NATO OTAN
Science & Technology Organization (STO)

An Approach to Estimate the Impact to Mission Functions Following a Cyber Breach

Maxwell Dondo
Defence Research and Development Canada
Ottawa Research Centre 3701 Carling Avenue
Ottawa ON K2G 6R7
CANADA

maxwell.dondo@drdc-rddc.gc.ca

ABSTRACT

The ability to plan, execute, and oversee military operations relies on well-defined operational functions, which for the Canadian Armed Forces (CAF) are command, sense, act, shield, and sustain. These functions, crucial in collaborative engagements and coalition campaigns, constitute a tailored balance essential for battlespace roles and are increasingly conducted in and through cyberspace. However, the increased frequency and sophistication of cyber attacks targeting the military's operations in and through cyberspace pose a threat to these foundational pillars of military capability, potentially endangering ongoing missions. Understanding the consequences of a cyber breach on these mission functions is therefore imperative for commanders to make informed decisions. To address this need, we propose employing Cyber Damage Assessment (CDA) measures to estimate the impact on specific operational functions following a cyber breach. Our approach involves ingesting operational and business data to determine metrics and measures representing losses resulting from a cyber breach. We then use fuzzy logic to aggregate measures for multiple key performance indicators for cyber damage with commanders' experiential knowledge regarding military capabilities and their corresponding losses, thereby providing estimates to the impacts on specific military functions following a cyber breach. Our results, which are self-consistent, offer impact estimates aligned with commanders' experiential insights, thus providing valuable input for decision-making in the face of a cyber breach scenario.

RESUME

La capacité de planifier, d'exécuter et de superviser des opérations militaires repose sur des fonctions opérationnelles bien définies, qui, pour les Forces armées canadiennes (FAC), sont : commander, détecter, agir, protéger et soutenir. Ces fonctions, essentielles dans les engagements collaboratifs et les campagnes en coalition, constituent un équilibre adapté aux rôles sur le champ de bataille et sont de plus en plus menées dans et par le cyberespace. Cependant, la fréquence et la sophistication croissantes des cyberattaques ciblant les opérations militaires dans et via le cyberespace représentent une menace pour ces piliers fondamentaux de la capacité militaire, mettant potentiellement en péril les missions en cours. Il est donc impératif pour les commandants de comprendre les conséquences d'une violation cybernétique sur ces fonctions opérationnelles afin de prendre des décisions éclairées. Pour répondre à ce besoin, nous proposons d'utiliser des mesures d'évaluation des dommages cybernétiques (CDA – Cyber Damage Assessment) pour estimer l'impact sur des fonctions opérationnelles spécifiques à la suite d'une violation. Notre approche consiste à intégrer des données opérationnelles et commerciales pour déterminer des indicateurs et des mesures représentant les pertes résultant d'une attaque cybernétique. Nous utilisons ensuite la logique floue pour agréger ces mesures à travers plusieurs indicateurs clés de performance des dommages cybernétiques, en les combinant avec les connaissances empiriques des commandants concernant les capacités militaires et les pertes correspondantes, afin de fournir des estimations de l'impact sur des fonctions militaires spécifiques à la suite d'une violation. Nos résultats, cohérents en eux-mêmes, offrent des estimations d'impact en accord avec les connaissances empiriques des commandants, fournissant ainsi des éléments précieux pour la prise de décision face à un scénario de cyberattaque.

KEYWORDS

Cyber breach; Cyber damage; Cyber security; Mission functions

1.0 INTRODUCTION

Joint functions, which for the Canadian Armed Forces (CAF) are command, sense, act, shield, and sustain [1], provide a critical operational framework of related activities and capabilities at all levels that allow commanders to plan, execute, synchronise, and oversee activities in joint operations [1], [2], [3]. These functions, which can be further broken down into subordinate tasks and related capabilities [2], [4], [5], are increasingly conducted in and through cyberspace. This shift makes them vulnerable to disruptive cyber breaches from sophisticated adversaries whose Tactics, Techniques, and Procedures (TTPs) are continuously evolving and increasing in frequency.

A cyber breach involves violating the Confidentiality, Integrity, or Availability (CIA) – the core principles of the CIA triad – of an organization's operations in cyberspace. Such breaches can affect any part of military operations in and through cyberspace, classified or unclassified, across three layers: physical, logical, and persona [3], [6]. At the physical layer, breaches can target Information Technology (IT) assets (e.g., enterprise networks), Operational Technology (OT) (e.g., devices managing physical assets like the Combat Management System (CMS)), or Platform Technology (PT) (e.g., embedded processors like those in Light Armoured Vehicle (LAV) gun controllers) [7]. The logical layer involves attackers targeting software components, such as code, data, firmware, or operating systems. At the persona layer, adversaries may exploit user accounts or identities, potentially using insider threats alongside external TTPs.

The disruptive nature of such attacks means that commanders need to be constantly apprised of their losses and damages to mission-critical capabilities following a cyber breach. This is essential to support their decision-making. For example, a cyber breach on a warship's CMS, means the ship may not be able complete its mission. Timely provision of such knowledge to the commander could allow them to make the decision to abort the mission or to continue with reduced capabilities. As explained in Section 2.0, understanding such impacts also enables commanders and stakeholders to benchmark the performance of their Cyber Intelligence (CyInt) and Cyber Mission Assurance (CMA) frameworks and evaluate the Return On Investment (ROI) of their Defensive Cyber Operations (DCO). Unlike kinetic warfare, where Battle Damage Assessment (BDA) methodologies are well established and widely used to assess the impact of attacks on enemy forces, infrastructure, and capabilities [8], no comparable methodology currently exists for quantifying the impact of cyber breaches, particularly with respect to their effects on mission functions. This gap highlights the urgent need for tools and methodologies that can assess the full scope of damages and losses following a cyber breach, thereby informing operational decisions.

As military operations increasingly depend on cyberspace, the vulnerability of mission-critical functions to cyber breaches has become a pressing concern. Traditional approaches to cyber damage assessments (CDAs) – such as survey-based methods and service-loss enumeration – are inadequate for capturing the complex, multidimensional nature of operational losses caused by cyber attacks [9], [10], [11]. These methods often fail to provide commanders with the comprehensive, real-time insights needed to understand how a cyber breach impacts mission performance.

That means the need for more robust frameworks that will not only quantify direct losses from cyber attacks but also provide timely and actionable insights to commanders regarding how breaches impact mission functions. However, no existing model can yet deliver the kind of comprehensive damage assessment needed to drive informed, real-time decision-making in the immediate wake of a cyber breach.

This paper addresses these challenges by building on prior research that quantified damages and losses resulting from cyber breaches [12], with a focus on mission data, infrastructure assessments, and operational metrics. We propose a novel approach that employs fuzzy logic to integrate these measures with commanders' experiential knowledge of mission disruptions, delivering more precise and actionable estimates of cyber breach impacts on mission functions. By generating dynamic damage and loss profiles from real-time operational data, our methodology equips military commanders with a critical tool for making well-informed, timely decisions to counter cyber threats.

The rest of this paper is organized as follows: Section 2.0 presents the background on CDA and reviews related literature. Section 3.0 describes the methodology and architecture of our proposed model in detail. Section 4.0 presents simulated applications and results. Section 5.0 discusses the importance of our work, while conclusions are drawn in Section 6.0, summarising the implications of our findings and suggesting directions for further research.

2.0 BACKGROUND ON MISSION FUNCTIONS AND CYBER DAMAGE ASSESSMENT

2.1 Mission Functions

Mission tasks are organized into broad functions [5], [13]. For example, CyInt capabilities related to collection, surveillance, and analysis are grouped under the *Sense* function. Disruption of any of these tasks, such as through a cyber breach, can compromise the entire *Sense* function and, by extension, the mission. Although our work focuses on five core mission functions – *Sense, Act, Sustain, Command, and Shield* – our proposed methodology can be extended to include additional functions, such as NATOs eight mission categories.[1]

The *Command* function is concerned with consolidating strategic, operational, or tactical concepts into an integrated framework [14]. It applies to both kinetic and cyber operations, where cyber systems play critical roles in C2 processes. The Sense function acts to provide commanders with knowledge. It is composed of all capabilities related to the collection and processing of data [14]. This function integrates intelligence and operations capabilities to ensure commanders have constant and coordinated Situational Awareness (SA) of the operating environment [2], [13], [14]. Capabilities that integrate manoeuvre, firepower, and information operations to achieve an effect constitute the Act function [14].

The *Shield* function safeguards a force, its capabilities, and its freedom of action in areas of responsibility[14]. Its primary objective is to reduce vulnerabilities in personnel, facilities, equipment, operations, installations, and activities, so that superior operational effectiveness in the conduct of operations is achieved and mission success is assured [2], [14], [15].

The *Sustain* function regenerates and maintains capabilities in support of operations [14]. It achieves this through the provision of personnel, logistics, medical services, and general support associated with military engineering that underpins the imperative for the continuous support and maintenance of forces and their combat capabilities throughout all mission stages [2], [15].

It should be noted that the primary objective of this work was to conduct a detailed and meaningful analysis of damages to mission functions in the context of a cyber breach. By leveraging our expertise with the CAF's operational framework, we were able to derive nuanced insights and provide robust inference data. Conducting a deeper analysis within this familiar context allowed us to generate more applicable and actionable conclusions that might otherwise be diluted in broader or less familiar frameworks. The CAF operates within

[1] Manoeuvre, Fires, Command and Control (C2), Intelligence, Information, Sustainment, Force protection, and Civil-Military cooperation [2].

a distinct national context, where its operational functions are shaped by specific strategic priorities and organizational structures. By focusing on the five core functions, this work ensures relevance and practicality, particularly as these align closely with NATO's priorities (e.g., the Command and Sustain functions are essentially the same). Future research could expand this analysis to NATO's broader operational framework, but our priority in this work was to ensure quality and depth by focusing on familiar contextual data.

2.2 Cyber Damage Assessment

Following a cyber breach[16], disruptions can be analyzed using a CDA, a framework to quantify the losses and damages resulting from such attacks. The CDA serves several purposes: benchmarking CyInt and CMA frameworks, evaluating cybersecurity ROI, optimizing resource allocation, and running what-if scenarios. While ideal CyInt aims to prevent breaches, a CDA provides key metrics to evaluate its effectiveness post-breach. Similarly, a CDA assesses the performance of CMA, which generates probabilistic risk scores to estimate potential losses, offering insights for its refinement and improvement. A CDA is also essential for assessing the ROI of DCO, aiding in resource allocation to strengthen cybersecurity measures.

In addition, a CDA supports the analysis of what-if scenarios, allowing organizations to model potential breach impacts. This capability is particularly valuable during exercises and wargaming, where it helps identify vulnerabilities and refine response strategies. To quantify these disruptions, prior research [12] outlined seven key performance indicators (KPIs) for a cyber breach as summarized in this section.[2]

Recovery (or mitigation) losses (KPI1), which are evaluated in terms of monetary value or time, account for the activity-based impacts associated with deploying an Incident Response Team (IRT) to manage a cyber breach. These impacts include work disruptions, IRT deployment costs, opportunity costs for incident response efforts, etc. [12]. An earlier timeline loss representation [12] facilitates stakeholders to analyze their recovery performance, recognising potential course of action (COA) strategies, and derive insights to enhance future breach responses.

The most common KPI of cyber damage is direct *business losses* (KPI2), encompassing performance penalties, data loss, ransom payments, theft, and so on[11], [12], [17], [18], [19]. According to the McAfee report [16], productivity losses – such as the inability of personnel to work due to a breach (e.g., warship deck crew affected by a compromised deck Machinery Control System (MCS) – are the most significant direct business impact. This is followed by ransomware demands, where criminals extort payments to release encrypted data [20]. Organizations can also incur substantial recovery costs and must invest heavily in safeguarding against competition exploiting stolen Intellectual Property (IP) [20].

Proprietary information losses (KPI3), including personally identifiable information (PII), data, and IP, often result from ransomware, malware, or data exfiltration attacks [12], [21]. Compromised PII can provide attackers with a competitive edge, as seen in claims of Russian data exfiltration by Ukraine, potentially enabling Ukraine to pre-empt Russian missions [22]. Recent high-profile breaches, such as the Solarwinds [23] and National Research Council (NRC) [24] incidents, highlight national security risks, where exposed PII of key personnel could assist adversaries in war planning. Similarly, the loss of IP benefits nation-states and illicit entities, granting strategic or economic advantages. For instance, Ukraine's destruction of Russian research data denies military applications of the research and inflicts financial losses, thereby securing a potential battlespace advantage [25].

[2] For an in-depth analysis of these losses, refer to Ref. [12]. In addition, the taxonomy is available in Appendix 1, Figure A1-9, for ease of reference.

Cyber breaches can significantly damage an organization's *reputation* (KPI4) [11], [16]. For instance, a breach of military cyber infrastructure could diminish public trust in the military's capability to ensure national defence, potentially creating undue pressure on the chain of command.

A direct consequence of a cyber breach is the disruption of operational services, resulting in *opportunity losses* (KPI5) [12]. The inability to fulfill the organization's value proposition represents a significant setback, with opportunity costs highlighting what could have been achieved in the absence of the breach [16], [17].

Wellness losses (KPI6), also referred to as psychological damage by some authors [11], encompass a wide range of well-being impacts on stakeholders, from minor frustrations to severe outcomes, such as loss of life [12]. A cyber breach can trigger negative emotions in stakeholders, potentially creating a toxic work environment and undermining overall morale.

Collateral damage (KPI7), as defined by the Law of Armed Conflict (LOAC) [26], [27], refers to the losses incurred by non-combatants, as well as the damage to their property following a cyber breach. The war in Ukraine provides examples of cyber breaches targeting critical infrastructure, such as the electrical grid [28], causing widespread damage to property, businesses, and lives.

All of the seven types of losses described above could have implications for the execution of mission functions and, in turn, impact the successful fulfilment of joint operations.

2.3 Related Work

2.3.1 Cyber Damage Assessment

There has been significant research on the losses incurred following a cyber breach. Furnell et al. [17] and Heyburn et al. [29] have compiled comprehensive lists to categorise various types of losses resulting from cyber breaches. This work has led to the development of their tool for collecting breach data, highlighting the extent of the problem and the analytical capabilities required to address it. As part of their yearly publications, IBM [9], Verizon [10], and McAfee [16] have recently released their mostly survey-based studies on the damages inflicted on organizations by various types of cyber breaches. However, their data is only informative and has limited use in specific environments, such as in the conduct of joint military missions, which is the subject of this paper.

Agrafiotis et al. [11], similar to Furnell et al. [17] and Heyburn et al. [29], conducted literature surveys to identify cyber damages faced by organizations and separately proposed the development of tools to understand the loss impacts. However, these surveys are proprietary and limited to the organizations that conducted them, making them unavailable for broader utilisation. In earlier work, Dondo et al. developed a taxonomy and framework for CDAs using econometric analytics, partly derived from the Factor Analysis of Information Risk (FAIR) approach [12], [30]. That work decomposes the CDA problem into seven KPIs for cyber damage (see Figure A1-9) and proposes metrics and measures to quantify them. In this paper, we expand upon this foundation by using these KPIs as the cornerstone of our approach.

2.3.2 Mission Characterisation and Impacts

The characterisation of mission functions, which consist of a "number of subordinate tasks and related capabilities..." [2], is not a new concept. In their Mission Function Task Analysis (MFTA) framework, Bernier et al. [5], [13], decomposed the capabilities and activities underpinning Cyber Operations (CO). While the scope of their work was limited to CO, its applicability extends to a broader context, encompassing the characterisation of activities in joint operations. Hence, we utilize their characterisation framework as the foundation for our comprehensive and generalized portrayal of capabilities within joint function contexts.

Extensive information on mission functions and their associated capabilities can be found in military doctrine, orders, and literature [2], [14], [15], [31]. While different categorisations of mission functions exist, their characteristics are very similar. For example, the Department of National Defence (DND)/ CAF Joint Publication breaks down mission activities into five functions [14]. In comparison, the United States (US) Joint Publication categorises them into seven mission functions: command and control, information, intelligence, fires, movement and manoeuvre, protection, sustainment [32]. In addition, the NATO Allied Joint Publication delineates eight functions: manoeuvre, fires, command and control, intelligence, information, sustainment, force protection, and civil-military cooperation [2]. For our research, we adhere to the DND/CAF Joint Publication's characterisations while seeking a broader perspective by consulting literature from US and NATO military publications.

A number of approaches have been used to estimate the impact from cyber attacks on missions. Earlier work by Musman et al. [33], only focus on impacts to operations in cyberspace, while Kim et al. [34] and Jang et al. [35], separately, but with some overlap, extend that estimate to include impacts to other components in kinetic operations. Their approaches are based on the mission dependency model by Jakobson et al. [36]. That work models assets as contributing to function damage, which in turn contribute to task impacts and then mission impacts. Our approach, which uses a different MFTA [5] taxonomy from Jakobson's, is based on a more rigorous coverage of the full spectrum of losses and damages that could be experienced following a cyber breach.

3.0 SELECTED APPROACH: CASE FOR USING FUZZY LOGIC

Previous research has attempted to establish metrics and measures to quantify losses and damages following a cyber breach [17], [35]. However, there remains a gap in methodologies that can translate these losses and damages into actionable estimates of their impacts on mission functions. The formulae utilized in works such as Ref. [34]and [35] do not align with DND/CAF definitions of mission functions [1], [5] and hence are not suitable for our needs. Consequently, we have opted for a different methodology that integrates calculated CDA metrics and measures with Subject Matter Expert (SME) insights into mission function impacts.

There are no accurate mathematical approaches to model the impact of a cyber breach on mission functions. However, a wealth of SME knowledge exists regarding these impacts, which we can leverage effectively. Fuzzy logic has emerged as a powerful methodology for modelling imprecise and uncertain data, making it well suited for this application. Its simplicity, effectiveness, and robustness in handling ambiguity enable more flexible reasoning. In addition, fuzzy logic excels at translating human linguistic expressions into a mathematical form, allowing us to incorporate expert insights with greater fidelity. It excels at converting qualitative statements (e.g., "high precision" or "low damage") into a form that can be processed mathematically, making it ideal for applications involving human expertise and subjective assessments.

While other approaches, such as Dempster-Shafer Theory (DST) and Multi-Attribute Decision-Making (MADM) techniques, could also be used, they are less suited to our needs. DST, though effective for handling conflicting evidence, is more complex to implement and requires more formal evidence representation than fuzzy logic. MADM techniques, used for evaluating and prioritising conflicting criteria, demand a more structured approach to defining attributes and weights, which does not align with the intuitive and qualitative reasoning necessary for our work. Furthermore, prioritisation is not our focus. Therefore, we elected to use fuzzy logic to model SME experiential knowledge regarding the impacts of mission functions for a given level of losses and damages as calculated by the CDA framework [12].

3.1 The Fuzzy Inference System for Mission Function Impacts

3.1.1 Basic Fuzzy Set Theory

The concept of fuzzy logic is centred on a theory to handle uncertainty and imprecision [37], [38]. Consider a collection of objects x in a universal set X, then the fuzzy set $\tilde{A}$ is defined as a set of ordered pairs represented in Equation 1 as:

$$\tilde{A} = \{(x, \mu_{\tilde{A}}(x)) | x \in X\} \tag{1}$$

where $\mu_{\tilde{A}}$ is the membership function of $\tilde{A}$: $\mu_{\tilde{A}} \in [0\ 1]$. It represents the degree by which x belongs to the fuzzy set $\tilde{A}$. An example of a fuzzy set representing an imprecise statement "almost 7" is

$$\tilde{A} = \{(6, 0.2), (7, 0.6), (8, 0.1)\}$$

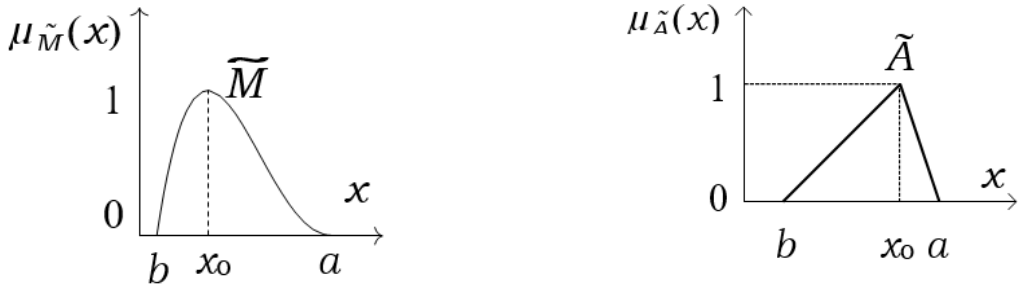
Classical set operations like union and intersection are also applicable to fuzzy set theory and are well documented in the literature [37], [38]. In this work we focus on the conjunction (AND) and disjunction (OR) operations for two fuzzy sets $\tilde{A}$ and $\tilde{B}$, as they are central to our approach. The conjunction and disjunction operations are respectively defined as:

$$\tilde{A} \text{ AND } \tilde{B} = \tilde{A} \cap \tilde{B} = \{(x, min(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x))) | x \in X\} \tag{2}$$

$$\tilde{A} \text{ OR } \tilde{B} = \tilde{A} \cup \tilde{B} = \{(x, max(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x))) | x \in X\} \tag{3}$$

We use both functions extensively throughout this work.

An important type of fuzzy set that we will deal with in this work is the fuzzy number, which is a generalization of real numbers. It is defined as a fuzzy set $\tilde{A}$ that satisfies that $\exists$ one $x_0 : x_0 \in \mathbb{R}$, $\mu_{\tilde{M}}(x_0) = 1$, and $0 \leq \mu_{\tilde{A}}(x) \leq 1$, $\forall x : x \in \mathbb{R}$. Examples of such two fuzzy numbers with a domain of $[b\ a]$ are shown in Figure 1.



(a) A fuzzy number $\tilde{M}$. (b) A triangular fuzzy number $\tilde{A}$.

Figure 1: Examples of fuzzy numbers.

The figure shows generalized and triangular fuzzy numbers, two of the many possible fuzzy membership functions, including triangular, Gaussian, etc. Triangular fuzzy numbers, as illustrated in Figure 1(b) are represented as $\tilde{A} = (b, x_0, a)$. They provide a simple and efficient method for modelling uncertainty, especially when precise data is unavailable [37], [38], [39], [40]. Common in military cyber assessments, they can be

used effectively to translate SME linguistic declarations into clear, interpretable formats for decision-makers. Their computational efficiency and proven success in uncertainty modelling make them an ideal choice for this analysis.

3.1.2 Fuzzy Inference System (FIS)

Decision-making, or the execution of reasoning tasks based on imprecise or uncertain information, is facilitated through a computational framework known as the fuzzy inference system (FIS). The FIS emulates human reasoning by applying fuzzy rules and variables to process input data and generate output results. These rules, expressed in linguistic terms, define the relationship between fuzzy input (antecedents) and output (consequents) variables, allowing the system to handle uncertainty and incorporate expert knowledge, even with incomplete or vague data [38], [41].

Several FIS types exist, such as Takagi, Sugeno, and Kang (TSK), Mamdani, and Tsukamoto, each differing mainly in the structure of their consequents [38], [41], [42]. Mamdani uses general membership functions for consequents, making it simpler and more intuitive, while Sugeno and TSK systems use mathematical functions, offering more precision but greater complexity. For our work, we chose the Mamdani FIS due to its simplicity, suitability for SME linguistic rules, and interpretability.

The FIS consists of four components [42]: a fuzzifier, a rule base, an inference engine, and a defuzzifier, as illustrated in Figure 2. The fuzzifier converts crisp input into a fuzzy value $\tilde{x}$, which is a fuzzy number defined by a membership function. For example, a fuzzy variable might be characterised by three triangular fuzzy numbers: "Low," "Medium," and "High." Fuzzification similarly defines the output fuzzy variable. The number of fuzzy numbers for each variable is determined at the design stage, balancing the required level of granularity with the number of rules needed to effectively represent the model. A higher number of fuzzy numbers increases the number of rules required to characterise the model.

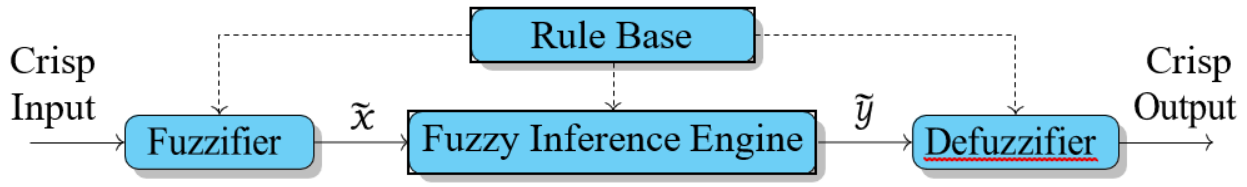


Figure 2: The fuzzy inference system.

The next step is to define fuzzy if-then rules that combine input and output variables using linguistic terms. Consider a problem with N fuzzy input variables $\tilde{x}_n : n = 1, 2, \cdots, N$ and an output variable $\tilde{y}$. Each input $\tilde{x}_n$ has a set of J_n fuzzy values $\{\tilde{A}_{n1}, \tilde{A}_{n2}, \cdots, \tilde{A}_{nJ_n}\}$ and the output has M fuzzy values $\{\tilde{B}_1, \tilde{B}_2, \cdots, \tilde{B}_M\}$. A typical if-then rule i is shown in Equation 4:

$$\text{Rule } i : \textbf{IF} \underbrace{\left((\tilde{x}_1 \text{ is } \tilde{A}_{1j}) \text{ AND } (\tilde{x}_2 \text{ is } \tilde{A}_{2k}) \text{ AND} \cdots\right)}_{\text{antecedent}} \textbf{THEN} \underbrace{(\tilde{y} \text{ is } \tilde{B}_m)}_{consequent} \tag{4}$$

where $1 \leq j, k \leq J_n$ and $1 \leq m \leq M$. The rules used in our work rely solely on the "AND" operator for rule evaluation; the "OR" and "NOT" operators are not utilized in any of our rules.

The FIS engine generates a fuzzy output $\tilde{y}$ from crisp inputs based on the if-then rules, involving two main processes: rule evaluation and rule aggregation. Rule evaluation (implication) applies fuzzy set operators

("AND", in our case) to the antecedents to determine each rule's firing strength. Rule aggregation then uses the fuzzy union "OR" operator (as in Equation 3) to combine the consequents, weighted by the firing strengths, resulting in a fuzzy output $\tilde{y}$.

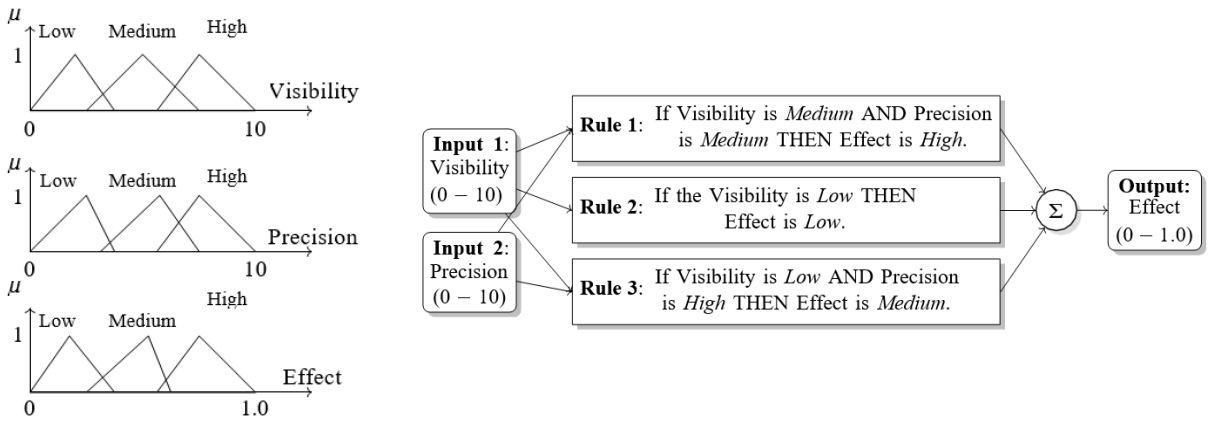
During defuzzification, the fuzzy output $\tilde{y}$ (an inferred membership function) is converted into a crisp value y_c. Various defuzzification methods, such as the centroid and Mean of Maximum (MOM) approaches, each have trade-offs in accuracy, complexity, and suitability for different systems [37], [38]. We chose the centroid method for its simplicity, effectiveness, and widespread use in fuzzy systems. It calculates the centre of gravity of the fuzzy set, yielding the crisp value y_c as follows:

$$y_c = \frac{\sum_i \mu(y_i) y_i}{\sum_i \mu(y_i)} \tag{5}$$

3.2 Illustration Example

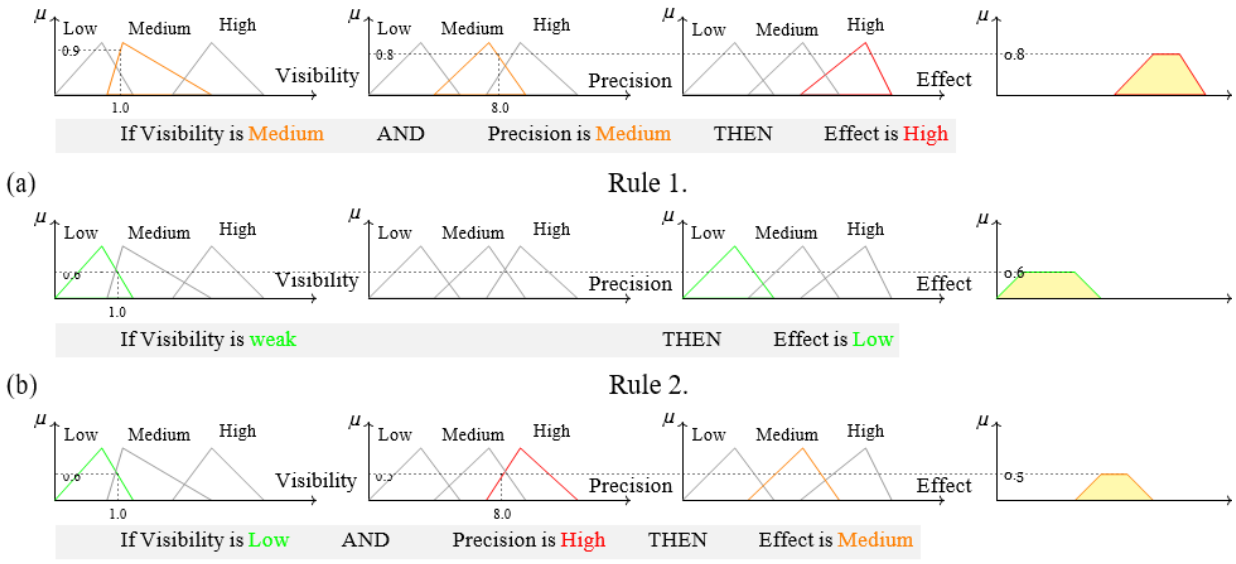
Consider a military effects estimation problem influenced by two factors: *weapon precision* and *target visibility*. An SME might express experiential knowledge in linguistic terms, such as: "When visibility is high and medium precision ordinance is used, the resulting effect is high." This can be formalized as the fuzzy rule: "If Visibility is High and Precision is Medium, then Effect is High." This problem can be effectively modelled using an FIS, as shown in Figure 3, simulating human reasoning with two inputs and one output.

The fuzzification process defines the three fuzzy variables: "Visibility," "Precision," and "Effect," as illustrated in Figure 3(a). Each variable is represented by three triangular fuzzy numbers corresponding to three levels: *Low, Medium,* and *High*. Next, we apply the rules from Figure 3(b) to crisp inputs of Visibility = 1.0 and Precision = 8.0. The resulting inference process is shown in Figure 4.



(a) Fuzzy inputs and output. **(b) The FIS.**

Figure 3: An illustration of a fuzzy inference system.



(c) Rule 3.

(d) Rule aggregation and defuzzification.

Figure 4: Illustration of implementation of the FIS in Figure 3 with crisp inputs of 1.0 and 8.0.

Next, the fuzzy union operator combines all the fuzzy outputs from each rule [43]. This aggregation results in the final fuzzy output, as shown in Figure 4(d). This output can then be defuzzified to produce a crisp value of 0.62, which can be used for decision-making. For a more detailed explanation of fuzzy logic and inference systems, see the literature [38], [40]-[42].

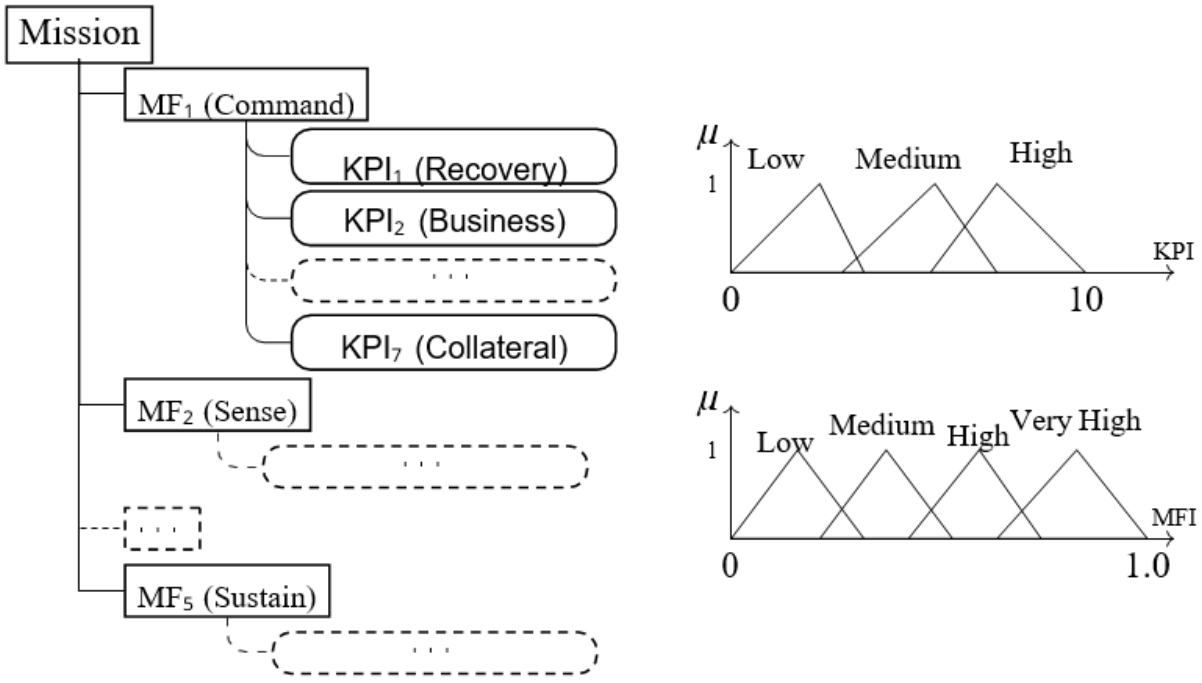
The following section presents our proposed approach for using fuzzy logic to estimate the impact on missions following a cyber breach, using the processes illustrated in Figure 3 to Figure 4.

3.3 Proposed Fuzzy Inference System for Impacts to Mission Functions

To analyze the impact of a cyber breach on the mission functions outlined in Section 2.0, we propose a method to characterise these functions and extract key features for quantifying the resulting damages and losses. Let the five mission functions – Command, Sense, Act, Shield, and Sustain – be denoted by $\mathrm{MF}_i \ \forall i : i = 1,\cdots,5$. Damage to each mission function is characterised using the KPIs for cyber damage, as explained in Section 2.0, and illustrated in Figure 5.

As shown in the figure, each mission function is associated with up to seven KPIs, reflecting how different forms of cyber damages or losses contribute to the overall impact. Where a mission function is impacted by fewer than the seven KPIs, this is accounted for in the rules of the corresponding FIS.

The first step in the analysis is fuzzification. As shown in Figure 5(b), each fuzzy KPI is modelled using three triangular membership functions: "Low," "Medium," and "High." The output mission function impact (mission function impact (MFI)) is represented by four membership functions: "Low," "Medium," "High," and "Very High." These choices of membership functions strike a balance between granularity and scalability while maintaining effectiveness.



(a) Overall model. **(b) KPI and MFI variables.**

Figure 5: The proposed model and the model variables.

Using the selected Mamdani FIS for the inference engine, the impact of a cyber breach on mission function i (MF_i) is determined as follows:

$$\text{Impact on MF}_i = \text{FIS}_i(\text{KPI}_1, \cdots, \text{KPI}_7) \tag{6}$$

where $\text{KPI}_1, \cdots, \text{KPI}_7$ are the crisp values of the fuzzy KPI input variable. The equation is illustrated in Figure 6 for the impact on MF_1. The crisp output MFI_1 represents the mission function impact.

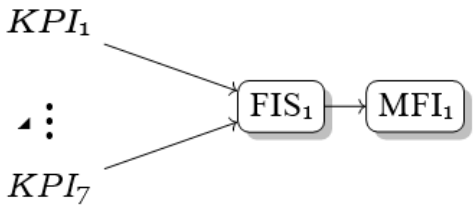


Figure 6: The fuzzy inference system for impacts on mission function MF_1.

The crisp input values in Equation 6, as illustrated in Figure 6, are modelled on a scale in [0 10]. An SME uses experiential knowledge or calculated metrics to assign these values. For example, if there are 100 deck servicemen on a warship and 40 are unable to work due to a cyber breach, then the crisp damage input could be 4. Other metrics, such as the reputation score (KPI4), are already expressed as a percentage and can be mapped to a 1–10 scale (e.g., a 40% reputation score would correspond to a crisp value of 4). This means the lowest input vector to Figure 6 is [0 0 0 0 0 0 0] and the maximum is [10 10 10 10 10 10 10], with the crisp output impact range modelled in [0 1].

The second step is rule generation. As outlined in Section 3.1, we propose to generate rules based on the linguistic declarations by SMEs about mission function impacts after a cyber breach. For example, the statement "*If losses to the recovery process, business continuity, proprietary information, opportunity, wellness, and collateral are all low, then the impact on the Command function should be low"* translates into the fuzzy rule: "*If KPI1 is Low and KPI2 is Low and KPI3 is Low and KPI4 is Low and KPI5 is Low and KPI6 is Low and KPI7 is Low, then MFI is Low*." These rules can be elicited from multiple SMEs using consensus-based methods like the Delphi method [44]. To generate the rules for this project, the author and two additional experts served as the SMEs, drawing on personal expertise and insights from military stakeholders on the impacts of cyber breaches. Given the impracticality of manually drafting all 2,187 possible rules, a novel rule generation assistant that uses the Euclidean distance (see Appendix 2) was developed to make this process less labour-intensive.

In that process, we first establish rules for extreme scenarios of low and very high damage, using the lowest-damage input vector [1 1 1 1 1 1 1] as a baseline, representing "Low" fuzzy values for each KPI. We then calculate the Euclidean distance from this baseline to each input rule vector, up to [3 3 3 3 3 3 3], which represents "High" fuzzy values for each KPI. Using consensus input from the SME, we partition these distances into four clusters corresponding to levels of cyber damage: *Low, Medium, High,* and *Very High*. Each rule is assigned a damage level (consequent) based on its cluster: Cluster 1 corresponds to *Low*, Cluster 2 to *Medium*, Cluster 3 to *High*, and Cluster 4 to *Very High*. A sample of these rules is shown in Table 1.

Table 1: Sample rules.

Count	Antecedent							Consequent	Rules
	KPI1	KPI2	KPI3	KPI4	KPI5	KPI6	KPI7	MFI	
1	1	1	1	1	1	1	1	1	*If KPI1 is Low and KPI2 is Low and KPI3 is Low and KPI4 is Low and KPI5 is Low and KPI6 is Low and KPI7 is Low, then MFI is Low.*
2	1	1	1	1	1	1	2	1	*If KPI1 is Low and KPI2 is Low and KPI3 is Low and KPI4 is Low and KPI5 is Low and KPI6 is Low and KPI7 is Medium, then MFI is Low.*
…									
60	2	2	2	2	2	2	1	2	*If KPI1 is Medium and KPI2 is Medium and KPI3 is Medium and KPI4 is Medium and KPI5 is Medium and KPI6 is Medium and KPI7 is Low, then MFI is Medium.*
…									
2167	3	3	3	3	3	3	3	4	*If KPI1 is High and KPI2 is High and KPI3 is High and KPI4 is High and KPI5 is High and KPI6 is High and KPI7 is High, then MFI is Very High.*

The first column in the table represents the rule count. Columns 2 to 8 represent the antecedents, while Column 9 shows the consequent. The final column presents the complete rule with the assigned antecedents. This defines all the rules needed for our approach. A detailed analysis of this clustering approach is described in Appendix 2. The FIS performs rule evaluation, aggregation, and defuzzification, producing a crisp MFI value, as shown in Figure 6, which is ready for decision-making.

To determine the overall Mission Impact (MI) for a mission following a cyber breach, we aggregate the impacts on each of the Mission Functions (MFs) [41], [42]. A simple approach would be to take the weighted average of the MFIs:

$$\mathrm{MI} = \sum_1^5 w_i \mathrm{MFI_i} \tag{7}$$

where $w_i : i = 1,\cdots,5$ are the weights assigned to each of the mission functions and $\sum_1^5 w_i$=1. However, defuzzifying the MF impacts first may lead to information loss. Therefore, we use a fuzzy aggregation function:

$$\text{Impact on mission} = \cup^5 (\mathrm{MF}_i) \tag{8}$$

Where [37], [38]

$$\tilde{A} \cup \tilde{B} = \{(x, max(\mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x)) \mid x \in X\} \tag{9}$$

The aggregation process is illustrated in Figure 7.

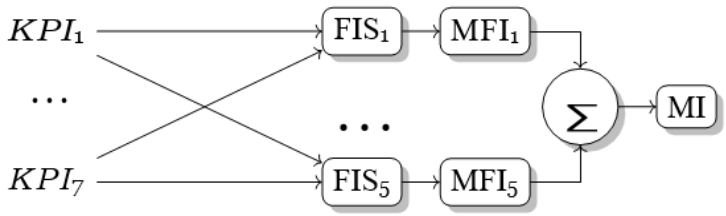


Figure 7: The overall fuzzy inference system for impacts on mission functions.

Each $\mathrm{FIS}_i : i = 1,\cdots,5$ corresponds to a mission function, and if weighting is required, fuzzy logic can incorporate weights into the aggregation. However, for this work, all mission functions are treated equally, with uniform weights of 1 assigned to each.

4.0 APPLICATION EXAMPLE

In this section, we demonstrate our approach through a simulated example.

4.1 Simulation Data

Our work utilized two primary sources of data. The first dataset consists of the KPIs established through the CDA methodology [12], as discussed earlier. Since no specific breaches fully covered the entire spectrum of our model, we simulated various levels of damage and loss representative of different cyber breach scenarios. To map these simulated values to the input space of our model, which ranges in [0 10], we drew on the experiential knowledge of the author and military stakeholders. Using the same CDA methodology, we fuzzified these inputs, along with the anticipated outputs, employing triangular fuzzy numbers as illustrated in Figure 5(b).

We elected to use the following fuzzifications: antecedent KPI={(0, 0, 3); (2, 5, 8); (7, 8, 10)} and consequent MFI = {(0, 0, 0.30); (0.25, 0.5, 0.75); (0.5, 0.75, 1); (0.75, 1, 1)}. These respectively represent the fuzzy categories of (*Low, Medium, High*) for the antecedents and (*Low, Medium, High, Very High*) for the consequents. The chosen triangular fuzzy numbers provide a practical balance of fuzziness and resolution for

both the input and output ranges. They are designed to capture the natural gradual transitions between the fuzzy categories for both antecedents and consequent.

The second dataset consists of a set of rules that map the inputs to the corresponding output, reflecting the impact on mission functions following a cyber breach. These rules, generated using the methodology presented in Section 3.3, capture the relationship between varying levels of damage and the subsequent effects on mission functions. A consensus-based method was employed to partition the Euclidean distances among the rules, with each cluster being assigned to a specific group. This process was repeated for each mission function. A sample of the generated and annotated rules is presented in Table 2.

Table 2: Sample annotated rules for the five mission functions.

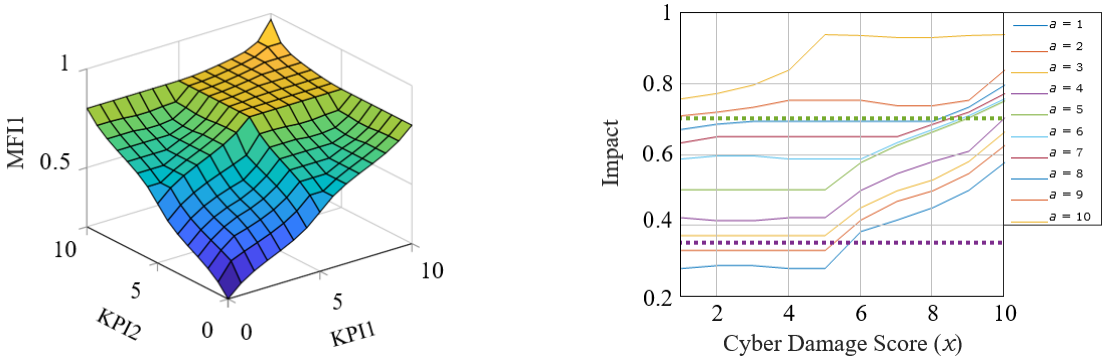
Rule	Command							Sense							Act							Shield							Sustain						
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1
3	1	1	1	1	1	1	3	2	1	1	1	1	1	1	3	1	1	1	1	1	1	3	2	1	1	1	1	1	1	3	2	1	1	1	1	1	3	2
4	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1
5	1	1	1	1	1	2	2	2	1	1	1	1	1	2	2	1	1	1	1	1	1	2	2	1	1	1	1	1	1	2	2	1	1	1	1	1	2	2	1
6	1	1	1	1	1	2	3	2	1	1	1	1	1	2	3	1	1	1	1	1	1	2	3	2	1	1	1	1	1	2	3	2	1	1	1	1	1	2	3	2

From the table, the first column lists the rule number. Columns 2 and 8 represent the fuzzy antecedents for the Command function, and column 9 indicates its consequent. This pattern is repeated for each of the other mission functions. It is important to note that, for the same set of rules, the consequents may differ, reflecting the distinct rule clustering for each mission function.

These rules are processed by the FIS, which supports the reasoning process of the fuzzy model. They encapsulate the expertise and reasoning of SMEs regarding the impact of cyber breaches on mission functions.

4.2 Results

The results of this implementation are illustrated in Figure 8.



(a) Mission function impacts based on two variables.

(b) Variation of impact with damage scores.

Figure 8: Variation of MFIs as a function of the KPIs.

Figure 8(a) shows the fluctuation of an MFI as a function of two selected KPIs. The surface illustrates a continuously increasing impact as the damage levels, represented by the KPIs, worsen. Similar trends were observed for the remaining pairs of KPIs.

Figure 8(b) illustrates a sample evaluation of one of our FISs, specifically the Command function FIS. Two boundaries are set to divide the impact into three granular levels of *Low, Medium,* and *High*, as shown by the two dashed lines. The FIS underwent evaluation against varying inputs using an input vector [*x a a a a a a*], where *x* and *a* represent constants within the range of [0 10]. Initially, *a* was set to a fixed value, followed by successive assignments of values to *x* (representing KPI1) from 0 to 10. These inputs were then sequentially applied to the FIS, ranging from [0 0 0 0 0 0 0] (representing no damage from any of the KPIs) to [10 0 0 0 0 0 0] (representing maximum damage from KPI1 only), and the corresponding output results were recorded. This process continued until the final input [10 10 10 10 10 10 10] (representing maximum damage from all KPIs). The figure shows the variations in mission function impact scores determined through these evaluations.

The figure shows an expected behaviour of increasing mission impacts for a given constant value of *a*, consistent with our expectation that higher damages and losses would correspond to higher impact scores. Within each graph, the impact generally increases with *x*, showing the expected consistency. However, a few graphs show contradicting patterns, such as that for $a = 1$, where an irregular trend is observed at $x = 3$ and $x = 5$. These few instances of non-monotonicity in the impact variation curves likely stem from the coarse-grained Euclidean distances, which assign multiple rules to the same damage levels. This could be addressed by identifying such rules and assigning discriminating weights to differentiate them. However, given the coarseness of our approximation intervals (*Low, Medium, High*), which allow for some fluctuation in scoring, these minor inconsistencies do not undermine the overall promising nature of our results.

The above experiments were repeated for each FIS corresponding to the five mission functions. Although the input and output fuzzy functions and membership functions were consistent across all FISs, each mission function had its own unique set of rules representing the KPIs influencing the impacts relevant to that mission function.

4.3 Test Cases

To evaluate our approach, we conducted three test cases: a generalized case and two specific use cases. These are presented as follows:

Use Case 1: General Case

In the generalized case, we tested ten vectors of normalised CDA damages and losses. We sequentially applied each vector to the five FISs corresponding to the five mission functions and assessed the resulting impacts of the losses represented by the vectors. The summary of these results is presented in Table 3.

Table 3: Sample mission function impact estimates.

KPIs for cyber breach							Mission function impact					MI	
KPI 1	KPI 2	KPI 3	KPI 4	KPI 5	KPI 6	KPI 7	Command	Act	Sense	Sustain	Shield	Aggr[4]	Mean
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.10	0.10	0.10	0.10	0.10	0.10	0.10
2.20	3.10	1.60	3.50	4.80	2.00	2.00	0.38	0.34	0.32	0.34	0.34	0.35	0.34
8.40	10.00	5.30	7.30	6.70	1.00	1.00	0.62	0.64	0.64	0.56	0.64	0.60	0.62
10.00	10.00	10.00	10.00	10.00	10.00	10.00	0.94	0.94	0.94	0.94	0.94	0.94	0.94
7.70	9.50	9.90	9.30	9.80	5.00	3.00	0.72	0.82	0.79	0.72	0.82	0.72	0.78
7.00	7.00	7.00	7.00	7.00	7.00	7.00	0.59	0.59	0.59	0.59	0.59	0.59	0.59
9.00	4.00	9.80	7.00	5.50	2.00	4.00	0.65	0.68	0.66	0.57	0.68	0.60	0.65
5.00	5.00	5.00	5.00	5.00	5.00	5.00	0.45	0.45	0.45	0.45	0.45	0.45	0.45
6.60	5.00	0.60	5.00	2.90	2.00	1.00	0.50	0.45	0.42	0.37	0.45	0.43	0.44
2.00	2.00	2.00	2.00	2.00	2.00	2.00	0.33	0.33	0.33	0.33	0.33	0.33	0.33

[5] Fuzzy aggregation.

In the table, colours green, yellow, and red indicate *low, medium,* and *high* impacts, respectively. The first seven columns represent the KPIs, the subsequent five columns represent the mission function impacts, and the final two columns present the mission impacts calculated using two different methods. For example, in the second row, a random KPI input vector of [2.2 3.1 1.6 3.5 4.8 2.0 2.0] resulted in mission function impacts ranging between [0.32 0.38], corresponding to low to medium impact levels. The aggregation of these mission function impacts produced mission impact scores of 0.35 and 0.34 as shown.

The results align consistently with the FIS reasoning defined by the rules and input data. Notably, rows 4 and 5 exhibit the highest impacts, primarily due to elevated antecedent levels. In addition, the results demonstrate varying impact levels across mission functions, reflecting the individual rules governing each FIS. These observations underscore the effectiveness of the model in accurately representing the nuanced impacts of different input scenarios.

Use Case 2: No Wellness and Collateral Damage Losses

In this scenario, the same antecedent vectors from Table 3 were applied to the FIS, but wellness and collateral damage losses, represented by KPI6 and KPI7, were excluded. The results, which are summarized in Table 4, reveal lower mission impact levels compared to those in Table 3.

Table 4: Sample impact estimates with no KPI6 and KPI7 in the antecedent.

KPIs for cyber breach							Mission function impact					MI	
KPI 1	KPI 2	KPI 3	KPI 4	KPI 5	KPI 6	KPI 7	Command	Act	Sense	Sustain	Shield	Aggr	Mean
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.10	0.10	0.10	0.10	0.10	0.10	0.10
2.20	3.10	1.60	3.50	4.80	0.00	0.00	0.10	0.34	0.10	0.34	0.34	0.34	0.24
8.40	10.00	5.30	7.30	6.70	0.00	0.00	0.52	0.64	0.64	0.56	0.64	0.54	0.60
10.00	10.00	10.00	10.00	10.00	0.00	0.00	0.94	0.94	0.94	0.75	0.94	0.79	0.90
7.70	9.50	9.90	9.30	9.80	0.00	0.00	0.71	0.79	0.77	0.67	0.79	0.70	0.75
7.00	7.00	7.00	7.00	7.00	0.00	0.00	0.51	0.59	0.51	0.57	0.59	0.50	0.55
9.00	4.00	9.80	7.00	5.50	0.00	0.00	0.52	0.66	0.64	0.49	0.66	0.55	0.59
5.00	5.00	5.00	5.00	5.00	0.00	0.00	0.10	0.45	0.10	0.45	0.45	0.36	0.31
6.60	5.00	0.60	5.00	2.90	0.00	0.00	0.10	0.37	0.32	0.37	0.37	0.35	0.30
2.00	2.00	2.00	2.00	2.00	0.00	0.00	0.10	0.33	0.10	0.33	0.33	0.33	0.24

The table shows relatively lower impacts than those presented in Table 3. Notably, the Sustain function exhibits the least impact overall, which is consistent with its FIS rules that assign strong reliance on personnel well-being and collateral damage losses. These results are consistent with the rule model and are plausible, as the Sustain function underpins critical activities such as logistics, infrastructure, and personnel management – domains that are highly dependent on human involvement. Consequently, reductions in wellness-related losses directly result in diminished impacts on Sustain-related capabilities. The overall lower mission impacts observed in this use case are in line with expectations derived from the FIS rules, highlighting the reduced influence of KPI6 and KPI7 losses.

Use Case 3: No Business, Reputational, Collateral damage, and Wellness Losses

The third use case presents a hypothetical scenario. Although it is generally improbable to eliminate business losses entirely – given that recovery efforts for a cyber breach often incur costs – this scenario serves as an academic exercise to isolate the effects of these factors. The results of this simulation are summarized in Table 5.

The table of results once again reflect the input antecedents and the reasoning of the FIS, demonstrating consistent alignment between the two. The Sustain function remains the least impacted, while the Act, Sense, and Shield functions exhibit significant impacts. This is a plausible outcome, as these functions are highly influenced by recovery, proprietary information, and opportunity cost losses.

These results align with expectations, highlighting the reasoning engine's effective implementation of the fuzzy rules.

Table 5: Mission function impact with an antecedent of KPI1, KPI3, and KPI5.

KPIs for cyber breach							Mission function impact					MI	
KPI 1	KPI 2	KPI 3	KPI 4	KPI 5	KPI 6	KPI 7	Command	Act	Sense	Sustain	Shield	Aggr	Mean
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.10	0.10	0.10	0.10	0.10	0.10	0.10
2.20	0.00	1.60	0.00	4.80	0.00	0.00	0.34	0.10	0.10	0.10	0.10	0.34	0.15
8.40	0.00	5.30	0.00	6.70	0.00	0.00	0.47	0.49	0.50	0.39	0.49	0.46	0.47
10.00	0.00	10.00	0.00	10.00	0.00	0.00	0.75	0.75	0.75	0.45	0.75	0.59	0.69
7.70	0.00	9.90	0.00	9.80	0.00	0.00	0.60	0.71	0.73	0.44	0.71	0.58	0.64
7.00	0.00	7.00	0.00	7.00	0.00	0.00	0.57	0.48	0.53	0.33	0.48	0.48	0.48
9.00	0.00	9.80	0.00	5.50	0.00	0.00	0.49	0.65	0.67	0.44	0.65	0.56	0.58
5.00	0.00	5.00	0.00	5.00	0.00	0.00	0.45	0.10	0.10	0.10	0.10	0.36	0.17
6.60	0.00	0.60	0.00	2.90	0.00	0.00	0.37	0.32	0.10	0.32	0.32	0.35	0.28
2.00	0.00	2.00	0.00	2.00	0.00	0.00	0.33	0.10	0.10	0.10	0.10	0.33	0.15

Overall, the results summarized in Table 3, 4 and 5 reflect expected stakeholders' experiential inputs into the impacts on mission functions following a cyber breach. The findings show encouraging consistency, which allows a clear differentiation of various levels of damage or losses to provide estimates of the disruption caused by the breach. Such results hold significance for decision-making processes.

5.0 DISCUSSION

We have developed a novel methodology using fuzzy logic to estimate the impact on mission functions following a cyber breach. The results are presented in the familiar granularity of *Low, Medium,* and *High*, typical in cyber security damage assessments. Such findings hold the potential to guide decision-making processes for stakeholders involved in joint operations. The mission function impact metrics obtained through this work could guide a mission commander in understanding the mission readiness of their capabilities, enabling them to take appropriate courses of action. For example, following a cyber breach, the results of this work can significantly aid commanders in making mission-critical decisions, such as whether to abort a mission, proceed with reduced capabilities, or implement workarounds. In addition to supporting operational decision-making, this work can also be applied to evaluate other decision-making frameworks, such as CyInt, CMA, and DCO. Furthermore, it can assist in resource allocation and provide scenario-based analysis, including running "what-if" scenarios commonly used in wargaming and military exercises.

The results from our approach are fully explainable. We show how the experiential knowledge that SMEs possess about cyber damages and losses can be translated into a relational model using fuzzy logic. By converting the linguistic declarations of SMEs into fuzzy rules, we were able to determine impact scores for various input cyber damage data characterised by its KPIs. These outcomes could help stakeholders in understand the source of the mission function impact score generated by our methodology.

However, there are still some outstanding challenges from our work. Validation of our results is one such challenge. As previously acknowledged by Arcelus et al. [45], the scarcity of verifiable measures in cyber security problems is a challenge we faced in our work. Nevertheless, as emphasised by these researchers,

self-consistency is an acceptable alternative for validation to the classical methodologies. Our results show reasonable self-consistency and, considering the model captures the experiential knowledge of experts, are representative of stakeholders' understanding regarding the impact on mission functions following a cyber breach. The promising results should thus be considered acceptable as reflections of mission function impacts resulting from a cyber breach.

As pointed out in the US Joint Publication (JP) 3-0, "Joint functions are related capabilities" that not only "reinforce and complement one another" but also demonstrate interdependence [32]. Consequently, these functions display a level of correlation that, if not adequately addressed, could result in inaccurate decision-making guidance. While we think our rules mitigate this potential inaccuracy, additional investigation is necessary to provide comprehensive guidance on ensuring independent scores for a given set of input damage data. We defer this aspect to potential future work.

Certain KPIs may be correlated, such as a loss in productivity (a business loss) and opportunity cost losses. While this correlation does not directly affect the inference of individual mission functions, it may influence the aggregation of mission function impacts. Therefore, possible future work could perform further analysis to assess how these correlated KPIs could affect the overall mission impact.

The scale of our problem posed challenges in rule generation, leading to a laborious process prone to inconsistency and errors. While we mitigated this using the Euclidean distance approach, it did not eliminate the few cases where graphs clearly did not exhibit a complete monotonic increase with escalating damage. This labour-intensive aspect could benefit from automated algorithms for improving the generation of consistent rules, potentially utilizing consensus approaches, such as the Delphi method [44], through tabletop exercises. We defer such investigations to potential future work. We focused on five mission functions as defined by the DND/CAF. This could limit the applicability of our approach only to partners that use the same number of mission functions. However, we argue that, although we did not test it in our work, our approach can be used with any mission functions. We defer the thorough testing of such cases to possible future work activities.

Further refinement is also needed to address scalability and granularity. The scale of tasks and capacities within each function group, as highlighted by the extensive entries in the US's Universal Joint Task List (UJTL) [4], presents a challenge. Our current analysis provides high-level insights into mission functions but lacks the granularity needed to address subordinate capabilities. For example, consider a cyber breach on a patrol frigate's Integrated Platform Management System (IPMS). This could disrupt its propulsion system and reduce its ability to manoeuvre – both critical functionalities within a warship's "move" capability, which is a subfunction of the "Act" function group, potentially necessitating the ship's return to the nearest port for repairs [7]. Merely informing the commander that the "Act" function is incapacitated may be insufficient. Although such information is useful, it would require further analysis to identify which specific capabilities within the "Act" function are impaired. Expanding our methodology to include subordinate capabilities would enhance its practical utility. Such refinements would not only improve decision-making precision but also address scalability concerns, making the approach more versatile for broader applications. We also defer such analyses to possible future work.

6.0 CONCLUSION

In this paper, we have introduced a novel methodology for quantifying the impact of cyber breaches on joint mission functions, representing a significant improvement in the assessment and response to cyber threats in military operations. Our approach uses fuzzy logic to combine predefined KPIs for cyber damage with commanders' experiential knowledge of mission function impacts to produce consistent and actionable insights. By classifying impacts as *Low, Medium,* or *High*, our approach provides a nuanced view of how cyber breaches affect individual mission functions and overall mission performance. The results underscore the

utility of our approach in enhancing the decision-making processes of commanders. It equips them with the means to make informed decisions on whether to continue or abort a mission in the aftermath of a cyber breach, based on a clear and quantifiable understanding of its effect on mission-critical capabilities. In addition, our approach supports decision-making on DCO, resource allocation, and the evaluation and improvement of the organization's CyInt and CMA frameworks. Our methodology can also be used to run what-if scenarios that are important in military exercises and wargaming, providing valuable foresight into the handling of potential cyber threats and vulnerabilities.

Future work will focus on integrating this methodology into the existing CDA framework [12], enhancing its applicability within current operational systems. To address the complexity of fuzzy rule generation, future research will aim to optimize and automate the process, reducing its labour-intensive nature and improving scalability. In addition, future work will expand the methodology to include subordinate capabilities within each mission function, further enhancing its practicality and reliability for commanders operating in battlespaces where activities are increasingly conducted in and through cyberspace.

7.0 REFERENCES

[1] Department of National Defence, "Canadian Armed Forces Joint Doctrine Note: Cyber Operations," Department of National Defence, Tech. Rep. JDN 2017-02, 2017.

[2] NATO Standard, "Allied Joint Publication-3 (AJP-3): Allied Joint Doctrine for the Conduct of Operations," North Atlantic Treaty Organization (NATO) Standard, 2019.

[3] Chairman of the Joint Chiefs of Staff (JCS), "Joint Publication (JP): Cyberspace Operations," US Department of Defense, Tech. Rep. JP 3-12, 2018. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3 12.pdf

[4] Joint Chiefs of Staff. (2024) Approved Universal Joint Task List (UJTL) Database. US Department of Defence. [Online]. Available: https://utdt.js.mil

[5] Bernier, M. and Perrett, K. "Mission-Function-Task Analysis for Cyber Defence," Defence Research and Development Canada-Ottawa Research Centre, External Literature DRDC-RDDC-2014- P30, 2014.

[6] NATO, "Allied Joint Doctrine for Cyberspace Operations," Allied Joint Publication, no. AJP 3-20, 2020.

[7] Horobetz, J. and Dondo, M. "Cyber Damage Assessment: Implications of a Cyber Breach on a Royal Canadian Navy Warship's Mission readiness," Defence Research and Development Canada–Ottawa Research Centre, Scientific Report DRDC-RDDC-2024-R073, 2024.

[8] NATO, "Allied Joint Doctrine for Joint Targeting," Allied Joint Publication, no. AJP 3-20, 2021.

[9] IBM, "Cost of a Data Breach: Report 2023," IBM Security, 2023.

[10] Verizon, "2023 Data Breach Investigations Report (DBIR)," Verizon, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[11] Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S., and Upton, D. "A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How they Propagate," Journal of Cybersecurity, 2018. [Online]. Available: https://www.paloaltonetworks.com/blog/2021/06/ the-cost-of-cybersecurity-incidents-the-problem/

[12] Dondo, M. and Nakhla, N., "An Integrated Framework and Taxonomy for Cyber Damage Assessment," in 27th International Command and Control Research & Technology Symposium, Oct. 2022.

[13] Chief of the Defence Staff, "Canadian Armed Forces Joint Doctrine Note: Cyber Operations," Department of National Defence, 2021.

[14] Chief of the Defence Staff, "Canadian Forces Joint Publication 3.0 (CFJP 3.0): Operations," Department of National Defence, 2017.

[15] Chief of the Defence Staff, "Canadian Forces Joint Publication 3.9 (CFJP 3.9): Targeting," Department of National Defence, 2014.

[16] Smith, Z.M., and Lostri, E. "The Hidden Costs of Cybercrime," McAfee, 2020.

[17] Furnell, S., Heyburn, H., Whitehead, A., and Shah, J.N. "Understanding the Full Cost of Cyber Security Breaches," Computer Fraud & Security, vol. 2020, no. 12, pp. 6-12, 2020.

[18] US Department of Justice, "Three Nigerian Nationals Indicted for International Cyber Fraud Conspiracy," 2020. [Online]. Available: https://www.justice.gov/usao-mn/pr/three-nigerian-nationals-indicted-international-cyber-fraud-conspiracy

[19] Gelinne, J., Fancher, J.D., and Mossburg, E. "The Hidden Costs of an IP Breach: Cyber Theft and the Loss of Intellectual Property," Deloitte Review, vol. 19, 2016.

[20] Javers, E. "Here's the Hacking Group Responsible for the Colonial Pipeline Shutdown," 2021. [Online]. Available: https://www.cnbc.com/2021/05/10/hacking-group-darkside-reportedly-responsible-for-colonial-pipeline-shutdown.html

[21] Sobers, R. "98 Must-Know Data Breach Statistics for 2021," Updated 2024. [Online]. Available: https://www.varonis.com/blog/data-breach-statistics

[22] Cluley, G. (2024, Mar.) Ukraine Claims it Hacked Russian Ministry of Defence, Stole Secrets and Encryption Ciphers. Bit-dender. [Online]. Available: https://www.bitdefender.com/blog/hotforsecurity/ukraine-claims-it-hacked-russian-ministry-of-defence-stole-secrets-and-encryption-ciphers/

[23] SolarWinds Corporation, "SolarWinds Corporation," US Securities and Exchange Commission, 2020.

[24] McGuinty, D. "National Security and Intelligence Committee of Parliamentarians: Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," Government of Canada, Tech. Rep., 2022.

[25] Toulas, B. "Ukraine: Hack Wiped 2 Petabytes of Data from Russian Research Center," Jan 2024. Online. BleepingComputer. [Online]. Available: https://www.bleepingcomputer.com/ news/security/ukraine-hack-wiped-2-petabytes-of-data-from-russian-research-center/

[26] Romanosky, S. and Goldman, Z. "Cyber Collateral Damage," Procedia Computer Science, vol. 95, pp. 10-17. Complex Adaptive Systems Los Angeles, CA November 2 – 4, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050916324590

[27] Parks,W.H. "Means and Methods of Warfare," Geo. Wash. Int'l L. Rev., vol. 38, p. 511, 2006.

[28] Pearson, P. "Russian Spies Behind Cyber Attack on Ukraine Power Grid in 2022 – Researchers," Reuters, Nov 2023. [Online]. Available: https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/

[29] Heyburn, H., Whitehead, A., Zanobettiand, L., and Shah, J.N. "Analysis of the Full Costs of Cyber Security Breaches," IPSOS Mori, vol. 2020, no. 12, pp. 6-12, 2020.

[30] Freund, J. and Jones, J. Measuring and Managing Information Risk: A Fair Approach. Butterworth-Heinemann, 2014.

[31] Chief of the Defence Staff, "Canadian Forces Joint Publication 5.0 (CFJP 5.0): The Canadian Forces Operational Planning Process (OPP)," Department of National Defence, 2021.

[32] Joint Chiefs of Staff, "Joint Publication 3-0: Joint Operations," US Department of Defense, 2017.

[33] Musman, S. and Temin, A. "A Cyber Mission Impact Assessment Tool," in 2015 IEEE International Symposium on Technologies for Homeland Security (HST). IEEE, 2015, pp. 1-7.

[34] Kim, S., Jang, J., Kwon, O.-J. Kim, J.-Y., and Shin, D. "Study on Cyber Attack Damage Assessment Framework," IEEE Access, 2022.

[35] Jang, J., Kim, K., Yoon, S., Lee, S., Ahn,M., and Shin, D. "Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated with Cyber Asset Damage," IEEE Access, 2023.

[36] Jakobson, G. "Mission Cyber Security Situation Assessment Using Impact Dependency Graphs," in 14th International Conference on Information Fusion. IEEE, pp. 1-8, 2011.

[37] Zimmermann, H.-J. Fuzzy Set Theory – and Its Applications. Springer Science & Business Media, 2011.

[38] Zimmermann, H.-J., "Fuzzy Set Theory," Wiley Interdisciplinary Reviews: Computational Statistics, vol. 2, no. 3, pp. 317-332, 2010.

[39] Takagi, T. and Sugeno, M. "Fuzzy Identification of Systems and its Applications to Modeling and Control," IEEE Transactions on Systems, Man, and Cybernetics, pp. 116-132, 1985.

[40] Lee, C.-C. "Fuzzy Logic in Control Systems: Fuzzy Logic Controller," IEEE Transactions on Systems, Man, and Cybernetics, vol. 20, no. 2, pp. 404-418, 1990.

[41] MathWorks, "Fuzzy Inference Process," 2023, R2023a. [Online]. Available: https://www.mathworks.com/help/fuzzy/fuzzy-inference-process.html#FP347

[42] Zhang, Y., Wang, G., Zhou, T., Huang, X., Lam, S., Sheng, J., Choi, K.S., Cai, J., and Ding, W. "Takagi-Sugeno-Kang Fuzzy System Fusion: A Survey at Hierarchical, Wide and Stacked Levels," Information fusion, vol. 101, p. 101977, 2024.

[43] Tomasiello, S., Pedrycz, W., and Loia, V. Fuzzy Inference Systems. Cham: Springer International Publishing, 2022, pp. 61-77. [Online]. Available: https://doi.org/10.1007/978-3-030-98974-3_5

[44] Lilja, K.K., Laakso, K., and Palomäki, J. "Using the Delphi Method," in 2011 Proceedings of PICMET '11: Technology Management in the Energy Smart World (PICMET), pp. 1-10, 2011.

[45] Arcelus, A., Perrett, K., Abdellaoui, N., and McKenzie, C. "Enterprise-Level Cyber Security Metrics: Validation Methodology and Sample Metrics Suite," Defence Research and Development Canada–Ottawa Research Centre, Scientific Report DRDC-RDDC-2015-R0294, 2015.

[46] Dondo, M. "Determination of Asset Criticality for Decision Support in Operational Networks," in 24th International Command and Control Research & Technology Symposium 29 – 31 October, Laurel, Maryland USA, 2019.

Appendix 1: TAXONOMY FOR CYBER DAMAGE ASSESSMENT

Figure A1-1 shows the taxonomy for cyber damage as adapted from [12].

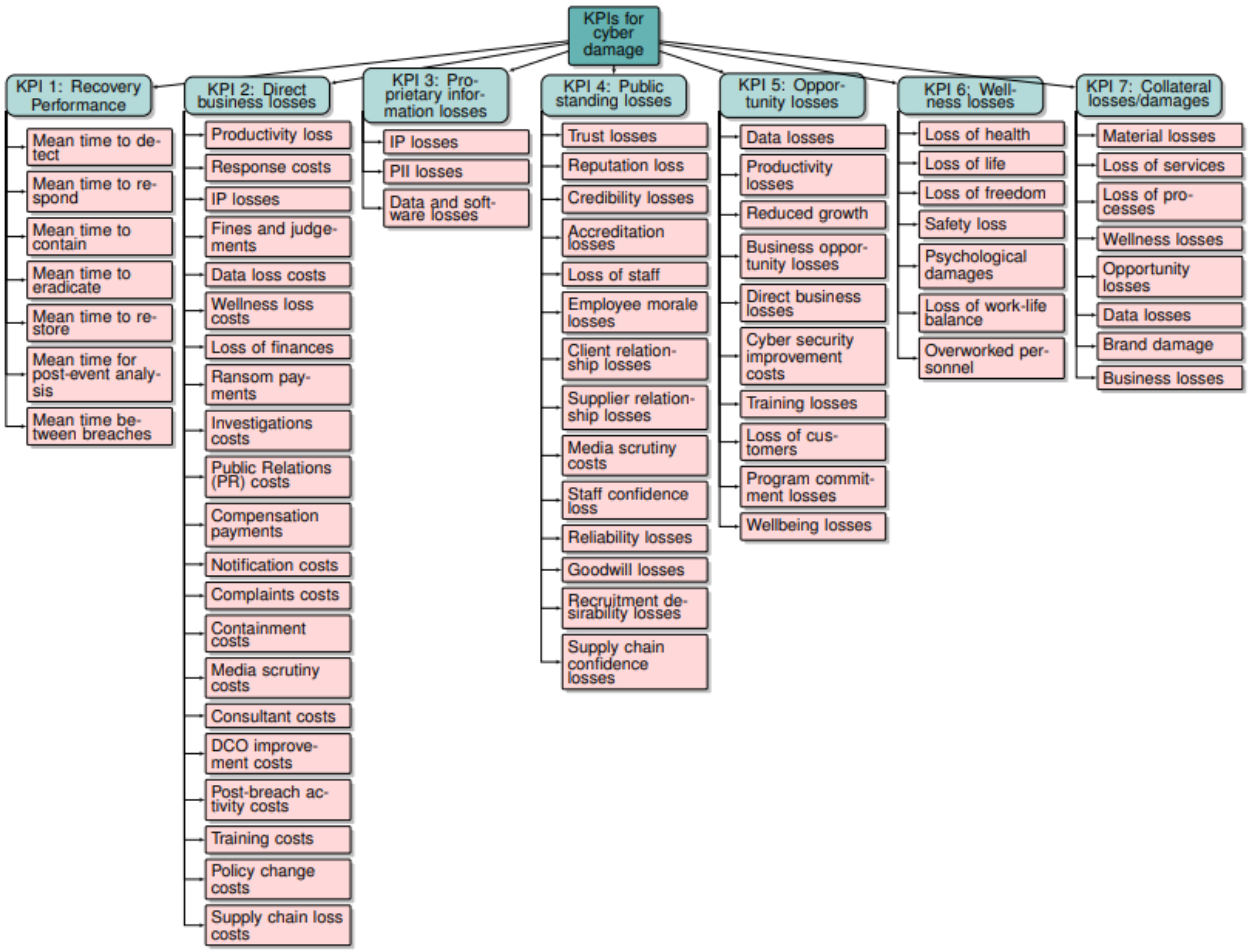


Figure A1-1: Taxonomy for cyber damage adapted from Ref. [12].

Appendix 2: RULE CREATION SUPPORT

In MATLAB[3]-based implementations, rules are compactly annotated to represent their antecedents and consequents [41]. For example, "*If KPI1 is Low and KPI2 is Low and KPI3 is Low and KPI4 is Low and KPI5 is Low and KPI6 is Low and KPI7 is Low, then MFI is Low.*" is represented as "1 1 1 1 1 1 1, 1 (1) : 1". The first seven annotation values correspond to the seven KPIs (the rule's antecedents), with each value indicating the membership function for the respective KPI. Here, all are set to "Low," represented by a 1. The number following the comma represents the consequent, in this case, the *impact to mission functions* for our work. Enclosed within parentheses, the value (1) indicates the rule weight[4]. Lastly, the ":1" represents the logical connective employed, in this case it is exclusively conjunctive.

Given the complexity of generating fuzzy rules for large-scale problems like ours, we propose a distance-based approach to rule creation. We begin by designating the antecedent [1 1 1 1 1 1 1] as the baseline, representing the lowest level of the consequent (impact). Each alternative antecedent combination corresponds to a different level of the consequent. To effectively distinguish these antecedents, we employ a distance clustering technique, which measures the proximity of each antecedent to the baseline.

Let r_0 = [1 1 1 1 1 1 1] be the baseline antecedent, and r_i (i = 1,$\cdots$,N_r) be the subsequent antecedents in a Fuzzy Inference System (FIS) with N_r rules. Initially, we tested the product approach $d_i = \prod_{j=1}^{7} r_{ij}$ for each rule, but it offered poor discrimination, with 93% of the rules occupying only 14% of the range space, leading to significant overlap among the first 2000 rules. Next, we considered the generalized Minkowski distance:

$$d_i = \left(\sum_{j=1}^{7} |r_j - r_0|^p \right)^{\frac{1}{p}}$$

Testing with p = 1 (Manhattan distance) resulted in overly granular distinctions, grouping around 400 rules into the same damage level. However, p = 2 (Euclidean distance) provided much better discrimination, aligning well with stakeholders' assessments. We therefore adopted this approach, leaving room for enhancements in possible future work.

The Euclidian distance d_i between each antecedent vector and the baseline is

$$d_i = \left(\sum_{j=1}^{7} (r_j - r_0)^2 \right)^{\frac{1}{2}}$$

The variations of such distances is show in Figure A2-2.

Through visual inspection, we used the experiential knowledge of a subject matter experts with respect to cyber damage to partition the range of Euclidean distances into four distinct clusters, as depicted in Figure A2-10. The lower section of this division corresponds to antecedent combinations yielding a "Low" (annotated as 1)

[3] The MATLAB Fuzzy Toolbox was used as the working environment for the simulation studies due to its reliability, logical framework, and visual clarity, which are essential for the mathematical operations required in this type of study.

[4] SMEs can assign rule weights as they see fit. Tools that could be used to do the assignment include the Analytic Hierarchy Process (AHP), entropy method, etc. [46].

consequent score. The subsequent division corresponds to a "Medium" (annotated as 2) consequent, followed by the "High" (annotated as 3) and "Very High" (annotated as 4) alternatives. An example of the resultant annotations using this method are shown in Table A2-1.

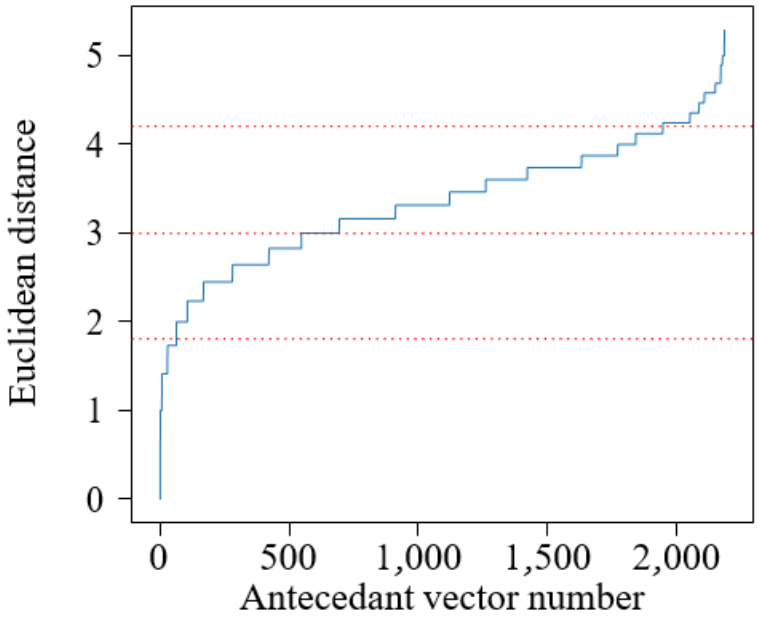


Figure A2-2: Rule clustering by Euclidean distances.

Table A2-1: Table 1 repeated for reader's convenience.

Count	Antecedent							Consequent	Rules
	KPI1	KPI2	KPI3	KPI4	KPI5	KPI6	KPI7	MFI	
1	1	1	1	1	1	1	1	1	*If KPI1 is Low and KPI2 is Low and KPI3 is Low and KPI4 is Low and KPI5 is Low and KPI6 is Low and KPI7 is Low, then MFI is Low.*
2	1	1	1	1	1	1	2	1	*If KPI1 is Low and KPI2 is Low and KPI3 is Low and KPI4 is Low and KPI5 is Low and KPI6 is Low and KPI7 is Medium, then MFI is Low.*
…									
60	2	2	2	2	2	2	1	2	*If KPI1 is Medium and KPI2 is Medium and KPI3 is Medium and KPI4 is Medium and KPI5 is Medium and KPI6 is Medium and KPI7 is Low, then MFI is Medium.*
…									
2167	3	3	3	3	3	3	3	4	*If KPI1 is High and KPI2 is High and KPI3 is High and KPI4 is High and KPI5 is High and KPI6 is High and KPI7 is High, then MFI is Very High.*

The table lists a sample set of fuzzy rules and their annotations. The first column in the table shows the rule count. Columns 2 to 8 show the annotated rule, which is made up of the antecedent. The consequent assigned to each antecedent is shown in Column 9. The next column states the rule, complete with the assigned antecedent.

By comparing the cluster assignments shown in Figure A2-10 with the rules themselves, which ideally capture these clusters, the SME can override these assignments. The SME can substitute them with experiential expert *if-then* rules that better encapsulate the problem at hand – specifically, the impact to missions following a cyber breach. Such overrides can be useful in cases where there are rule overlaps, an exercise that we defer to possible future work.