Mathematical Modelling of Cyber Warfare: A Quantitative Framework for Pre-Conflict Analysis

LTC Bernd Weissenberger, M.Sc.

NATO Modelling & Simulation Centre of Excellence (MSCOE), Rome, Italy

E-mail: bernd.weissenberger@mscoe.org
bernd.weissenberger@unibw.de

Received: 1. Decembre 2025
Published: 5. Decembre 2025

Abstract

The evolution of warfare in the digital age has transformed cyberspace into a central domain of strategic competition and military operations. Nation-state actors increasingly employ cyber tools to achieve geopolitical objectives without resorting to kinetic force, exploiting vulnerabilities in interconnected critical infrastructures. This paper presents a mathematical framework to quantify and simulate the pre-conflict phase of cyber warfare, integrating offensive and defensive cyber capabilities (OCC and DCC) within the PMESII analytical model. The proposed approach provides a structured, quantitative foundation for assessing the strategic effects of cyber operations and supports decision-making under uncertainty.

Keywords: cyber warfare, mathematical modelling, PMESII, simulation, hybrid warfare, strategic analysis

1. Introduction

1.1 Background

In the 21st century, cyberspace has emerged as a crucial theater of conflict and influence. As military, political, and economic systems become increasingly interconnected, cyber operations offer states non-kinetic means to project power, influence outcomes, and destabilize adversaries. These operations - ranging from espionage and disruption to full-scale strategic attacks - are now integral components of national defense strategies.

1.2 Purpose of the Paper

This paper proposes a mathematical modelling framework to quantify the strategic effectiveness of cyber operations in the pre-conflict phase of hybrid warfare. It seeks to bridge the gap between qualitative cyber strategy research and quantitative simulation by integrating probability theory, differential equations, and systems modelling into a cohesive analytical structure.

1.3 Paper Structure

Following the Introduction, Section 2 (Motivation) outlines the limitations of current approaches to cyber modelling. Section 3 (Framework) presents the conceptual basis linking cyber warfare to PMESII domains. Section 4 (Methodology) details the mathematical formulation. Section 5 (Example) shows a first prototype, and Section 6 (Conclusion) summarizes findings and future directions.

2. Motivation

2.1 Problem Statement

While cyber operations are widely analyzed from political, ethical, and strategic perspectives, few studies offer quantitative tools to model their systemic effects. Traditional wargames and simulations often lack dynamic, time-dependent mechanisms to capture cascading consequences across political, military, economic, social, information, and infrastructure domains.

2.2 Goal

The goal of this study is to create a scalable and data-driven model for simulating cyber conflicts, capable of quantifying both the probability of successful attacks and their cross-domain impacts using PMESII indicators. This enables scenario planners and analysts to assess cyber power as a measurable strategic factor.

3. Cyber Warfare Framework

3.1 Conceptual Foundations

Cyber power, as defined by Nye [1], combines hard and soft power in the digital domain. Libicki [2] emphasizes the signaling and shaping potential of cyber operations, while Rid [3] highlights their ambiguous nature between espionage, sabotage, and warfare. Building on this foundation, the proposed model aligns cyber dynamics with PMESII dimensions to represent systemic impacts across interdependent domains.

3.2 Integration with PMESII

The model extends the PMESII framework by mapping cyber effects across Political, Military, Economic, Social, Information, and Infrastructure systems. For example, an attack on information infrastructure may indirectly degrade economic and social stability, captured mathematically through cross-domain coefficients and feedback loops [4].

4. Methodology

4.1 Model description

The model employs equations to represent time-dependent relationships between offensive (OCC) and defensive (DCC) cyber capabilities. Probabilistic functions estimate success rates of attacks, while resilience metrics adjust dynamically based on cumulative system degradation and recovery (Figure 1: System dependencies).

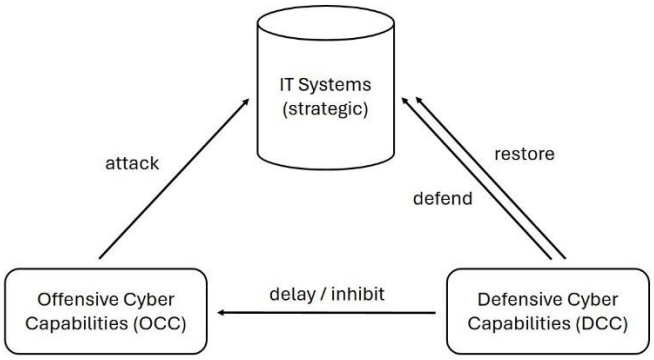

Figure 1: System dependencies

The model comprises three principal components. First, the *IT-system layer* (see Figure 2) does not denote a single service; rather, it represents the aggregate of all IT assets and services within an organisation. Each modelled system is assigned a category - critical, high, medium, or low (C/H/M/L)—as defined in consultation with subject-matter experts from the German Federal Office for Information Security (BSI) [5]. In addition, the level of protection of each system is assumed to improve over time, reflecting rising organisational awareness, enhanced personnel proficiency, and the maturation of software security features. For integration with the strategic simulator, every IT system is mapped to the PMESII schema, enabling cross-domain analysis of cyber effects

$$PMESII_s = \sum_i w_{is}$$

where $\boldsymbol{w_{is}}$ are mapping weights.

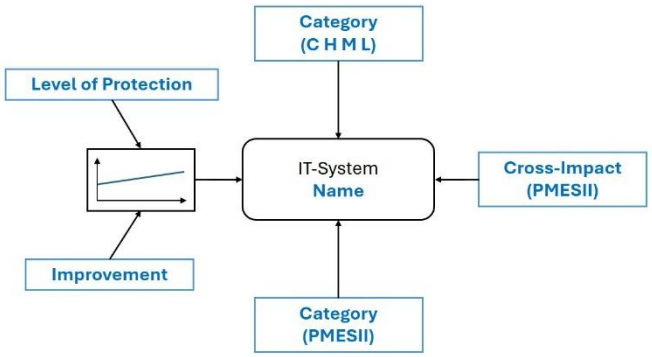

Figure 2: IT-System

Second, the Defensive cyber capabilities (DCC) (Figure 3). During a workshop with representatives from the BSI, the DCCs were described not merely as human resources, but as encompassing the collective skills, structures, and capabilities of the entire cyber defence organisation. According to BSI experts, these capabilities are typically organised in response teams, which can be formed on demand depending on the incident type and severity. Each team possesses specialised,

problem-specific competencies. The exact number of deployable teams remains classified.

In the model and subsequent simulation, two parameters are therefore considered: 1. the skill level of each team and 2. the number of teams available for deployment.

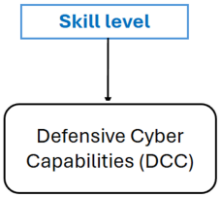

Figure 3: Defensive Cyber Capabilities (DCC)

Third, the Offensive cyber capabilities (OCC) (Figure 4). Similar to the defensive domain, the third and final component of the model represents the Offensive cyber capabilities. Based on discussions with experts at both national and international levels, as well as insights gained from professional conferences such as DEF CON and Black Hat, the concept of OCC is understood to encompass far more than mere personnel strength. It includes the skills, tools, and operational vectors that constitute the offensive cyber domain - notably the utilisation of advanced capabilities such as zero-day exploits and other specialised attack methods. Accordingly, the model incorporates two primary parameters: (1) the skill level of offensive teams and (2) the number of available teams, each with its own distinct expertise and attack vectors (the details of which are classified).

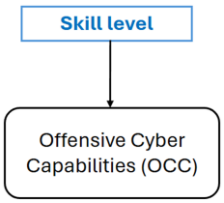

Figure 4: Offensive Cyber Capabilities (OCC)

4.2 Data Sources

Empirical data from exercises such as NATO CCDCOE's Locked Shields provide baseline parameters for cyber attack success rates and defensive efficiency. Simulation outputs are calibrated using open-source datasets and expert assessments to ensure both realism and adaptability to diverse conflict scenarios.

4.3 Mathematical Model Design

As described in the preceding sections, the overall model consists of three core components, each with its own specific parameters. In the following subsections, these components are treated separately and their behaviour during a cyber attack is translated into mathematical form.

4.3.1 Systems

According to the German Federal Office for Information Security, every IT system possesses a basic level of protection at any given time. This protection improves gradually due to continuous updates, patches, investments in security, and the increasing training level of administrators (Figure 5).

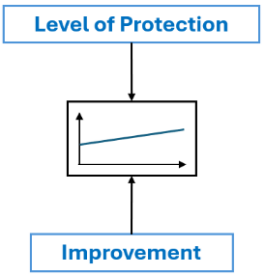

Figure 5: Protection Level of IT-Systems

Over the time horizon of the simulation, we therefore model the protection level of an individual system ias a linearly increasing function:

$$S_i(t) = m_i + c_i$$

where:

- $\boldsymbol{S_i(t)}$ denotes the effective protection level of system iat time t,
- $\boldsymbol{c_i}$ is the initial baseline protection at the start of the simulation,
- $\boldsymbol{m_i}$ is the rate at which protection improves over time (e.g. due to hardening measures and organisational learning).

Systems are categorised as critical, high, medium, or low (C/H/M/L) importance based on expert input, and each system is mapped to at least one PMESII dimension to enable cross domain analysis of cyber effects (a purely linear trend is a simplification and may later be replaced by saturating growth).

4.3.2 Defensive cyber capabilities (DCC)

The mathematical representation of the DCC is deliberately simple. Following BSI subject matter experts, the overall defensive performance of a response team can be approximated by a percentage value between 0% and 100%, reflecting skills, training, processes, and available tools.

For a given defensive team j, we model its effectiveness as a constant:

$$D_j(t) = d_j, 0 \leq d_j \leq 0$$

where d_j captures the aggregated training level and organisational maturity. In a more advanced version, d_j could itself evolve over time as a function of experience and

resource allocation, but for the present study it is assumed to be time invariant.

4.3.3 Offensive cyber capabilities (OCC)

Among the three components, the Offensive cyber capabilities (OCC) are the most complex to model. The corresponding function should represent the temporal progress of an attack from initial reconnaissance to a successful compromise. Combined with the protection level of the target system and the additional protection provided by the DCC, this function yields the overall probability of a successful intrusion.

Both personal experience and expert interviews with penetration testers in governmental and private settings indicate that this process is not linear in time. Instead, the success probability is initially low, then increases as attackers discover viable vectors, and eventually saturates: if no compromise has occurred after a certain time, additional time does not substantially increase the chance of success.

To support this intuition with data, empirical evidence was obtained from the Locked Shields cyber defence exercise organised annually by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Locked Shields [6] is the world's largest and most complex live fire cyber defence exercise, involving multinational teams defending critical infrastructure systems under realistic attack.

For the 2025 iteration, approximately 8,000 systems were deployed and defended by about 4,000 blue force personnel, while a three digit number of red team attackers conducted operations. From the captured network traffic (around 2 TB of data), 9,775 distinct cyber attacks were identified. Using packet timestamps, the duration from attack start to successful compromise was determined. These attacks were grouped into time intervals of roughly 30 time units (Figure 6); for example, in the interval 8.5–37.9 three attacks were successful, while no attack succeeded after time 361.7.

8.492	3
37.9243917	60
67.3567833	489
96.789175	1311
126.221567	1584
155.653958	2085
185.08635	2066
214.518742	1348
243.951133	605
273.383525	181
302.815917	40
332.248308	2
361.6807	0

Figure 6: Table of successful attacks

When plotted, the distribution of successful attacks over time resembles a normal (Gaussian) distribution (Figure 7).

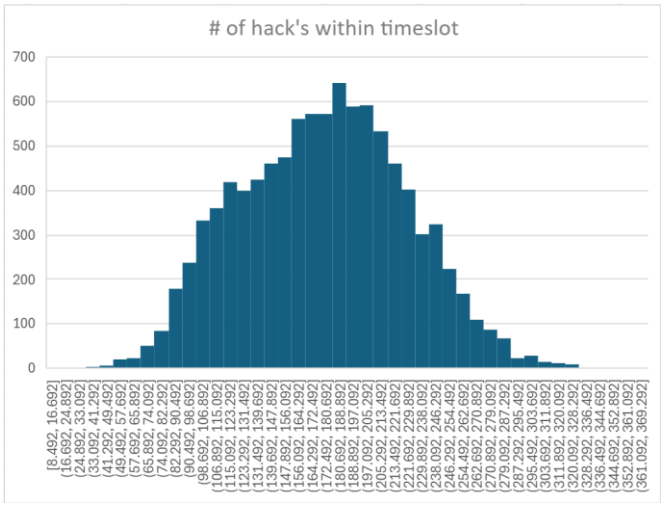

Figure 7: Distribution Over Time

An analysis of the empirical distribution yields a skewness of 0.057 (no significant left/right skew) and a kurtosis of –0.429 (slightly flatter than a perfect Gaussian) (Figure 8).

Metric	Value
Mean	175.1241089
Standard Deviation	49.87257723
Skewness	0.057023164
Kurtosis	-0.428520213

Figure 8: Parameters of the normal distribution

A Q–Q plot confirms the goodness of fit (Figure 9):

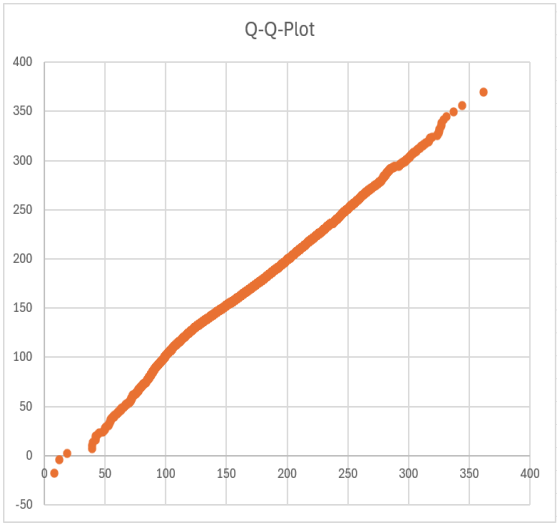

Figure 9: Q-Q-Plot

Based on these findings, the cumulative distribution function (CDF) of a normal distribution is a reasonable model for the time dependent success probability of an offensive operation (Figure 10),

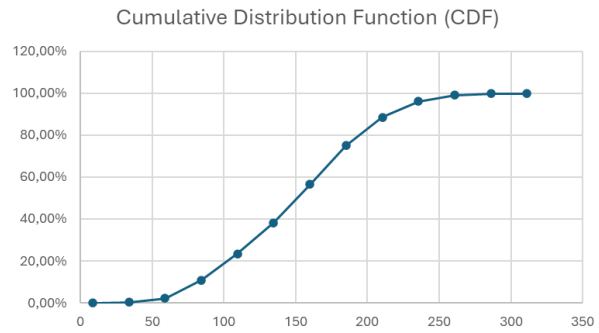

Figure 10: Cumulative Distribution Function (CDF)

$$\Phi(x) = P(X \leq x) = \frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{x} e^{-\frac{(t-\mu)^2}{2\sigma^2}} dt$$

where **μ** and **σ** are fitted to the Locked Shields data.

However, the exact CDF involves an integral over the normal density, which is computationally expensive in large scale Monte Carlo simulations. To reduce runtime, the CDF is approximated by a scaled sigmoid function:

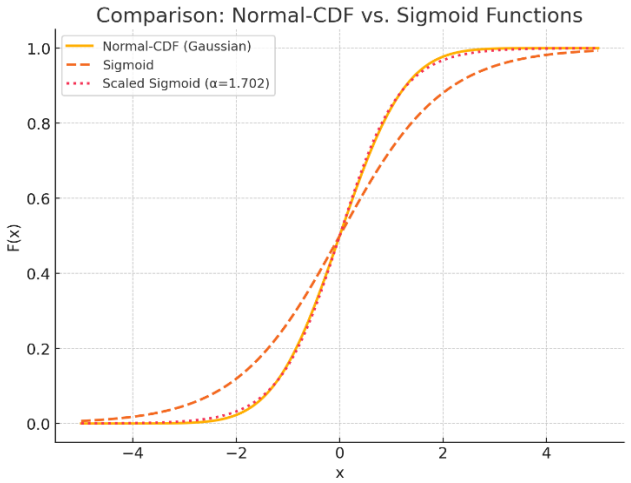

Figure 11: Normal Distribution vs. Sigmoid Function

Figure 11 compares the curves of a complex CDF (orange line) with those of a sigmoid function (red dash line) and a scaled sigmoid function (red dot line). It is evident that the CDF is approximately identical to the scaled sigmoid function (scale factor = 1.702). Therefore, the following function can be used instead of the complex CDF:

$$\Phi(x) \approx \sigma_{1.702}(x) = \frac{1}{1 + e^{-1.702x}}$$

With an appropriate scaling factor (here approximately 1.702), the maximum absolute error is around 1% in the central region, and typically between 0.5% and 1.0% across the relevant domain. Given the high speed up (approximately a factor of three in computation time), this approximation is acceptable for Monte Carlo simulation purposes.

4.3.4 Recovery Process

The final part of the model concerns the recovery of compromised systems. BSI experts describe recovery as a phased process: *"System recovery is carried out in phases (Figure 12). First, the core functions—representing roughly two-thirds of total system capability—are restored. Subsequently, the remaining, less critical functions are gradually brought back online until full system functionality is achieved"*.

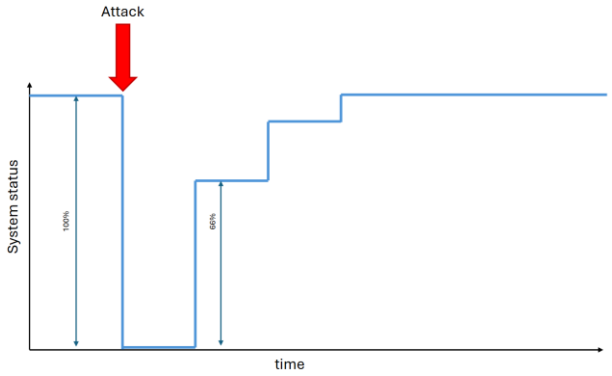

Figure 12: Recovery Process I

This behavior can be approximated by the charging curve of a capacitor in electrical engineering (Figure 13 green line):

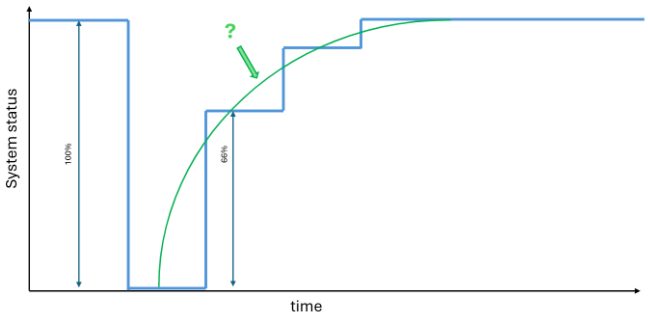

Figure 13: Recovery Process II

$$R(t) = R_{\max}(1 - e^{-t/\tau})$$

where:

- $\boldsymbol{R(t)}$ is the recovery level at time t,
- $\boldsymbol{R_{max}}$ is the fully restored capability (normalized to 1),

- τ is the time constant capturing both DCC effectiveness and system complexity.

After approximately 5τ, the system is considered fully restored for practical purposes. While this continuous function smooths over the stepwise nature of real recovery, it captures the empirically observed pattern of rapid restoration of core functions followed by slower restoration of non-critical services.

5. Example and Prototype

Using the proposed model, it is possible to simulate, on an evidence based footing, the probability of successful cyber attacks against specific systems under defined conditions. A Monte Carlo simulator is particularly well suited for this purpose, as it allows many stochastic realisations of OCC, DCC, and system parameters to be explored. The aggregated results of this pre simulation are then passed to a higher level heuristic or strategic simulator as input parameters.

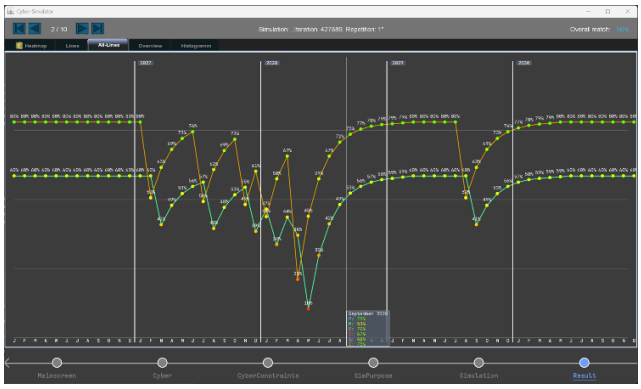

Figure 14: Prototype

Combined with additional elements such as a PMESII cross impact matrix and country specific characteristic, this enables the exploration of potential cross domain consequences of cyber campaigns (Figure 14). For example, the prototype demonstrates how cyber-attacks against infrastructure systems can, with a delay, degrade military capability and how long full restoration of those systems would take.

6. Conclusion

6.1 Summary

This study provides a quantitative foundation for cyber warfare modelling, addressing a key gap in the integration of cyber power within strategic analysis. By formalizing OCC and DCC interactions and aligning them with PMESII dimensions, the model offers a reproducible tool for pre-conflict simulation and policy evaluation.

6.2 Outlook

Future research should focus on enhancing empirical calibration, incorporating AI-driven adaptive models, and integrating human decision-making variables to capture the complex dynamics of cyber deterrence and escalation.

7. References

[1] J. S. Jr. Nye, “Cyber Power.” Harvard Kennedy School, May 2010. Accessed: Nov. 29, 2025. [Online]. Available: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf

[2] M. L. M. C. L. is the Maryellen, R. L. K. D. V. P. in C. S. S. at the U. S. N. Academy, adjunct senior management scientist at the R. C. H. work involves the national security implications of information technology, N. as I. I. Cybersecurity, cyberwar H. lives in Kensington, and M. M. S. F. T. A. V. Biography, “Cyberspace in Peace and War, Second Edition,” U.S. Naval Institute. Accessed: Nov. 29, 2025. [Online]. Available: https://www.usni.org/press/books/cyberspace-peace-and-war-second-edition

[3] T. Rid, *Cyber war will not take place*. Oxford New York: Oxford University Press, 2013.

[4] B. Weissenberger, “Seeding Success: Generating Valid and Realistic PMESII Start Values for Serious Wargames and Simulators,” in *NATO Modelling & Simulation Centre of Excellence*, Rome, Sept. 2024. Accessed: Nov. 29, 2025. [Online]. Available: https://www.mscoe.org/document/seeding-success-generating-valid-and-realistic-pmesii-start-values-for-serious-wargames-and-simulators/

[5] “Bundesamt für Sicherheit in der Informationstechnik,” Bundesamt für Sicherheit in der Informationstechnik. Accessed: Nov. 29, 2025. [Online]. Available: https://www.bsi.bund.de/DE/Home/home_node.html

[6] “Locked Shields.” Accessed: Nov. 29, 2025. [Online]. Available: https://ccdcoe.org/exercises/locked-shields/