Resilience of M&S Capabilities

COL Steve Banks, Mr. Brian Vogt, Prof. Jan Hodicky, Dr. Alberto De Paoli. Mr. Bugra Ayyıldız
NATO Supreme Headquarters Allied Command Transformation
Norfolk, Virginia
Stephen.Banks, Brian.Vogt, Jan.Hodicky, Bugra.Ayyildiz, Alberto.DePaoli, @nato.into

ABSTRACT

The resilience of NATO's Modeling and Simulation (M&S) capability is critical for effective wargaming, operations planning, analysis, and training across complex environments. As NATO faces increasingly sophisticated adversaries and evolving technological landscapes, maintaining M&S capabilities and capacity is essential. This paper explores 9-Step M&S Resiliency Process to evaluate and enhance the resiliency of NATO's M&S capability.

Resilience refers to the ability of a system to prepare for, absorb, recover from, and adapt to strategic shocks that can be initialized inside or outside of the system. More broadly, resiliency ensures continued stability of the system. Basic presumption of this research is that M&S capability can be seen as loosely coupled system of systems with their baseline M&S capacities that are consumed by M&S Users. Therefore, all protective/corrective actions should increase the M&S capacity withing these systems and assured that system of systems stay stable even if exercised by shocks.

The primary research output is a DOTMLPFI informed process to enhance M&S resilience capacities beyond baseline requirements by managing the impacts of potential threats and shocks. The results underscore the need for a comprehensive approach to M&S resilience that not only addresses a need to adapt M&S discipline to emerging technologies but also emphasizes organizational agility, training and experimentation continuity, strong leadership and cross-national collaboration. This research contributes to the broader understanding of M&S resilience, offering practical recommendations for NATO and allied forces to improve the reliability and effectiveness of M&S tools in the face of emerging global threats.

ABOUT THE AUTHORS

Colonel Steve Banks is the branch head for Modelling and Simulation and Learning Technologies at NATO HQ SACT in Norfolk, Virginia. He oversees NATO capability programs, including Next Generation Modelling and Simulation, and Education, Training, Exercise and Evaluation Functional Services. Commissioned in the U.S. Army in 1998, he transitioned from armor branch to simulations operations in 2006, holding diverse leadership roles across tactical, instructional, and operational assignments worldwide. A veteran of deployments to Kuwait, Iraq, and Afghanistan, Colonel Banks holds degrees in Electrical Engineering, Business Administration, Military Operations, and Strategic Studies.

Mr. Brian Vogt is the section head for M&S at NATO HQ SACT in Norfolk, Virginia. He is also the programme director for NATO's Next Generation Modelling & Simulation programme. He is a retired U.S. Army Lieutenant Colonel where he served as an Armor Officer in Korea, Kuwait, and Iraq and served as a Simulations Operations Officer. He holds a masters degree in Modeling, Virtual Environments, and Simulations from the Naval Postgraduate School.

Prof. Jan Hodicky Jan Hodicky has been working as the M&S Technical SME in NATO Allied Command for Transformation in Norfolk. He got his Ph.D. in M&S at the University of Defense and in 2022 he became Full Professor at the same university. From 2013 till 2016 he was Doctrine, Education and Training Branch Head in NATO Modeling and Simulation Centre of Excellence in Rome. Then he was the lead on M&S strategic studies in Czech MoD for 2 years. He has been active member in NATO Science and Technology Organization Modelling and Simulation Group (NMSG) for more than 16 years.

Mr. Hüseyin Buğra Han Ayyıldız is the deputy programme director of NATO's Next Generation Modelling & Simulation programme at NATO HQ SACT in Norfolk, Virginia. Before joining to the programme as the requirements manager, he worked as a principal procurement officer and branch head (Modelling and Simulation) at Türkiye's military procurement agency (SSB). He has an MBA degree from University of Pittsburgh, and he is an alumnus of NATO Defense College.

Dr. Alberto De Paoli is a Modelling and Simulation Analyst at NATO HQ SACT in Norfolk, Virginia. Previously he was a PhD student at Università degli Studi di Genova in Strategic Engineering.

Resilience of M&S Capabilities

COL Steve Banks, Mr. Brian Vogt, Prof. Jan Hodicky, Dr. Alberto De Paoli. Mr. Bugra Ayyıldız
NATO HQ Supreme Allied Command Transformation
Norfolk, Virginia
Stephen.Banks, Brian.Vogt, Jan.Hodicky, Bugra.Ayyildiz, Alberto.DePaoli @nato.into

INTRODUCTION

Modeling and Simulation (M&S) capabilities are integral to NATO's strategic and operational effectiveness. They support a wide range of activities, including training, mission rehearsal, decision support, and capability development. However, the increasing complexity of the operational environment, characterized by rapid technological advancements and sophisticated adversaries, poses significant challenges to the resilience of M&S systems. Ensuring that these systems can withstand, recover from, and adapt to various disruptions is paramount.

More specifically, Russia's war in the Ukraine and other recent international conflicts demonstrate the modern war is both global and fought across all five domains of air, land, sea, space, and cyber. As M&S technologies have matured and militaries have integrated M&S tools into their operations, the reliance on the availability of those tools during conflict has also grown significantly. Therefore, nations, militaries, and industry need to ensure these capabilities are resilient in the sense that they are continuously available during periods of crisis by withstanding both incidental and intentional disruption.

M&S Resiliency

The concept of resilience in M&S encompasses the system's ability to maintain operational effectiveness in the face of internal and external shocks. This includes cyber-attacks, hardware failures, software bugs, and other unforeseen events. Given the interconnected nature of NATO's M&S infrastructure, a disruption in one component can have cascading effects across the entire system. Therefore, a holistic approach to resilience is required, one that considers all facets of the system.

M&S Resilience refers to the ability of a system to prepare for, absorb, recover from, and adapt to strategic shocks that can be initialized inside or outside of the system. More broadly, resiliency ensures continued stability of the system. Basic presumption of this research is that M&S capability can be seen as loosely coupled system of systems with their baseline M&S capacities that are consumed by M&S Users. Therefore, all protective/corrective actions should increase the M&S capacity withing these systems and ensure that system of systems remains stable even if impacted by shocks.

In the context of this paper, resilience is assessed through the lens of the DOTMLPFI construct. DOTMLPFI is a comprehensive framework utilized by the U.S. Department of Defense and NATO to systematically assess and address capability gaps within military operations. The acronym stands for:

Doctrine: The principles and tactics guiding military operations.
Organization: The structural arrangement of military units and command hierarchies.
Training: The preparation and education of personnel to perform their duties effectively.
Materiel: The equipment and technology required to support military functions.
Leadership and Education: The development and instruction of leaders to guide and manage forces.
Personnel: The recruitment, management, and welfare of military members.
Facilities: The physical infrastructure supporting military activities.
Interoperability: The ability of military forces to operate cohesively with allies and partners.

This framework aids in identifying materiel and non-materiel solutions to capability gaps and ensures that all aspects of military capability are considered during planning and development processes. Recognizing that M&S capabilities comprise a loosely coupled system-of-systems (SoS). Each constituent system within this SoS provides baseline simulation capacity that is used by operational users across the Alliance.

Figure 1 below describes the behavior of M&S Capability when reacting to any internal or external shock and individual DOTMLPFI Capacity as it tries to recover from that event. A shock to an M&S system can occur affecting more than one component across DOTMLPFI. As depicted below, the baseline capability is degraded due to a shock, and the recovery from that shock (red line) is important to ensure the M&S service is available to the users.

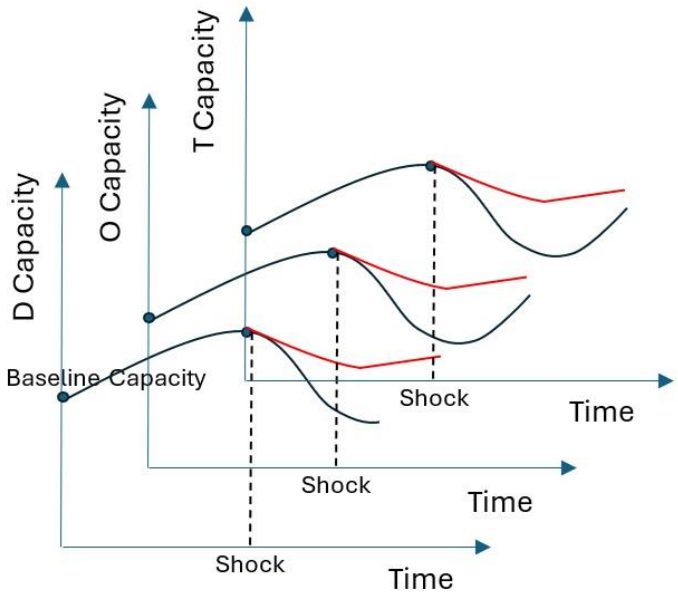

Figure 1. A M&S Capability reaction on a strategic shock within DOTMLPFI framework.

PROBLEM STATEMENT

NATO has integrated M&S capabilities across many application areas such operational analysis, strategic studies, computer-assisted wargaming, operations planning, and computer-assisted exercises to name a few specific areas. This integration has also created a dependency on these systems during crisis and conflict. Therefore, how should NATO, and the member nations, ensure M&S capability resiliency?

APPROACH

The proposed approach to conduct a 9-step process is shown in the figure below.

9 Step M&S Resiliency Process

1. Define the Scope and Objectives
2. Use a Threat Taxonomy
3. Map Threats to DOTMLPFI
4. Conduct a Risk Assessment
5. Evaluate Dependencies and Single Points of Failure
6. Use Red Teaming and Stress Testing
7. Review Historical Failures and Lessons Learned
8. Integrate Threat Analysis into Resilience Planning
9. Continuously Monitor and Reassess

Figure 2. The 9-Step M&S Resiliency Process. This process is a continuous process to ensure critical M&S capabilities remain available during crisis for operations planning, wargaming, analysis, and exercises.

The following explanation and example includes a notional, or fictitious, capability to explore the application of the proposed 9-Step M&S Resiliency Process. A notional capability, NATO Operational Wargaming Environment, is used in leu of a real M&S capability for operational security reasons.

1. DEFINE THE SCOPE AND OBJECTIVES

Define the strategic or operational reason for conducting the threat assessment. Examples include ensuring mission readiness, supporting resilience planning, or ensuring M&S capabilities during conflict or crisis. For example, 'This assessment supports the readiness of the NATO Operational Wargaming Environment for operational planning during a crisis.' Next Describe the M&S system or capability being assessed, including system name, function, users, and major components. For example, 'System: NATO Operational Wargaming Environment (NOWE). Purpose: Strategic-level decision support. Components: Game engine, scenario editor, AI agents, servers, and facilities.'

2. USE A THREAT TAXONOMY

To conduct a thorough and effective threat assessment for Modeling & Simulation (M&S) systems, it is essential to organize potential threats into a structured taxonomy. A well-designed threat taxonomy allows stakeholders to systematically evaluate vulnerabilities across all aspects of the system—technical, operational, organizational, and geopolitical. By categorizing threats, organizations can better identify gaps in resilience planning, prioritize mitigation efforts, and anticipate cascading effects across interconnected systems.

Below is a detailed taxonomy of threat types, each accompanied by representative examples relevant to M&S capabilities in a NATO or defense context:

Break threats into logical categories to ensure a comprehensive assessment:

Threat Type	Examples
Cybersecurity	Cyber threats are among the most urgent risks to M&S systems. These include malware infections, ransomware attacks, phishing schemes targeting simulation personnel, and unauthorized access to networks that host M&S services. Compromised credentials or unpatched vulnerabilities in federation gateways or scenario servers could lead to data breaches, simulation manipulation, or denial of service during critical operations.
Technical obsolescence	Many M&S platforms rely on legacy software and hardware that are no longer supported or updated. These outdated systems can introduce security vulnerabilities, compatibility issues, and performance degradation. Obsolete modeling engines, unsupported HLA implementations, or expired software licenses can undermine simulation fidelity and create maintenance bottlenecks.
Data integrity	The effectiveness of simulations depends heavily on the accuracy, authenticity, and consistency of input and output data. Threats in this domain include corrupted scenario data, falsified or manipulated simulation results, and reliance on unverified third-party data sources. In AI-enabled systems, adversarial inputs or synthetic data poisoning could skew outcomes, degrade trust, and reduce training value.
Personnel	Skilled simulation professionals are a critical asset—and potential vulnerability. Loss of experienced staff, inadequate training, or overreliance on a few subject matter experts can lead to operational disruptions. Insider threats, whether intentional or accidental, can also compromise data, delay exercises, or create access risks. Personnel turnover without proper knowledge transfer further exacerbates institutional fragility.
Interoperability	M&S systems in NATO contexts often require federation between national and partner platforms. Interoperability threats arise from incompatible standards, inconsistent use of protocols (e.g., HLA vs. DIS), lack of compliance with STANAGs, or limited testing between systems. Poor integration may lead to misaligned simulation states, data loss in transmission, or ineffective training outcomes during coalition operations.
Supply chain	M&S capabilities increasingly depend on commercial off-the-shelf (COTS) tools, third-party software components, and hardware procured from global vendors. Disruptions in the supply chain—whether due to logistical delays, component shortages, or hostile foreign control—can affect availability, maintenance, and trust. Hidden vulnerabilities in source code, firmware, or software libraries represent serious threats to system integrity.

Threat Type	Examples
Physical threats	While often overlooked, physical threats remain relevant to M&S system continuity. Natural disasters (e.g., floods, earthquakes) can damage simulation labs or data centers. Kinetic attacks or sabotage may target critical simulation infrastructure during times of conflict. Power outages, facility break-ins, or inadequate environmental controls can also pose significant operational risks.
Political/Policy	M&S programs are influenced by national and alliance-level policies. Sudden changes in funding priorities, export control restrictions on simulation software, or shifts in leadership support can delay modernization efforts or reduce capability scope. Political instability or strategic realignment may deprioritize long-term investments in M&S, undermining resilience.
Institutional	Resilience can be weakened by structural or organizational misalignments. Examples include unclear ownership of M&S systems, lack of a central authority coordinating simulation integration across NATO, or poor communication between developers and users. Failure to institutionalize best practices or incorporate lessons learned into planning cycles creates an environment vulnerable to repeat mistakes and fragmented development.

By applying this threat taxonomy, analysts and stakeholders can conduct a multi-dimensional risk analysis that accounts for both internal weaknesses and external threats. It also facilitates the application of frameworks like DOTMLPFI and risk matrices by ensuring no major threat category is overlooked.

3. MAP THREATS TO DOTMLPFI

The DOTMLPFI framework—Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Interoperability—provides a comprehensive structure for assessing the resilience of Modeling & Simulation (M&S) capabilities. By analyzing each domain, stakeholders can systematically identify vulnerabilities, dependencies, and areas for improvement.

- ***Doctrine:*** Are the roles, responsibilities, and applications of simulation clearly articulated within operational concepts and guidance documents? Do current doctrines address resilience in contested, degraded, or denied environments?
- ***Organization:*** Are M&S functions appropriately distributed across the enterprise, or is there excessive reliance on a specific unit, system, or facility? Are organizational structures in place to support rapid response to disruptions?
- ***Training:*** Are users and operators adequately trained to detect, respond to, and recover from M&S-related disruptions, including cyber incidents, degraded performance, or scenario anomalies? Is resilience incorporated into training curricula?
- ***Materiel:*** Are the hardware and software platforms supporting M&S current, secure, and maintained with sufficient lifecycle support? Have systems been stress-tested and hardened against known vulnerabilities?
- ***Leadership and Education:*** Do leaders understand the strategic importance and operational dependencies of M&S? Are they actively engaged in resilience planning and informed about the risks associated with simulation systems?
- ***Personnel:*** Are roles and responsibilities clearly defined within the M&S workforce? Is there sufficient depth of expertise and succession planning to mitigate the risk of personnel loss or turnover?
- ***Facilities:*** Are the physical environments that host M&S infrastructure (e.g., labs, data centers, simulation hubs) secure, redundant, and resilient to environmental threats (e.g., power outages, HVAC failure, internet disruptions)?
- ***Interoperability:*** Are M&S systems architected to function effectively across joint, interagency, multinational, and multi-domain operations? Do they comply with interoperability standards and enable seamless integration with external C2, ISR, and live/synthetic feeds?

4. CONDUCT A RISK ASSESSMENT

Use a traditional Risk Matrix (Likelihood × Impact) to assess each identified threat.

		Impact				
		Negligible	Minor	Moderate	Significant	Catastrophic
Likelihood	Certain	Low Medium	Medium	Medium High	High	High
	Likely	Low	Low Medium	Medium	Medium High	High
	Possible	Low	Low Medium	Medium	Medium High	Medium High
	Unlikely	Low	Low Medium	Low Medium	Medium	Medium High
	Rare	Low	Low	Low Medium	Medium	Medium

Figure 3. Typical Risk Assessment Matrix where Likelihood and Impact are assessed to understand the overall risk.

First, for each identified threat, the likelihood should be rated (e.g., Rare to Certain). Then each threat should then be rated on the impact (e.g., Negligible to Catastrophic). This will identify the critical vulnerabilities (high-risk/high-impact items).

5. EVALUATE DEPENDENCIES, CRITICAL NODES AND SINGLE POINTS OF FAILURE

Modeling and Simulation (M&S) systems are inherently complex, often functioning as a system of systems comprised of numerous interdependent software tools, hardware platforms, data pipelines, and communication interfaces. These interdependencies can span functional domains (e.g., training, planning, analysis) and operational levels (e.g., tactical through strategic). Understanding how these components interact is essential to uncovering vulnerabilities that may not be visible when components are assessed in isolation.

This step focuses on identifying and mapping the dependencies that exist between various parts of the M&S ecosystem. For example, certain simulation tools may rely heavily on real-time or near-real-time data feeds from live sensors, intelligence systems, or external command and control (C2) platforms. Others may depend on external services such as cloud-based scenario repositories, services protocols, or AI-based agents for scenario generation and adjudication.

As part of this analysis, it is essential to identify critical nodes—components, systems, or services whose disruption would significantly degrade the performance or availability of the overall M&S capability. These may include federation gateways that link multiple simulation environments, scenario generation servers, high-performance computing nodes, centralized data repositories, or even specialized personnel with unique technical knowledge.

A key part of this activity is the identification of single points of failure (SPOFs), which are components or dependencies that, if compromised or disabled, would cause the entire system to fail or become severely limited in function. These can be technical (e.g., a single federated data broker), organizational (e.g., reliance on a specific contractor or expert), or even geographical (e.g., a data center with no redundant site).

This analysis should result in a visual or tabular mapping of system dependencies and critical nodes, highlighting areas that require redundancy, enhanced protection, or contingency planning. The goal is to ensure that M&S capabilities can maintain continuity and resilience—even when exposed to cyber-attacks, technical faults, or operational stressors.

6. USE RED TEAMING AND STRESS TESTING

The use of Red Teams has become an increasingly vital practice in military planning and operations, particularly for evaluating the resilience and security of complex systems such as Modeling and Simulation (M&S) environments. Red teaming provides a structured and adversarial approach to identifying vulnerabilities by simulating realistic threat vectors—ranging from cyber intrusions and technical failures to operational disruptions and kinetic attacks. When applied effectively, this method uncovers hidden dependencies, challenges existing assumptions, and informs mitigation strategies that may otherwise go unconsidered.

In the context of M&S threat assessments, Red Teaming should involve multi-disciplinary participation from all relevant stakeholders, including system developers, simulation operators, cybersecurity personnel, scenario designers, and exercise planners. This ensures that the threat models and adversarial actions reflect a broad range of expertise and operational realities.

Red Teaming activities can take several forms, but tabletop exercises are especially useful in simulating and discussing the impact of disruptions within a controlled yet dynamic setting. These exercises should explore a diverse set of scenarios across a continuum of threat types and intensities. For example:

- **Environmental hazards** such as severe weather events affecting power and connectivity
- **Insider threats** involving credential misuse or intentional sabotage by authorized users
- **Hardware failures** like a crashed simulation server or gateway router failure during federation
- **Adversarial cyber-attacks** including ransomware, denial of service, or data manipulation
- **Physical attacks** targeting central simulation facilities, network operations centers, or deployed command nodes

In parallel to Red Teaming, stress testing should be conducted to evaluate how the M&S systems behave under degraded or high-load conditions. This may include simulating reduced network bandwidth, partial data corruption, system latency, or the loss of federated components. Stress testing enables system owners to understand performance thresholds, determine graceful degradation paths, and plan failover procedures that preserve mission-critical functions.

Together, Red Teaming and stress testing form a powerful combination for assessing the resilience of M&S capabilities. They expose weaknesses, test existing contingency plans, and drive improvements in architecture, process, training, and governance—ensuring that NATO's M&S capabilities are robust, adaptive, and mission-ready under a wide array of threat conditions.

7. REVIEW HISTORICAL FAILURES AND LESSONS LEARNED

A critical component of any robust threat assessment is the systematic review of historical incidents, operational missteps, and systemic shortfalls associated with M&S capabilities. Learning from the past enables organizations to anticipate future vulnerabilities, avoid repeat mistakes, and continuously improve resilience across technical, organizational, and procedural dimensions.

Examine Documented Failures and Underperformance. Begin by cataloging and analyzing instances where M&S systems failed, underperformed, or introduced risk during training events, exercises, or operational support. These incidents may include system outages during mission-critical periods, inaccurate data modeling that led to flawed analysis, software bugs that compromised simulation fidelity, or misaligned user expectations that reduced training value. It's also essential to investigate near-miss events—scenarios where failures were narrowly avoided due to ad hoc workarounds or personnel intervention.

Sources may include:

- Exercise logs and simulation control reports
- Downtime records and IT service reports
- Observations from technical controllers and users

Each event should be analyzed in terms of:

- Root cause(s) (technical, human, procedural, etc.)
- Systemic implications for resilience and readiness
- Contributing factors (e.g., poor integration, outdated hardware, inadequate testing)

Review AARs (After Action Reviews) and Exercise Reports. After Action Reviews (AARs) are a rich source of insight for identifying patterns of risk and operational friction. Focus on AARs from large-scale NATO or national exercises, coalition wargames, and operational-level simulations where M&S was integrated into decision-making or training workflows. In particular, identify:

- Observed shortfalls in M&S system reliability, speed, or realism
- Gaps in operator or user training that contributed to degraded performance
- Failures in interoperability between national or service-specific systems
- Communication or coordination breakdowns related to simulation execution

Identify Recurring Issues and Systemic Weaknesses. Through aggregation and comparative analysis, identify trends and recurring weaknesses that persist across different M&S events or environments. These may include:

- Repeated failures of specific subsystems (e.g., federation gateways, scenario editors)
- Chronic underinvestment in training or technical refresh
- Overreliance on single contractors or SMEs with institutional knowledge

- Inadequate integration of cyber defense measures in simulation networks

Where possible, quantify the operational impact of these failures—such as delayed certification, exercise disruption, or reduced training value—and assess their implications for future missions.

Institutionalize Lessons Learned. To avoid relearning the same lessons, incorporate findings into:

- System requirements documents and acquisition planning
- Configuration control boards and change management processes
- Training curricula for operators, planners, and maintainers
- NATO-wide knowledge sharing mechanisms and repositories

Additionally, ensure that feedback loops are in place so that lessons learned from exercises directly inform system upgrades, scenario design improvements, and stakeholder training initiatives.

8. INTEGRATE THREAT ANALYSIS INTO RESILIENCE PLANNING

Threat analysis should not be treated as a standalone activity or a one-time exercise. Rather, it must be fully integrated into the broader framework of resilience planning to ensure that M&S capabilities can absorb, adapt to, and recover from disruptions—whether technical, organizational, operational, or adversarial in nature.

Update M&S Resilience and Continuity Plans. The insights and findings generated during the threat assessment should directly inform updates to existing M&S resilience strategies and continuity of operations plans (COOP). This includes:

- Revising system architecture documentation to reflect new vulnerabilities
- Enhancing response protocols for identified threat scenarios (e.g., cyberattacks, data corruption, node failure)
- Establishing recovery time objectives (RTO) and recovery point objectives (RPO) for mission-critical simulation services
- Adding redundant systems, alternate sites, or failover procedures to address single points of failure

A living resilience plan—regularly updated through iterative threat assessments—ensures that simulation and wargaming systems remain capable of supporting real-time decision-making, high-fidelity training, and coalition interoperability, even under degraded or contested conditions.

Inform Capability Development Roadmaps. Threat assessments should also shape the future evolution of M&S capabilities by influencing strategic planning, budget decisions, and modernization initiatives. By identifying current weaknesses—such as technical obsolescence, dependency on proprietary tools, or gaps in operator training—organizations can:

- Prioritize investments in modular, scalable, and interoperable M&S tools
- Justify funding for infrastructure hardening or system diversification
- Guide research and development efforts toward solutions that enhance survivability and adaptability

The threat analysis findings should be synthesized into actionable recommendations and included in capability development roadmaps such as the NATO Defence Planning Process (NDPP), national simulation modernization strategies, or Joint M&S innovation initiatives.

Align Mitigation Strategies with Broader Operational and Security Plans. For threat mitigation efforts to be effective, they must be synchronized with overarching operational objectives, cybersecurity strategies, and mission assurance frameworks. This means:

- Ensuring that M&S-related mitigation actions are included in cyber defense exercises and NATO operational readiness plans
- Aligning technical mitigations (e.g., patch management, endpoint monitoring) with enterprise IT security protocols and compliance standards (e.g., STANAGs, NIST RMF)
- Coordinating organizational and personnel resilience actions (e.g., training rotations, skill sustainment, succession planning) with workforce management and readiness programs

Cross-functional coordination is key—resilience is not just a technical problem, but a multi-dimensional effort involving leadership, policy, personnel, and partnerships.

Embed Threat Awareness into the M&S Lifecycle. Finally, resilience must be embedded into the M&S capability lifecycle—from initial design through deployment and sustainment. This involves:

- Conducting threat assessments as part of every major upgrade or system integration effort
- Including resilience considerations in capability requirement documents and acquisition strategies
- Establishing feedback loops so that insights from operational use and exercise performance are used to refine threat models and mitigation strategies

9. CONTINUOUSLY MONITOR AND REASSESS

A resilient Modeling and Simulation (M&S) capability requires more than just a one-time threat assessment—it demands a persistent, adaptive, and forward-looking approach to threat monitoring and risk management. Given the rapid evolution of emerging technologies and the increasing sophistication of adversaries, continuous reassessment is essential to keeping pace with the dynamic threat landscape.

Establish a Threat Intelligence Feed Specific to M&S Domains. To maintain awareness of new and emerging threats, organizations should establish or subscribe to a dedicated threat intelligence capability tailored to M&S systems. Unlike traditional IT systems, M&S platforms often have unique vulnerabilities:

- Integration with legacy systems and simulation engines
- Specialized federation interfaces (e.g., HLA, DIS)
- Use of synthetic or classified data sources
- Dependencies on real-time or mission-critical information feeds

A domain-specific threat intelligence feed should monitor for:

- Vulnerabilities in commonly used M&S software and protocols
- Supply chain risks related to simulation tool vendors
- Exploits targeting AI/ML models used in synthetic scenario generation
- Insider threats within highly specialized simulation teams
- Emerging adversary TTPs (tactics, techniques, and procedures) aimed at degrading decision-support environments

This intelligence should be operationalized through regular briefings, integration with risk dashboards, and collaboration with organizations such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and national cyber intelligence agencies.

Schedule Periodic Reassessments. Threat landscapes are not static—and neither should your threat assessments be. Establish a recurring schedule for periodic reassessments of M&S capabilities and associated risks. Depending on the system's criticality and use, these reassessments may occur:

- Annually for high-value or mission-critical M&S systems
- After any major system upgrade, integration, or federation change
- Following major NATO or national exercises, where new lessons are learned
- After detection of a cyber event or operational failure that may have exposed weaknesses

Each reassessment should revisit previously identified vulnerabilities, validate the effectiveness of mitigation measures, and incorporate any changes in system configuration, operational use, or external threat posture.

Update Threat Models as Technologies and Adversary Capabilities Evolve. As technology evolves, so too must the threat models used to analyze and protect M&S systems. Emerging technologies such as artificial intelligence, quantum computing, cloud-native federations, and augmented reality introduce both capabilities and risks.
Threat models should be routinely updated to reflect:

- New threat vectors, such as data poisoning in AI-based simulations
- Shifting geopolitical dynamics that may increase targeting of NATO or partner training systems
- Changes in adversarial doctrine that involve simulation denial, manipulation, or mimicry
- Technological transitions (e.g., migration from on-premise to hybrid cloud environments)

Modern threat modeling techniques such as MITRE ATT&CK, STPA-Sec (System-Theoretic Process Analysis for Security), and attack tree analysis can be applied and adapted to the M&S domain to produce living models that remain relevant and actionable.

Institutionalize a Culture of Proactive Risk Awareness

Beyond technical tools and checklists, it is essential to foster an organizational culture that embraces proactive risk identification and continuous improvement. This includes embedding threat monitoring into daily operations and planning cycles, encouraging staff to report anomalies or emerging concerns, hosting periodic resilience workshops,

Red Team drills, or scenario-based wargames that test new threats and building cross-functional communities of interest to share intelligence and best practices across nations, services, and simulation communities.

THREAT ASSESSMENT TEMPLATE AND EXAMPLE

Here is a Threat Assessment Template tailored for a specific M&S capability—a NATO Joint Training Environment—but easily adaptable to AI-based simulation systems or wargaming platforms. It integrates a threat taxonomy, DOTMLPFI mapping, and risk matrix structure.

Threat Assessment Template: NATO Wargaming System (Notional)

1. Capability Overview

Field	Description
System Name	NATO Operational Wargaming Environment (NOWE)
Purpose	Support strategic/operational planning, concept development, and decision support
Users	NATO planners, analysts, exercise designers, and multinational partners
Key Components	Game engine, scenario editors, data models, AI agents, user interfaces
Interdependencies	Input from intelligence systems, C2 simulations, modeling frameworks

2. Threat Taxonomy Analysis (Subset)

Threat Category	Specific Threats	Systems Affected	Detection/Mitigation	Comments
Cybersecurity	AI manipulation, model injection, phishing	Game engine, AI agents	Partial	Weak model validation
Data Integrity	Corrupted input data affecting outcomes	Scenario editor	No	Needs secure data pipelines
Technical Obsolescence	Unmaintained open-source libraries	Simulation engine	Unknown	Perform software dependency review

3. DOTMLPFI Threat Mapping (Subset)

Domain	Vulnerabilities / Threats	Resilience Measures
Doctrine	Limited integration of wargaming in operational planning	Update NATO wargaming doctrine
Training	Lack of trained adjudicators or designers	Establish NATO wargaming certification
Interoperability	Inconsistent data formats	Adopt common scenario data exchange standards

4. Risk Matrix (Subset)

Threat	Likelihood	Impact	Risk Level	Mitigation Priority	Owner
Model tampering (AI)	Medium	High	High	Critical	AI Dev Team
Untrusted scenario data	High	Medium	Medium	High	Scenario Design Team
Software obsolescence	High	Low	Medium	Medium	System Admin

5. Recommendations and Action Plan (Subset)

Action	Description	Lead	Timeline	Status
AI integrity audit	Audit AI agents for model poisoning risk	Cyber Defense Centre	[Date]	Planned
Scenario data validation	Implement structured scenario data pipeline	Wargaming Support Cell	[Date]	Proposed

Figure 4. Threat Assessment Template of a national system, NATO Wargaming System

INSIGHTS

The M&S Resiliency Process is similar to the often quoted, "Plans are nothing, but planning is everything" axiom. The exercise going through this deliberate process identifies blind spots, then develops and implements mitigation solutions before there is a problem. It is also true that the outcome of this process will not be better than the diligence and the effort practitioners put into the process. Therefore, it is incumbent on leaders in the M&S community to be the champion for delivering M&S systems that are resilient to their militaries, nations, and the alliance.

Working through the M&S Resiliency Process will identify responsible agencies for execution of the action plan. Many times, the organization responsible for providing services may not understand their role in ensure the systems are resilient. The template proposed above ensures all organizations understand their roles and responsibilities in the larger context of the M&S system and mitigates the risk of two organizations mistakenly believing the other has the responsibility for an action.

For too long the M&S community have developed, fielded, and used M&S systems that are not deliberately designed to be resilient to threats. As militaries increasingly rely on M&S for planning, analysis, wargaming, and exercises, it is critical these systems remain available during crisis and conflict. M&S resiliency must be integrated into the planning, development, procurement, operations, and sustainment of the system.

CONCLUSION

Resilience is a critical attribute of NATO's M&S capabilities, ensuring their effectiveness in dynamic and contested environments. By applying the 9-step M&S Resiliency Process, this study provides a comprehensive assessment of current resilience levels and offers actionable recommendations for enhancement. Implementing these recommendations will position NATO, nations, and militaries to better withstand and adapt to current and future challenges, maintaining the integrity and reliability of its M&S infrastructure.

ACKNOWLEDGEMENTS

This work was motivated by the experience of Ukrainian military in their war with Russia shared through the Partnership for Peace Consortium ADL Working Group.

REFERENCES

Afina, Y., Inverarity, C., & Una, B. (2020, July 17). *Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems.* Retrieved from https://www.chathamhouse.org/sites/default/files/2020-07-17-cyber-resilience-nato-command-control-communication-afina-inverarity-unal_0.pdf

National Institute of Standards and Technology. (2018, December). *Risk Management Framework for Information Systems and Organizations.* Retrieved from NIST Special Publication 800-37: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NATO. (2024). *BI-STRATEGIC COMMAND DIRECTIVE 080-121, NATO MODELLING AND SIMULATION DIRECTIVE.* Brussels.

Presenall, A., Nickolaus, M., & Banks, S. (2025). *Connections: The Quarterly Journal*. Retrieved from https://connections-qj.org/ru/system/files/24.1.05_adl.pdf

Pullen, J., Kraft, J., Mevassvik, O., & Wagner, C. (2021). Modelling and Simulation in NATO Federated Mission Networking. *NATO Modelling and Simulation Symposium.* Amsterdam, Netherlands.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

United States Department of Defense. (2007). *DoD Modeling and Simulation (M&S) Management.* Washington, DC.