



ARL-TR-10474 • OCT 2026



Exploratory Modeling of Tactical Cyberspace Windows of Superiority

by M. A. Thomas and Stephen Raio

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.



Exploratory Modeling of Tactical Cyberspace Windows of Superiority

M. A. Thomas and Stephen Raio
DEVCOM Army Research Laboratory

REPORT DOCUMENTATION PAGE

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
October 2026	Technical Report	START DATE July 1, 2025	END DATE March 3, 2026
4. TITLE AND SUBTITLE Exploratory Modeling of Tactical Cyberspace Windows of Superiority			
5a. CONTRACT NUMBER		5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
5d. PROJECT NUMBER		5e. TASK NUMBER	5f. WORK UNIT NUMBER
6. AUTHOR(S) M. A. Thomas and Stephen Raio			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DEVCOM Army Research Laboratory ATTN: FCDD-RLA-ND Aberdeen Proving Ground, MD 21005			8. PERFORMING ORGANIZATION REPORT NUMBER ARL-TR-10474
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.			
13. SUPPLEMENTARY NOTES			
14. ABSTRACT Cyberspace windows of superiority are windows limited in time and scope in which mission execution is unlikely to face prohibitive interference from the cyberspace domain. If commanders could identify or predict such windows, they could increase the chances of successful mission execution by taking advantage of them or by taking steps to create or extend those windows. We use exploratory modeling with synthetic data to consider the feasibility of, and requirements for, a quantitative approach to estimate or predict the existence of a cyberspace window of superiority under the constraints at the tactical edge. The exploratory modeling exercise highlights challenges that must be overcome, including data availability and imbalance, the propagation and communication of imprecise and second-order probability, and the identification and modeling of dependencies, with implications for computational cost. It concludes that tailored solutions will require modular modeling, abstraction, automation, and cloud reachback. A cyberspace window of superiority modeling tool would likely be a component of an automated mission planning tool.			
15. SUBJECT TERMS cyberspace; superiority; mission planning; mission-based cyber risk assessments; multidomain; operations; exploratory modeling; probabilistic modeling; Network, Cyber, and Computational Sciences			
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED	UU 34
19a. NAME OF RESPONSIBLE PERSON Melissa A. Thomas			19b. PHONE NUMBER (Include area code) (520) 713-7868

STANDARD FORM 298 (REV. 5/2020)

Prescribed by ANSI Std. Z39.18

Contents

List of Figures	iv
Acknowledgments	v
Declaration of Generative AI and AI-Assisted Technologies	vi
1. Introduction	1
2. Cyberspace Windows of Superiority: Model Requirements and Constraints	2
3. CWoS Estimation: A High-Level Approach	3
4. A Hierarchical Probabilistic Model to Estimate a CWoS	6
5. Exploratory Modeling	7
5.1 Level 3: Occurrence of External Events That Could Cause Interference	9
5.2 Level 2: Probability of Interference with Mission-Prerequisite Conditions Given the Occurrence of the Events	9
5.3 Standardize the Priors	10
5.4 Level 1: Calculate CWoS	11
6. CWoS Metamodeling Considerations	13
6.1 Data Availability and Imbalance	13
6.2 Imprecise and Second-Order Probability	14
6.3 Dependencies among Conditions	17
7. Conclusion	19
8. References	21
List of Symbols, Abbreviations, and Acronyms	25
Distribution List	26

List of Figures

- Figure 1. An example CWoS problem definition. Mission-critical tasks are supported by systems for which mission-prerequisite conditions are true. “OR” relationships reflect system redundancy..... 5
- Figure 2. Mission-prerequisite conditions over time can be broken into smaller CWoS estimates. For CWoS estimate 1, only motor functionality is required; for CWoS estimate 2, both motor and camera functionality are required. 6
- Figure 3. An example of a three-layer CWoS model. The probability of a CWoS is calculated as the probability of a Boolean statement of the mission-prerequisite conditions. The probability of mission-prerequisite conditions is modeled using Bayesian logistic regression, conditioned on the occurrence of external cyberspace interference events..... 7
- Figure 4. Problem definition of a simple CWoS model. Mission-critical tasks are identified, supporting systems are identified, and external actions and events that could falsify mission-prerequisite conditions are identified. 8
- Figure 5. A posterior predictive kernel density estimation of the probability that the mission-prerequisite condition “LiDAR functions” is satisfied. .. 12

Acknowledgments

The authors would like to thank Dr. Kelly Toppin (ICF International, Inc.), Dr. Joshua Crone (ARL), and Dr. Scott Lathrop (RTX BBN Technologies) for their helpful comments on this report.

Declaration of Generative AI and AI-Assisted Technologies

CamoGPT was used for some AI-assisted coding. All code was personally checked, run, and debugged by the authors. Gemini Enterprise was used to review sections of the report for clarity, to flag potential errors, and to ensure conformity of mathematical notation. The output was reviewed and verified and any resulting corrections were implemented manually by the authors.

1. Introduction

Multidomain operations employ capabilities in the land, air, sea, space, and cyberspace domains. These operations create “windows of superiority” that allow friendly forces to maneuver, create dilemmas for enemy forces, and protect friendly operations (U.S. Army Training and Doctrine Command 2018, p. x–xii). Cyberspace windows of superiority (CWoS) are windows limited in time and scope in which mission execution is unlikely to face prohibitive interference from the cyberspace domain (Raio 2023, p. 5). If commanders could identify or predict such windows, they could increase the chances of successful execution of multidomain missions by taking advantage of them or by taking steps to create or extend those windows.

In previous work, Thomas and Raio (2025) examined existing literature and tools to identify gaps and develop requirements for a quantitative model that would provide estimates to enable tactical commanders to identify, predict, and create a CWoS. They called for a model that could produce explainable, replicable results, make use of modular modeling, and propagate and communicate uncertainty about estimates.

A tactical CWoS model is inherently context-specific, depending on the mission, the supporting systems, the threat, and the operating environment. This means that there cannot be one single model that estimates or predicts the existence of a CWoS. However, there are some characteristics of the problem that would be common to any CWoS modeling effort. To explore the feasibility of developing a CWoS estimate, this report proposes a problem definition process that expands on the process used for mission-based cyber risk assessments (MBCRAs) and describes a high-level modeling approach. Exploratory modeling with synthetic data is then used to apply this approach to identify challenges that CWoS modelers are likely to face. This exercise highlighted challenges of data availability and imbalance, the propagation and communication of imprecise or second-order probability, and identification and modeling of dependencies, with implications for computational cost and feasibility. When coupled with the need to develop models tailored for particular missions and circumstances and the constraints at the tactical edge, these challenges suggest that a CWoS model must be part of a suite of automated mission planning tools and that a CWoS estimate must be thoughtfully scoped.

Section 2 summarizes cyberspace windows of superiority and describes the modeling requirements and constraints as set out in Thomas and Raio (2025). Sections 3 and 4 propose a high-level approach to CWoS modeling, consisting of a process of problem definition and a hierarchical probabilistic model. Section 5 instantiates the model using an illustrative mission, synthetic data, and specific

models to expose possible modeling issues. Section 6 discusses the modeling considerations raised of data availability, imprecise uncertainty, and dependencies, and their implications for computational cost and feasibility. Section 7 concludes.

2. Cyberspace Windows of Superiority: Model Requirements and Constraints

While leveraging a CWoS could increase the chances of successful mission execution, it does not guarantee freedom from prohibitive interference. Raio (2023) uses the term “cyberspace supremacy” to describe such absolute advantage. Moreover, a CWoS is necessarily limited in duration and scope. The scope may be limited to a geographic area, a network or system, to the conduct of certain actions in cyberspace, or some combination. Cyberspace superiority also does not guarantee mission execution, which can fail for reasons unrelated to interference from the cyberspace domain. Finally, cyberspace superiority cannot guarantee achievement of mission objectives, as it is possible to execute a mission as planned but still not achieve objectives.

“Prohibitive interference” occurs when an external action or event affects a mission-critical system and prevents it from providing a functionality or being in a condition or state that is required for mission execution. We define prohibitive interference as being from the cyberspace domain if 1) any external act or event, regardless of provenance, prevents a mission-critical cyberspace system from providing the required functionality or being in the required state; or 2) an external act or event in cyberspace prevents a mission-critical non-cyberspace system from providing the required functionality or being in the required state.

Because a CWoS cannot be directly observed, its present or future existence must be estimated. Thomas and Raio (2025) described the desired characteristics of a model producing a CWoS estimate. The model must capture the entire scope of a CWoS as defined. It must also capture changes over time and phases of the mission, as a given system or system functionality could be critical at one time or in one mission phase and unimportant in another. It would be capable of both identifying CWoS in the present and predicting it over a specified time window for a given scope.

The approach to modeling must be able to incorporate and leverage disparate forms of information. The events that constitute prohibitive interference include high-impact, low-probability, and difficult-to-detect events, such as zero-day cyberspace attacks on friendly tactical systems. Data for modeling is likely to be sparse, unbalanced, and of diverse types, ranging from historical data on system intrusions to subject matter expert (SME) estimates of the probability of occurrence of an event.

Because a CWoS model would be used for high-risk use cases, the estimate must be explainable, defensible, replicable, reproducible, and capable of validation. Moreover, because the existence of a CWoS can only be estimated with uncertainty, this uncertainty must also be communicated to mission owners to provide context for decisions regarding model estimates.

While a review of the literature revealed helpful methodologies and tools, none satisfied those requirements. A CWoS estimate has much in common with a mission-based cyber risk assessment. MBCRAs seek to identify risks to the mission from cyber compromise. MBCRAs use mission and system decomposition to scope the problem by identifying mission-essential tasks and the systems and system functions that support their execution. MBCRAs then analyze the impact of system compromise on the mission. However, with a few notable exceptions, most MBCRAs support decisions to acquire, develop, or improve systems, prioritizing decisions according to the risk a system vulnerability poses to a hypothetical mission (Thomas and Raio 2025). By contrast, a CWoS estimate supports the decision making of multidomain mission owners who would use a CWoS estimate to inform mission planning and execution decisions. They may take evasive, defensive, or offensive action in any domain to increase the likelihood, duration, or scope of a CWoS. They may choose to make changes to the mission itself or to the assignment or configuration of supporting systems to increase the probability of a CWoS or take advantage of one.

Moreover, most MBCRA methodologies reviewed were not suitable for use at the tactical edge. Most are qualitative, produced using SMEs to identify vulnerabilities and score the likelihood of their exploitation and their effect on the mission. These methods may not be available for use in the field because of the lack of SMEs and may not produce explainable, defensible, replicable, or reproducible results desirable for high-risk use cases.

3. CWoS Estimation: A High-Level Approach

This research explores filling that gap by extending the problem definition process used by MBCRAs and defining a high-level probabilistic modeling approach to estimate the probability that all requisite system conditions for mission execution are true. This high-level model could then be populated as needed with mission and system-specific submodels.

Most MBCRAs scope their analyses using mission decomposition and mapping and system mapping to identify mission-critical systems. The proposed CWoS problem definition process extends that approach by requiring definitions of minimum system states or capabilities for the accomplishment of mission-critical

tasks that are combined into a single Boolean statement of mission-prerequisite conditions.

1. ***Mission-critical tasks and standards.*** *The mission owner must define the mission and set the minimum acceptable standards for mission execution,* which reflect the mission owner's intent. Accordingly, problem definition begins with decomposition of the mission into tasks and identification of those mission-critical tasks that must be completed to the prescribed standard to qualify as mission execution in the eyes of the mission owner. The accomplishment of some critical tasks may depend on others; these relationships must also be mapped to, for example, trace the impact of a system compromise through multiple inter-related mission tasks.

2. ***System mapping.*** The systems that will be assigned to support the execution of mission-critical tasks to the minimum standard ("mission-critical systems") must be identified. Because the analysis is limited to cyberspace windows of superiority, only mission-critical cyberspace systems and mission-critical non-cyberspace systems whose required functionality could be affected by cyberspace means are included.

3. ***Identification of mission-prerequisite conditions.*** For each mission-critical system and task, the mission owner or staff must identify those functionalities, conditions, or states that the system must provide to enable execution of the mission-critical task. This would likely be a subset of the system's key performance parameters as identified by the acquisitions community. A "key performance parameter" is a "performance attribute of a system considered critical or essential to the development of an effective military capability" (Department of Defense 2021).

4. ***Boolean statement of mission-prerequisite conditions.*** These system conditions are summarized in a single Boolean statement. Because a CWoS is defined to be a state in which friendly operations are unlikely to face prohibitive interference in cyberspace, and the statement defines the conditions that are necessary to permit friendly operations, by definition, a CWoS exists if this statement is unlikely to be falsified by interference from the cyberspace domain. Because some systems may offer redundant functionality for resiliency, the Boolean statement of required functionalities or conditions may also include "OR" relationships, as shown in Figure 1, where the Boolean statement is *(Condition 1 OR Condition 2) AND (Condition 3 AND Condition 4)*.

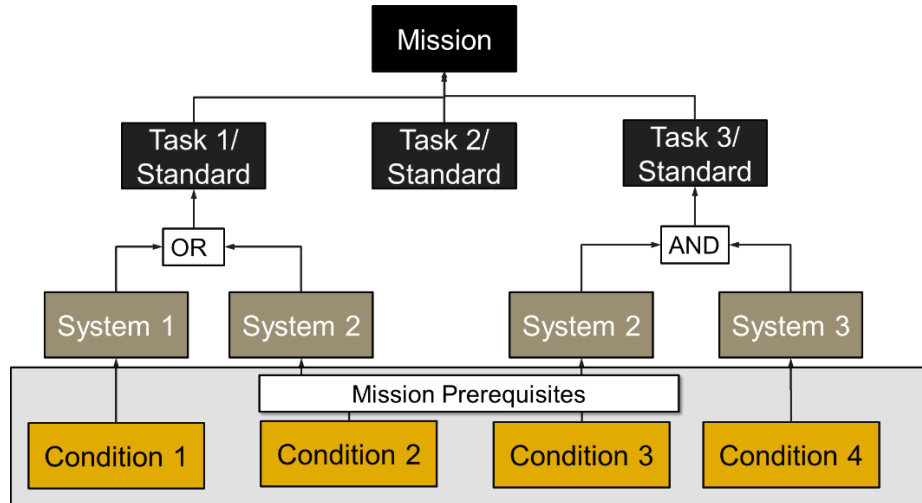


Figure 1. An example CWoS problem definition. Mission-critical tasks are supported by systems for which mission-prerequisite conditions are true. “OR” relationships reflect system redundancy.

5. Specification of problem definitions for distinct time windows or mission phases (optional). The mission owner’s requirements from mission-supporting systems may depend on the time or the mission phase. Mission phases can be modeled separately to produce separate CWoS estimates. It is also possible to imagine a timeline in which the mission owner’s requirements for system functionalities have distinct start and stop times (Figure 2). Problem definition would require specifying this timeline and the start and stop times. The timeline could then be broken into discrete time windows with consistent system requirements and modeled separately to produce separate CWoS estimates. Although it is possible to imagine a variable that changes requirements continuously, the complexity of modeling would likely require discretization.

Problem definition is a necessary, but nontrivial, prerequisite to estimation. Mission tasks, standards, systems, and mission-prerequisite conditions for complicated missions would be extremely difficult for human tactical commanders and staff to specify completely and with granularity. This is especially true given the resource constraints and tight planning time windows under which they operate—perhaps 96 h at the division level and less at lower echelons (Thomas and Raio 2025, p. 20). In addition, missions can be fluid. Missions change in execution and in response to the environment and adversary action. Mission systems may be lost or even gained, changing the system-to-task mapping.

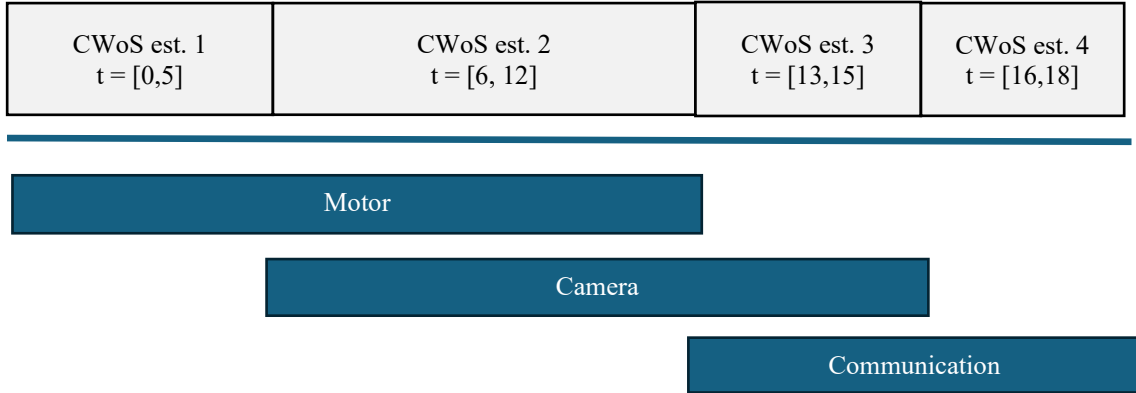


Figure 2. Mission-prerequisite conditions over time can be broken into smaller CWoS estimates. For CWoS estimate 1, only motor functionality is required; for CWoS estimate 2, both motor and camera functionality are required.

We anticipate that this problem definition would be best accomplished with the use of automated mission-planning tools that ingest real-time data on mission parameters, propose courses of action to commanders, and operate locally or have networked reachback to a library of templates, mission or system models, and running estimates. Automation of mission planning is a current, active area of research (BAE Systems 2021; Kane et al. 2021; Defense Advanced Research Projects Agency n.d.). Similarly, the task of developing a tailored CWoS model may not be feasible for human tactical teams given their constraints.

In the interim, it may be possible to develop templates for mission problem definitions for simple, common missions. Customization at the tactical edge may be possible, but would depend on available resources, including time, expertise, and data. It would be important to ensure that the use of automation and templates did not make tactics more predictable.

4. A Hierarchical Probabilistic Model to Estimate a CWoS

The purpose of a CWoS model is to identify and predict a CWoS over a period of interest. In the ideal case, it would have causal traceability that would allow a commander to identify actions that could improve the probability, certainty, or scope of a CWoS or take actions to leverage it for mission execution. We propose a three-level probabilistic model that estimates the probability of a CWoS, equated with the probability that the Boolean statement of mission-prerequisite conditions is true over the period of interest.

In most cases, a CWoS estimate must be expressed as a probability. A CWoS is defined to be a state in which the truth of the Boolean statement of mission-prerequisite conditions is likely. However, the truth of mission-prerequisite

conditions may not be known with certainty in the present, and future conditions cannot be observed or known with certainty. Uncertainty about the truth of the conditions may be both aleatory (due to a random process, irreducible) and epistemic (due to a lack of knowledge, theoretically reducible with further observation).

A CWoS model consists of at least three levels. The top-level model calculates the probability of a CWoS over the period of interest, given the Boolean statement of mission-prerequisite conditions and the probability that each condition is true. The second-level submodels estimate the probability that each condition is true over the period of interest, given the occurrence of interference events. The third-level interference models predict the probability of interference over the time period or mission phase of interest. The structure is a directed acyclic graph, not necessarily a tree, as the same event or act of interference may affect more than one condition or system (Figure 3).

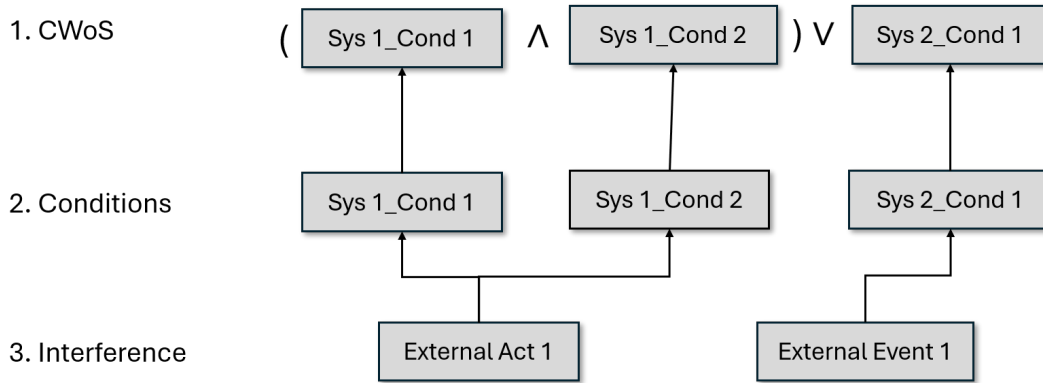


Figure 3. An example of a three-layer CWoS model. The probability of a CWoS is calculated as the probability of a Boolean statement of the mission-prerequisite conditions. The probability of mission-prerequisite conditions is modeled using Bayesian logistic regression, conditioned on the occurrence of external cyberspace interference events.

5. Exploratory Modeling

To identify issues that require further consideration, we modeled a simple, illustrative mission using synthetic data. Here, the purpose of modeling was to identify modeling issues and explore relevant modeling techniques, rather than to estimate empirical relationships. The data are randomly generated. The specific modeling outcomes are not relevant and are not reported.

In this scenario, the mission is to conduct reconnaissance along a path to a location, identifying and reporting people and cars. This mission is conducted in a single phase and has three mission-critical tasks: navigation, object identification, and reporting.

To accomplish these tasks, the commander assigns a single autonomous robot. The robot has several required functionalities or capabilities. It requires a motor and a navigation system to navigate a path; it can use either the camera or light detection and ranging (LiDAR) for object identification along the path; it uses some software algorithm to identify objects; and it must be able to communicate its location and the objects identified across a network. The mission-prerequisite conditions are a functioning *Motor*, *Nav_System*, *Camera or LiDAR*, *Algorithm*, and *Network*. Figure 4 illustrates the model and the mission-prerequisite conditions that must be true for mission execution.

$$p(\text{CWoS}) = p(\text{Motor}) \text{ AND } p(\text{Nav System}) \text{ AND } (p(\text{Camera}) \text{ OR } p(\text{LiDAR})) \text{ AND } p(\text{Algorithm}) \text{ AND } p(\text{Network})$$

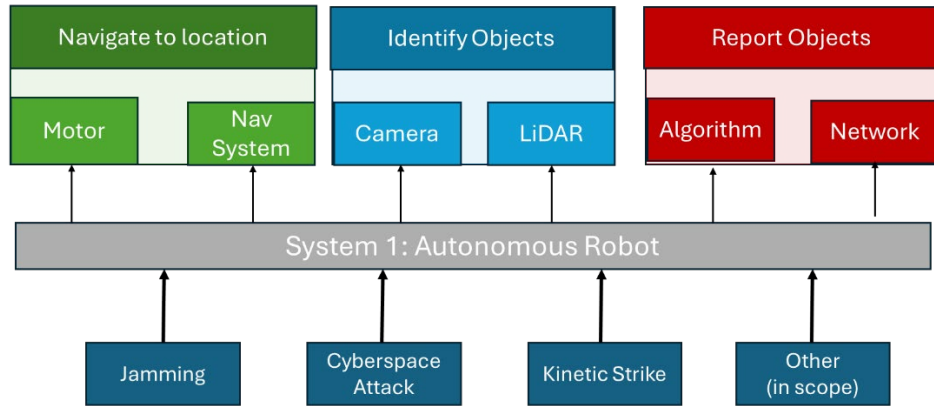


Figure 4. Problem definition of a simple CWoS model. Mission-critical tasks are identified, supporting systems are identified, and external actions and events that could falsify mission-prerequisite conditions are identified.

We could describe the mission-prerequisite conditions more granularly by defining minimum standards to which each task must be accomplished and the system conditions that allow accomplishment of the task to standard. For example, we could define a mission standard that the route must be accomplished within a period of time, t , and a mission-prerequisite condition that the motor that can move the robot at a speed of $\text{route distance}/t$. For this toy case, however, we imagine that tasks are either accomplished or not, and a functioning subsystem provides all necessary functionalities to accomplish the task.

The external events that are explicitly modeled for this scenario that could have an impact on the ability of the system to supply the necessary functionalities are jamming, a cyberspace attack, and a kinetic strike. These are not mutually exclusive or all inclusive. There may be other possible acts of interference; however, they are not modeled here. For simplicity, this model assumes that these events are independent. The cost of modeling dependencies is discussed later in the report.

The model is a three-level probabilistic model for prediction of a CWoS. The model consists of layer three, the probability of occurrence of external events that could cause prohibitive interference in the cyberspace domain, modeled as independent Bernoulli random variables; layer two, which calculates, for each mission-prerequisite condition, the probability that the condition is not falsified because of the occurrence of the events; and layer one, which calculates the probability that the mission-prerequisite conditions have not been falsified because of the occurrence of interference from the cyberspace domain. (Because mission-prerequisite conditions could be falsified by other causes, this cannot be equated with satisfaction of mission-prerequisite conditions or successful mission execution.)

5.1 Level 3: Occurrence of External Events That Could Cause Interference

Each of the interference actions or events is modeled as a Bernoulli random variable that occurs with some probability, p . More formally, let $X = \{X_1, X_2, \dots, X_k\}$ be the set of k binary random variables representing the occurrence of interference events, where $X_i \in \{0,1\}$. For this scenario, $k = 3$:

$$X_1 = X_{Jamming}$$

$$X_2 = X_{Cyberspace}$$

$$X_3 = X_{Kinetic}$$

The probability of occurrence of each of these events is $\pi_i \in [0,1]$:

$$X_i \sim \text{Bernoulli}(\pi_i), \text{ where } E[X_i] = \pi_i$$

For this simple model, we assume that these events are independent. However, they could be dependent if, for example, the missions were conducted during a conflict in which an adversary took multiple actions to interfere. Modeling begins with a draw of the occurrence of these events, given this distribution.

5.2 Level 2: Probability of Interference with Mission-Prerequisite Conditions Given the Occurrence of the Events

Let $C = \{C_1, C_2, \dots, C_n\}$ be the set of mission-prerequisite conditions. Here, $n = 6$:

$$C = \{C_{Motor}, C_{Nav_system}, C_{Camera}, C_{LiDAR}, C_{Algorithm}, C_{Network}\}$$

For each condition, the probability that the condition will not be prohibited by interference from the cyberspace domain is modeled as the outcome of a Bayesian logistic regression with the interference events as predictor variables.

Let p_j be the probability that the mission-prerequisite condition C_j faces no prohibitive interference from the cyberspace domain, given the occurrence of cyberspace interference events X . This probability is modeled using Bayesian logistic regression:

$$\text{logit}(p_j) = \ln\left(\frac{p_j}{1-p_j}\right) = \beta_{j,0} + \sum_{i=1}^k \beta_{j,i} X_i$$

The index j refers to the condition; the index i refers to the interference event.

For simplicity, again, we assume that the conditions are conditionally independent given the predictors. However, this may not be true if, for example, the failure of multiple conditions is influenced by a shared system attribute or an environmental variable. In such cases, multivariate Bayesian logistic regression (multiple dependent variables) or a probit model might be better approaches (O'Brien and Dunson 2004; Martin et al. 2021).

5.3 Standardize the Priors

For the level 2 model, we assume no information about the parameters of the interference events other than they can only increase the probability of prohibitive interference. Accordingly, the prior distributions for the predictor parameters are modeled as negative half-normal distributions with mean 0, an upper bound of 0, and a standard deviation of 5. The prior distribution for the intercept, $\beta_{j,0}$, is the Python Bambi default prior, a scaled Normal distribution (Westfall 2017). The prior distribution for the intercept is not set to equal one because there may be other prohibitive interference events that are not explicitly modeled. In a more complex model, it is possible to imagine better informed priors or more granular condition models, such as fault trees, or models that control for common system features and environmental conditions.

$$\beta_{j,0} \sim N(0, \sigma_0^2)$$

$$\begin{aligned} \beta_{j,i} &\sim \text{Negative HalfNormal}(\mu = 0, \sigma = 5), & \beta_{j,i} &\leq 0, \\ &\text{for } j = 1, \dots, n \text{ and } i = 1, \dots, k \end{aligned}$$

5.4 Level 1: Calculate CWoS

Finally, the probability of the existence of a CWoS is given by the probability of the truth of a Boolean statement of mission-prerequisite conditions, here defined as

$$CWoS = C_{Motor} \wedge C_{Nav_System} \wedge (C_{Camera} \vee C_{LiDAR}) \\ \wedge C_{Algorithm} \wedge C_{Network}$$

This probability is calculated using the conditional probability of the truth of each of the conditions. Here, p_j represents the conditional probability $P(C_j = 1 | X = x)$ as calculated using the Bayesian logistic regression model in Level 2.

$$P(CWoS = 1) \\ = p_{Motor} * p_{Nav_System} * (1 - (1 - p_{Camera})(1 - p_{LiDAR})) \\ * p_{Algorithm} * p_{Network}$$

This model calculates the probability of a CWoS for a specific scenario of the occurrence of events that could cause prohibitive interference in the cyberspace domain. In practice, it is unlikely that a mission owner would know whether those events occurred or will occur. However, given the probabilities of a CWoS for different event scenarios, it would be possible to use available information about the probability of the underlying interference events to generate a predictive marginal probability of a CWoS.

To explore the performance and implications of this model, synthetic data were generated for the occurrence of interference events and their impact on conditions to inform priors. Interference events were modeled as Bernoulli variables and their occurrence was generated with sample draws. Whether a condition did not face prohibitive interference was treated as a Bernoulli variable whose probability was subjectively estimated based on the combination of interference events that occurred. For example, if both *Jamming* and *Kinetic Strike* occurred, the navigation system was judged very likely to fail, so the probability that the *Nav_System* condition would not face prohibitive interference was assigned to be very low.

Separation occurs where predictors perfectly predict an outcome. It can interfere with parameter estimation in statistical models, although these problems may be less severe in Bayesian models with weakly informative priors (Altinisik 2020). To avoid separation, no combination of events was assigned a probability of the satisfaction of a condition of either 0% or 100%. In addition, noise, in the form of a draw from a normal distribution, $N(0, 0.5)$, was added to the probability that the condition would not face prohibitive interference.

The modeler received the data without knowledge of how the data were generated and divided it into training and test data sets. The data was checked for class imbalance, given that prohibitive interference from cyberspace is rare. Each condition was modeled as a Bayesian logistic regression as previously discussed.

Each condition model was fitted to the training data, generating posterior distribution samples for each parameter across four Markov chains using the No-U-Turn Sampler (Hoffman and Gelman 2014). The resulting model was summarized, the trace plotted, and R-hat statistics (denoted as $\hat{R}$) checked to identify improper posteriors or convergence failures of the Markov chains (Vehtari et al. 2021).

Predicted probabilities for each condition were generated using the fitted model and test data, flattening the data from the Markov chains and draws, to compare the predictions to ground truth. Posterior predictive checks of the mean and standard deviation for each condition were conducted and compared to those of the outcomes in the data. The nonparametric posterior predictive distribution was visualized using kernel density estimation with the 95% credible interval indicated (Figure 5). A probabilistic confusion matrix was generated, with mean values of true and false negatives with credible intervals based on samples drawn from posterior distributions, again using the test data for ground truth (Markoulidakis and Markoulidakis 2024). Probabilistic F1, Precision, Recall, and Accuracy scores were generated with their credible intervals. These checks assume no information about the occurrence of the interference events, but more information about interference events could enable more specific estimates.

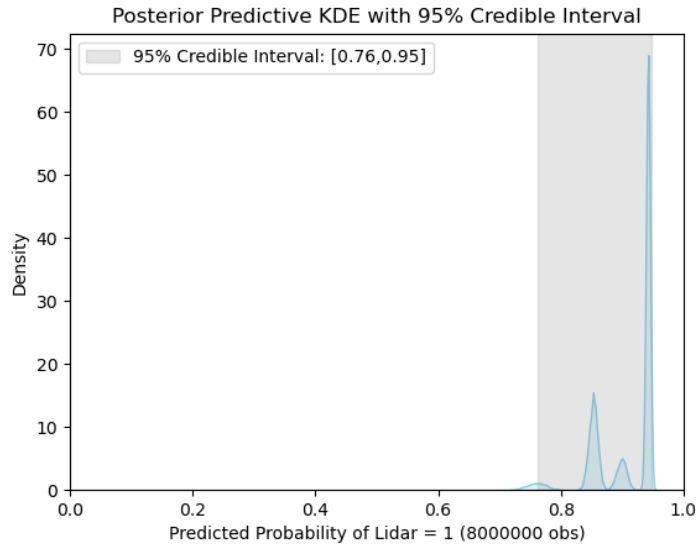


Figure 5. A posterior predictive kernel density estimation of the probability that the mission-prerequisite condition “LiDAR functions” is satisfied.

Finally, the estimated probability of a CWoS was calculated based on the test data, assuming that mission-prerequisite conditions are conditionally independent given interference events. The independence assumption allowed calculation of samples of the joint probability of mission-prerequisite conditions (equivalent to “AND”) by simple multiplication of samples of the posterior predicted probabilities of the conditions. The union (equivalent to “OR”) was calculated as the inverse of the joint probability that all conditions were false. The probability distribution of a CWoS was then estimated using kernel density estimation and the 95% credible interval was indicated.

This model assumed a single time period of interest, with fixed probabilities for interference events and for the conditional probabilities of mission-prerequisite conditions given those events over that period. However, as discussed in the optional final step of problem definition, the relevant CWoS models and data may change as a function of time. In the simpler cases, time itself would be relevant to an estimation of the probability of interference events or the truth of mission-prerequisite conditions (where, for example, systems become more vulnerable over time). In more complicated instances, one could imagine additional time-sensitive predictors, such as adversary behavior, environmental conditions, or some form of autocorrelation.

6. CWoS Metamodeling Considerations

The exploratory modeling exercise highlighted three principal challenges that must be addressed to develop a CWoS model for a specific case. The first is data availability and imbalance. The second is how to estimate and convey the uncertainty about the probability that mission-prerequisite conditions will not face prohibitive interference from the cyberspace domain (imprecise and second-order probability), while being mindful of computational cost and feasibility. The third is how to address possible dependencies among conditions, as dependencies can introduce computational complexity, difficulty in modular modeling, and high uncertainty.

6.1 Data Availability and Imbalance

There may be knowledge about empirical relationships that can inform models. For example, some types of malicious cyberspace action are only possible for certain systems, configurations, or versions. As is done in most MBCRAs, a CWoS model could draw on SME evaluations of the likelihood and likely impact of events or their impacts on systems (Thomas and Raio 2025). However, in most cases, these estimates would be based on or reinforced with data-based inference.

Ideally, there would be ample data about the frequency of occurrence of external events that constitute interference in the cyberspace domain and on their impact on system functionality for every system commonly used in tactical missions. The data would include relevant environmental variables that could affect the probabilities of occurrence, such as geographic location, time, whether it occurred in active conflict, the identity and nature of the adversary, and relevant system-specific variables (such as model or configuration). The data would be based on a shared ontology to enable cross-organizational usage.

That data is not routinely collected. It may be possible to collect relevant data for particular use cases, but some factors make this difficult. The amount of data that must be collected increases with the rarity of the events. Prohibitive interference from cyberspace with tactical missions is very rare in competition, and some forms, such as cyberattacks, may even be rare in conflict. (For more on the competition continuum, see Joint Chiefs of Staff [2022], p. I-4.) In the case of the CWoS toy model, given the comparative rarity of condition failures, the models had high metrics for precision, recall, and accuracy but wide credible intervals for predictions of negative values (condition failures).

Some types of interference are less observable and may not even be detected. Condition failures may not be recorded or ascribed to prohibitive interference from cyberspace, even when this is the cause. Routine forensic analysis is currently prohibitively expensive, although there may be a future where it is more easily automated and less costly. Interference that is not ultimately prohibitive is even less likely to be detected and recorded.

Moreover, the rate of change in cyberspace is substantial. Change includes the development, obsolescence, and evolution of systems, vulnerabilities, and tactics. Data will age out, be made suddenly obsolete, or even be made once again relevant by a technological or tactical development.

As a consequence, the data to support inference will, at best, be imbalanced and incomplete and, at worst, be obsolete. Both imbalanced data and the methods for addressing imbalance affect model performance, making the choices of how to address imbalance context specific (Chen et al. 2024).

6.2 Imprecise and Second-Order Probability

A CWoS estimate is a probability of the existence of a CWoS, which is a function of the probability that mission-prerequisite conditions do not face prohibitive interference from the cyberspace domain, which in turn depends on the probability of the occurrence of interference events. However, there may be uncertainty about

these underlying probabilities, resulting in uncertainty about the CWoS estimate. This uncertainty must be communicated to a mission owner along with the estimate to allow the owner to evaluate the reliability of the model estimate when making high-risk decisions, much like the confidence level assigned to intelligence products.

There are two broad approaches to modeling uncertainty about probability. The first, called “imprecise probability,” seeks to delimit the set of all possible probability values consistent with available information. For example, a SME could say that a key system could possibly be jammed, but it is not likely. If *jamming* is a variable with a Bernoulli distribution, this could be translated as a constraint on the parameter p , $0 \leq p \leq 0.51$, describing a set of possible probability values (Suppes and Zanotti 1989; Fine 1994; Coolen et al. 2025). Where there are multiple variables, *credal sets* capture the space of possible combinations as an n -sided polytope; the points that define the outer hull of this polytope define the limits on possible values. Dempster–Shafer theory assigns probabilities to mutually exclusive sets of outcomes, rather than individual outcomes (Misuri et al. 2018). *Probability boxes*, or “p-boxes,” most commonly show uncertainty as upper and lower bounds for a cumulative distribution function (CDF) but could be used to represent any other partial information about the CDF, such as its support (the range of values that have a positive probability) (Faes et al. 2020). These approaches do not suggest that any of the possible probabilities is more likely than another.

The advantage of these approaches is that they can capture different fidelities of information about the probability, from a simple lower or upper bound to a set of possible cumulative distribution functions, without the need for additional assumptions. Their conclusions are logical consequences of the available information, defensibly consistent with their premises. The results are replicable and reproducible. However, if these sets are combined mathematically, uncertainty compounds. If there are multiple variables with imprecise probability, it may well be the case that there is insufficient information to provide a useful estimate. Because they are multidimensional spaces, it may also be difficult to convey the results of such an analysis in an intuitive way to a human audience.

Where there is very granular information, it may be possible to assign a probability to each possible probability value. This is called “second-order probability.” Hierarchical Bayesian models, which assign probability distributions to model the parameters of a probability distribution, are second-order probability models.

Bayesian models produce probability distribution functions that represent the probability that a variable takes a value rather than point values (Johnson et al. 2022), although these results are often summarized by calculating the mean or by

identifying the 95% credible interval, an interval in which the true value of the parameter is believed to lie with a 95% probability. Most Bayesian models focus on uncertainty about the values of model parameters in parametric models and regressions. However, Bayesian approaches can also be used to model other types of uncertainty, such as uncertainty about model specification (Wasserman 2000; Wang 2023).

Bayesian modeling begins with an assumed probability distribution of the variable (a “prior distribution”) that reflects current belief about the probability of the variable’s possible values. Subsequent observational data is used to update the prior to a “posterior distribution” that gives the probability of values given the observed data, by means of a “likelihood function” that specifies how consistent the observed data is with each possible value of the variable. The posterior distribution is used for prediction, with the goal of providing the best estimate, given information available (Johnson et al. 2022).

Bayesian approaches are attractive for the CWoS problem because they can leverage disparate forms of information for the selection of the prior distribution. For example, in the illustrative CWoS model, the knowledge that interference events have a negative impact on the probability that a condition is free of prohibitive cyberspace interference suggests that the prior distribution of parameters should be truncated so that all values are negative, as was done in the illustrative CWoS model. However, unlike methods that define sets of possible probabilities, Bayesian approaches require that assumptions be made. Bayesian models require a full specification of the prior distribution and the likelihood function, even when there is not enough information to justify those choices. If there is no information, an “uninformative” or “weakly informative” prior is used, such as a uniform distribution that assigns the same probability to all values or a flat, wide normal curve.

In theory, if there is enough observational data, the posterior will converge on the true distribution through iterative updating, making the original choice of prior irrelevant. However, an uninformative prior is still an assumed probability distribution. In practice, and particularly if there is insufficient data, the choice of prior can strongly affect predictions. There is no single rule about how much observational data is required for convergence, different algorithms for computational inference may converge at different rates, and there is no guarantee that convergence will happen at all if, for example, the model is misspecified (Mengersen and Tweedie 1996; Grünwald and Van Ommen 2017). The impact of the prior on the posterior should not be underestimated, particularly if the prior is not scaled appropriately given the data (Van Dongen 2006; Westfall 2017). In

Joyce’s words, “Bayesianism is a garbage-in-garbage-out enterprise” (Joyce 2011, p. 423).

At the same time, particularly for continuous distributions, the prior is often selected for modeling convenience. There are “conjugate families” of probability distributions that allow comparatively simple analytic calculations of posterior distributions if the prior and likelihood functions are in the same family, making them attractive choices (Johnson et al. 2022, p. 97). For nonparametric probability density functions, methods of computational inference are used to estimate the posterior probability distribution function, as was done in this exploratory modeling effort. These methods are computationally costly and, for some, the cost can even be prohibitive beyond a relatively small number of variables (Gray and Moore 2003; Gramacki 2018; Wang 2023; Winter et al. 2024, p. 59–62). The cost of computational inference can, in turn, prompt additional convenience assumptions, such as the use of discrete distributions rather than continuous distributions, with loss of fidelity, or assumptions of independence between continuous variables that are not justified by knowledge or data, as was done in this illustrative model.

In short, each of the approaches to represent uncertainty about probability has advantages and disadvantages. The desire for a defensible, replicable, and reproducible estimate implies the need to minimize assumptions for modeling convenience and therefore suggests the use of Bayesian methods only when either there is sufficient data to justify the prior specification or to allow for convergence on the posterior, as well as sufficient data to validate the model predictions. If there is limited data, it may be preferable to use a probability interval, p-box, or credal set to draw whatever conclusions are defensible. If there is insufficient data to make a defensible estimate, then no estimate should be provided.

In addition to uncertainty about model parameters, there may also be uncertainty about the values of predictor variables (e.g., if there is measurement error) or about model specification (the set of predictors and their relationships). Future work may need to explore the representation, propagation, and communication of combinations of these types of uncertainty for CWoS. There are ways to express and combine uncertainty of multiple types, but they can be computationally difficult, and the results are not always intuitively understandable (Huard and Mailhot 2006; Ajami et al. 2007; Abdi et al. 2024).

6.3 Dependencies among Conditions

A third issue that was raised by the CWoS modeling exercise was the consideration and treatment of the dependency of the mission-prerequisite conditions. Conditions are dependent if information about the state of one condition provides information

about the state of another. Failure to account for existing dependencies between conditions in the probabilistic top-level CWoS model can lead to inaccurate CWoS estimates, essentially through double-counting correlated variables. At the same time, properly accounting for dependencies can significantly raise the computational cost of estimating multivariate densities.

Conditions may be dependent, independent, or the dependency of conditions may be unknown. In a knowledge-driven approach, modelers represent dependencies that they know exist in the world. For example, the probability of the failure of two mission-prerequisite conditions of a system would be dependent if the probabilities were both affected by the same characteristic of that system. In a data-driven approach, dependencies among variables are inferred by analyzing the data to look for patterns.

A given CWoS model, drawing on different combinations of condition models and models of external interference, would have a different pattern of dependencies. As mentioned, assumptions are sometimes made for modeling convenience and the model validated by testing it against ground truth data. But the specificity of the CWoS model to particular missions, systems, and environments would limit the availability of ground truth data for testing and validation. Moreover, even if convenience assumptions were shown not to degrade the model's ability to predict using a given data set, there is no way to know if this is generalizable. The same model with the same assumptions may not perform acceptably on different data.

It would be possible to treat dependencies as unknown and instead calculate the maximum lower and upper bounds of the CWoS estimate (Fréchet inequalities). However, unless there are only a few conditions, this approach could result in such wide bounds that the final CWoS estimate is uninformative.

Dependencies between external events may also be likely, where, for example, an adversary does multiple actions that constitute interference from the cyberspace domain during a conflict. This would affect estimates of weights in the condition models, which would affect the explainability of CWoS results, although it would not affect the predictive power of the condition model (Gelman et al. 2025, p. 365; James et al. 2023, p. 107). More concerning, however, is that the patterns of dependency may not be consistent in the dataset (non-stationarity), which would affect the accuracy of condition predictions.

In short, the generation of a tailored CWoS model requires some way to identify and model dependencies. This would likely require reachback to an application capable of identifying dependencies through a data-driven approach or to a library that contains dependency information about different combinations of events, conditions, and systems.

7. Conclusion

Raio (2023) defined a cyberspace window of superiority. Thomas and Raio (2025) called for a defensible, explainable estimate that identifies or predicts a CWoS. This would enable tactical commanders to make decisions to increase the probability, duration, or scope of a CWoS and take advantage of a CWoS to maximize the probability of successful mission execution.

To estimate the existence of a CWoS, this article proposed extending the MBCRA problem definition and using a hierarchical, probabilistic modeling approach to represent and propagate uncertainty. It then applied that approach using synthetic data and a simple use case to further explore modeling complexities. The modeling exercise raised issues of data availability and data imbalance, the propagation and communication of imprecise and second-order probability, and identification and modeling of dependencies, with implications for computational cost and feasibility. There are multiple methods for addressing these challenges, but all have both advantages and disadvantages. Beyond the high-level modeling approach, the optimal structure of a CWoS model is necessarily context specific and data dependent.

One possible approach to tailored modeling is for the hierarchical CWoS model to accommodate flexible modeling approaches by utilizing abstraction. Submodels could communicate with higher-level models only through defined interfaces so that higher levels could be agnostic about the modeling approaches used below. This would also allow different teams and subject matter experts to contribute to different parts of the model without requiring a refactoring of the whole. The choice of modeling approach for submodels would be dictated by considerations of complexity, data availability, computational power, and knowledge of the problem space.

To have a shared interface, either all uncertainty about probability would be rendered at the lowest common denominator of information—for example, as probability intervals—or convenience assumptions such as uninformative priors would be used to allow communication of probabilities in more granular forms such as PDFs.

However, the use of abstraction is complicated by the fact that submodels may not be independent. There must be a means to identify, propagate, and communicate dependencies so that they can be accounted for at higher levels. A possible area for further research might be consideration of how methods to manage software dependencies might be used to propagate mathematical dependencies.

The CWoS model must also be thoughtfully scoped. As currently defined, “prohibitive interference from the cyberspace domain” is very broadly scoped. As a practical matter, it will likely be necessary to scope the model more tightly given the cost of computational inference for non-parametric PDFs. At the same time, it may not be possible to have very granular CWoS models simply because of the cost of computing with many variables, especially if modeling dependencies. However, this, in turn, would mean that a CWoS estimate might address only part of the overall CWoS problem and picture or that it would be sufficiently general to make it difficult for the mission owner to know how to take action to improve the estimate.

Most importantly, both because of the information required for problem definition, the likely complexity of that definition, and the need to tailor models for specific missions and systems, it seems unlikely that resource-constrained human planning teams would be able to do this at the tactical edge. Instead, problem definitions would more likely be produced by an automated mission planning system and the resulting CWoS estimate would inform such a system. CWoS modeling would require some form of automated modeling with reachback to cloud compute and data. Both automated mission planning and automated modeling are current areas of research.

8. References

- Abdi K, Celse B, McAuley K. Propagating input uncertainties into parameter uncertainties and model prediction uncertainties—a review. *The Canadian Journal of Chemical Engineering*. 2024;102(1):254–273. <https://doi.org/10.1002/cjce.25015>
- Ajami NK, Duan Q, Sorooshian S. An integrated hydrologic Bayesian multimodel combination framework: confronting input, parameter, and model structural uncertainty in hydrologic prediction. *Water Resources Research*. 2007;43(1). <https://doi.org/10.1029/2005WR004745>
- Altinisik Y. A comparative study on the performance of Frequentist and Bayesian estimation methods under separation in logistic regression. *Communications Faculty of Science University of Ankara Series A1 Mathematics and Statistics*. 2020;69(2):1083–1103. <https://doi.org/10.31801/cfsuasmas.614492>
- BAE Systems. BAE Systems’ mission planning autonomy software transitions from DARPA to U.S. Air Force. BAE Systems; 2021 Jan 20. <https://www.baesystems.com>
- Chen W, Yang K, Yu Z, Shi Y, Chen CLP. A survey on imbalanced learning: latest research, applications and future directions. *Artif Intell Rev*. 2024;57(6):137. <https://doi.org/10.1007/s10462-024-10759-6>
- Coolen FPA, Troffaes MC, Augustin T. Imprecise probability. In: Lovric M, editor. *International encyclopedia of statistical science*. 2nd ed. Springer-Verlag; 2025. p. 1158–1162.
- Defense Advanced Research Projects Agency. SBIR: improving battle planning through AI. Defense Advanced Research Projects Agency; n.d. <https://www.darpa.mil/research/programs/improving-battle-planning-through-ai>
- Department of Defense. Manual for the Operation of the Joint Capabilities Integration and Development System; 2021. <https://www.waru.edu/sites/default/files/2024-01/Manual%20-%20JCIDS%20Oct%202021.pdf>, Appendix G to Enclosure B (“Development of Performance Attributes”), p. B-G-2, Section 2.3.1
- Faes M, Daub M, Beer M. Engineering analysis with imprecise probabilities: a state-of-the-art review on P-boxes. *Proceedings of the 7th Asian-Pacific Symposium on Structural Reliability and Its Applications*. University of Tokyo; 2020. <https://lirias.kuleuven.be/retrieve/589507>

- Fine TL. Upper and lower probability. In: Humphreys P, editor. *Patrick Suppes: scientific philosopher*. Springer; 1994. p. 109–133. http://link.springer.com/10.1007/978-94-011-0774-7_5
- Gelman A et al. *Bayesian data analysis*. 3rd ed. 2025 Feb 20. <https://sites.stat.columbia.edu/gelman/book/>
- Gramacki A. *Nonparametric kernel density estimation and its computational aspects*. Springer International Publishing (Studies in Big Data); 2018. <http://link.springer.com/10.1007/978-3-319-71688-6>
- Gray AG, Moore AW. Nonparametric density estimation: toward computational tractability. *Proceedings of the 2003 SIAM International Conference on Data Mining (SDM)*. Society for Industrial and Applied Mathematics (Proceedings); 2003. p. 203–211. <https://epubs.siam.org/doi/abs/10.1137/1.9781611972733.19>
- Grünwald P, Van Ommen T. Inconsistency of Bayesian inference for misspecified linear models, and a proposal for repairing it. *Bayesian Analysis*. 2017;12(4):1069–1103. <https://projecteuclid.org/journals/bayesian-analysis/volume-12/issue-4/Inconsistency-of-Bayesian-Inference-for-Misspecified-Linear-Models-and-a/10.1214/17-BA1085.short>
- Hoffman MD, Gelman A. The No-U-Turn sampler: adaptively setting path lengths in Hamiltonian Monte Carlo. *J Mach Learn Res*. 2014;15(1):1593–1623. <https://www.jmlr.org/papers/volume15/hoffman14a/hoffman14a.pdf>
- Huard D, Mailhot A. A Bayesian perspective on input uncertainty in model calibration: application to hydrological model “abc.” *Water Resources Research*. 2006;42(7). <https://doi.org/10.1029/2005WR004661>
- James G, Witten D, Hastie T, Tibshirani R, Taylor J. *An introduction to statistical learning with applications in python*. 2nd ed. Springer; 2023. <https://www.statlearning.com/>
- Johnson A, Ott MQ, Dogucu M. *Bayes rules! An introduction to applied Bayesian modeling*. CRC Press; 2022.
- Joint Chiefs of Staff. *Joint campaigns and operations [restricted site]*. Joint Chiefs of Staff Report No.: JP 3-0. 2022. https://jdeis.js.mil/new_pubs/jp3_0.pdf
- Joyce JM. The development of subjective Bayesianism. In: Gabbay DM, Hartmann S, Woods J, editors. *Handbook of the history of logic*. Vol. 10. North-Holland. (Inductive Logic); 2011. p. 415–475. <https://www.sciencedirect.com/science/article/pii/B9780444529367500124>

- Kane S, Moody V, Harradon M. Towards incorporating AI into the mission planning process. In: Degen H, Ntoa S, editors. Artificial intelligence in HCI. Springer International Publishing; 2021. p. 216–228.
- Markoulidakis I, Markoulidakis G. Probabilistic confusion matrix: a novel method for machine learning algorithm generalized performance analysis. *Technologies*. 2024;12(7):113. <https://doi.org/10.3390/technologies12070113>. <https://www.mdpi.com/2227-7080/12/7/113>
- Martin GP, Sperrin M, Snell KIE, Buchan I, Riley RD. Clinical prediction models to predict the risk of multiple binary outcomes: a comparison of approaches. *Statistics in Medicine*. 2021;40(2):498–517. <https://doi.org/10.1002/sim.8787>
- Mengersen KL, Tweedie RL. Rates of convergence of the Hastings and Metropolis algorithms. *The Annals of Statistics*. 1996;24(1):101–121. <https://doi.org/10.1214/aos/1033066201>
- Misuri A, Khakzad N, Reniers G, Cozzani V. Tackling uncertainty in security assessment of critical infrastructures: Dempster-Shafer Theory vs. Credal Sets Theory. *Safety Science*. 2018;107:62–76. <https://doi.org/10.1016/j.ssci.2018.04.007>
- O’Brien SM, Dunson DB. Bayesian multivariate logistic regression. *Biometrics*. 2004;60(3):739–746. <https://doi.org/10.1111/j.0006-341X.2004.00224.x>
- Raio S. Toward a conceptual framework for cyberspace windows of advantage. DEVCOM Army Research Laboratory (US); 2023. Report No.: ARL-MR-1080.
- Suppes P, Zanotti M. Conditions on upper and lower probabilities to imply probabilities. *Erkenntnis* (1975-). 1989;31(2/3):323–345. <https://www.jstor.org/stable/20012242>
- Thomas MA, Raio S. Cyberspace windows of superiority: gaps and challenges. DEVCOM Army Research Laboratory (US); 2025. Report No.: ARL-MR-1132.
- U.S. Army Training and Doctrine Command. The U.S. Army in multi-domain operations 2028. Army Training and Doctrine Command (US); 2018. TRADOC Pamphlet 525-3-1.
- Van Dongen S. Prior specification in Bayesian statistics: three cautionary tales. *J Theor Bio*. 2006;242(1):90–100. <https://doi.org/10.1016/j.jtbi.2006.02.002>

- Vehtari A, Gelman A, Simpson D, Carpenter B, Bürkner P-C. Rank-normalization, folding, and localization: an improved $\hat{R}$ for assessing convergence of MCMC (with discussion). *Bayesian Analysis*. 2021;16(2):667–718. <https://projecteuclid.org/journals/bayesian-analysis/volume-16/issue-2/----Custom-HTML----Rank/10.1214/20-BA1221.short>
- Wang J. An intuitive tutorial to Gaussian process regression. *Comput Sci Eng*. 2023;25(4):4–11. <https://ieeexplore.ieee.org/abstract/document/10360364/>
- Wasserman L. Bayesian model selection and model averaging. *J Math Psychol*. 2000;44(1):92–107. <https://doi.org/10.1006/jmps.1999.1278>
- Westfall J. Statistical details of the default priors in the Bambi library. *arXiv*; 2017. *arXiv:1702.01201*. <https://doi.org/10.48550/arXiv.1702.01201>
- Winter S, Campbell T, Lin L, Srivastava S, Dunson DB. Emerging directions in Bayesian computation. *Statistical Science*. 2024;39(1):62–89. <https://doi.org/10.1214/23-STS919>

List of Symbols, Abbreviations, and Acronyms

CDF	Cumulative Distribution Function
CWoS	Cyberspace Windows of Superiority
DARPA	Defense Advanced Research Projects Agency
LiDAR	Light Detection and Ranging
MBCRA	Mission-Based Cyber Risk Assessment
SME	Subject Matter Expert

1 DEFENSE TECHNICAL
(PDF) INFORMATION CTR
DTIC OCA

1 DEVCOM ARL
(PDF) FCDD RLB CB
TECH LIB