (2021). A Worked Example of Braun and Clarke's Approach to Reflexive Thematic Analysis. *Quality & Quantity*, *56*(1), 1391–1412.

https://doi.org/https://doi.org/10.1007/s11135-021-01182-y

Cresswell, K., & Williams, R. (2026). Large-scale system-level digitalisation initiatives in the National Health Service in England: insights from three national evaluations. *Npj Digital Medicine*. https://doi.org/10.1038/s41746-026-02495-8

Damar, M., Özen, A., & Yılmaz, A. (2024). Cybersecurity in The Health Sector in The Reality of Artificial Intelligence, And Information Security Conceptually. *Journal of AI*, *8*(1), 61–82. https://doi.org/10.61969/jai.1466340

Elgabry, M. (2023). Towards cyber-biosecurity by design: an experimental approach to Internet-of-Medical-Things design and development. *Crime Science*, *12*(1). https://doi.org/10.1186/s40163-023-00181-8

Grass, E., Pagel, C., Crowe, S., & Ghafur, S. (2024). A stochastic optimisation model to support cybersecurity within the UK national health service. *Journal of the Operational Research Society*, *76*(7), 1–12. https://doi.org/10.1080/01605682.2024.2436063

Hung. (2025). Multilateral cooperation in building critical infrastructure security and resilience: case of American deterrence of Chinese cyberthreats. *Journal of Cyber Policy*, *9*(3), 1–26. https://doi.org/10.1080/23738871.2024.2443421

Kello, M., Hill, S., Hill, Z., & Stevens, T. (2026). *Building NHS Resilience to Ransomware: Central Oversight and Shared Capability Sponsored by White Paper*. https://www.kcl.ac.uk/warstudies/assets/building-nhs-resilience-to-ransomware.pdf

Komariah, K., Hamad, I., & Sari, Y. (2025). Cyber Public Relations Management In The Era Of Public Informations Disclosure. *Moestopo International Review on Social, Humanities, and Sciences*, *5*(1), 62–73. https://doi.org/10.32509/mirshus.v5i1.111

Li, J. (2025). Governing High-Risk Technologies in a Fragmented World: Geopolitical Tensions, Regulatory Gaps, and Institutional Barriers to Global Cooperation. *Fudan Journal of the Humanities and Social Sciences*, *19*. https://doi.org/10.1007/s40647-025-00445-4

Manantan, M. B. (2020). The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea. *Issues & Studies*, *56*(03), 2040013. https://doi.org/10.1142/s1013251120400135

Mauro, M., Noto, G., Prenestini, A., & Sarto, F. (2024). Digital transformation in healthcare: Assessing the role of digital technologies for managerial support processes. *Technological Forecasting and Social Change*, *209*(123781), 123781. https://doi.org/10.1016/j.techfore.2024.123781

Muthuppalaniappan, M., & Stevenson, K. (2020). Healthcare Cyber-Attacks and the COVID-19 Pandemic: an Urgent Threat to Global Health. *International Journal for Quality in Health Care*, *33*(1). https://doi.org/10.1093/intqhc/mzaa117

Neubauer, M., Schick, D., Schreiter, M., Stark, J., Eymann, T., & Schlieter, H. (2026). Bridging digital transformation in public health with digital responsibility. *Electronic Markets*, *36*(1). https://doi.org/10.1007/s12525-025-00868-7

NHS England. (2024). NHS England » Synnovis cyber incident. In *www.england.nhs.uk*. https://www.england.nhs.uk/synnovis-cyber-incident/

Rajput, K., Darzi, A., & Ghafur, S. (2025). Overlooked and under-reported: the impact of cyberattacks on primary care in the UK National Health Service. *The Lancet Digital Health*, *7*(7), 100879. https://doi.org/10.1016/j.landig.2025.100879

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure.

Sensors, *23*(8), 4060. https://doi.org/https://doi.org/10.3390/s23084060

Schelling, T. C. (1956). An Essay on Bargaining. *The American Economic Review*, *46*(3), 281–306. https://www.jstor.org/stable/1805498

Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*, *40*(7), 898–926. https://doi.org/10.1080/01402390.2017.1307741

Sinha, R. (2024). The Role and Impact of New Technologies on Healthcare Systems. *Discover Health Systems*, *3*(1), 1–14. https://doi.org/10.1007/s44250-024-00163-w

Sollof, J. (2025). Cyber attack cost Synnovis estimated £32.7m in 2024. In *Digital Health*. https://www.digitalhealth.net/2025/01/cyber-attack-cost-synnovis-estimated-32-7m-in-2024/

Stoumpos, A. I., Kitsios, F., & Talias, M. A. (2023). Digital Transformation in healthcare: Technology Acceptance and Its Applications. *International Journal of Environmental Research and Public Health*, *20*(4). https://www.mdpi.com/1660-4601/20/4/3407

Synnovis. (2022). About Synnovis. In *Synnovis*. https://www.synnovis.co.uk/about-synnovis

Synnovis. (2024). Cyber Attack Information Centre. In *Synnovis*. https://www.synnovis.co.uk/cyberattack-information-centre

Teichmann, F. (2026). International legal responses to ransomware: toward a ban on payments? *International Cybersecurity Law Review*, *7*. https://doi.org/10.1365/s43439-025-00167-z

Toparti, O., Rajput, K., Darzi, A., & Ghafur, S. (2026). Cybersecurity in connected medical devices: a policy agenda for the NHS. *Npj Digital Medicine*, *9*(1), 204. https://doi.org/10.1038/s41746-026-02534-4

Tu, C.-C., Tien, H.-P., & Hwang, J.-J. (2024). Untangling threat perception in international relations: an empirical analysis of threats posed by China and their implications for security discourse. *Cogent Arts & Humanities*, *11*(1). https://doi.org/10.1080/23311983.2024.2335766

Turel, M. (2025). When Cyberattacks Turn Deadly: The Silent Crisis in Healthcare. *Neurology India*, *73*(3), 565–566. https://doi.org/10.4103/neurol-india.neurol-india-d-25-00348

Tytler, J. (2025). Ransomware attack costs Synnovis GBP 32.7 million | Cyber Intelligence Briefing: 24 January 2025. In *S-rminform.com*. S-RM. https://www.s-rminform.com/cyber-intelligence-briefing/cyber-intelligence-briefing-24-january-2025

Warren, J. (2025). NHS ransomware attack contributed to patient's death. *BBC*. https://www.bbc.com/news/articles/cp3ly4v2kp2o

Whyte, C. (2016). Ending cyber coercion: Computer network attack, exploitation and the case of North Korea. *Comparative Strategy*, *35*(2), 93–102. https://doi.org/10.1080/01495933.2016.1176453

Whyte, C., & Etudo, U. (2025). Finding the thieves amongst the liars: Thinking clearly about cyber-enabled influence operations. *European Journal of International Security*, 1–19. https://doi.org/10.1017/eis.2025.10016

Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). The Guilford Press PP - New York ; London.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Sage Publications PP - Thousand Oaks, California.