# JUMP: Tactical Cyber Mission Planning

**Tim Dudman, Sowdagar Badesha**
Riskaware
Bristol
UNITED KINGDOM
tim.dudman@riskaware.co.uk
sowdagar.badesha@riskaware.co.uk

**Marco Casassa Mont**
BMT Defence & Security UK
Bath
UNITED KINGDOM
marco.casassamont@bmtglobal.com

## *ABSTRACT*

*The Joint User Mission Planning (JUMP) application is a concept demonstration environment to understand the impact of land, air and maritime activities on the cyber domain and vice versa for Joint Force mission planning using state-of-the-art analytics and interactive visualisations. JUMP will provide the underpinning research to the defence community on where analytics and visualisation can be implemented to best effect within a coherent tactical mission planning context. It will also provide prototype tools and techniques to support a military commander to accomplish a wide-range of mission-planning tasks, including mission rehearsal immediately ahead of the mission, re-planning during the live mission, and following the mission as part of de-briefing.*

*JUMP is being developed for the UK Ministry of Defence (MOD) by BMT and Riskaware, pulling together mapping, visualisation, cyber analytics and graph-based technologies. These technologies were originally developed as part of a 2015 UK MOD Centre for Defence Enterprise themed challenge titled "novel approaches to human interaction with cyberspace to increase military situational awareness". JUMP was recently demonstrated at the NATO Information Systems and Technology (IST) workshops on cyber resilience and cyber modelling and simulation. The current focus is to support complex socio-technical systems and Electro-Magnetic (EM).*

## 1.0 OVERVIEW

The JUMP concept demonstration environment utilises a Research and Development (R&D) prototype tool to understand the impact of land, air and maritime activities on the cyber domain and vice versa for joint force missions using state-of-the-art analytics and interactive visualisations. JUMP is providing underpinning research to the defence community on where analytics and visualisation can be implemented to best effect within a coherent tactical mission planning context. At the end of the programme of work it will provide the detail required for a requirements document for tools and techniques to support a military commander to accomplish a wide-range of mission-planning tasks, including mission rehearsal immediately ahead of the mission, re-planning during the live mission, and following the mission as part of de-briefing.

JUMP is being developed for the UK MOD by BMT [1] and Riskaware [2], integrating mapping, visualisation, cyber analytics and graph-based technologies. These technologies were originally developed as part of a 2015 UK MOD Centre for Defence Enterprise themed challenge titled "novel approaches to human interaction with cyberspace to increase military situational awareness", and are aligned with research within NATO into cyber resilience for tactical mission planning [3].

The overall aim of the JUMP programme is to continue the R&D and demonstrate the potential for Joint User mission planning concepts across the land, air, maritime, cyber and EM spectrum. The project provides a proof-of-concept military application allowing collaborative understanding and interaction with the combined operating picture; communicating implications of the cyber battle to non-cyber commanders; and giving the cyber commander awareness of the wider non-cyber mission objectives [4]. Feedback on the effectiveness of JUMP is being elicited through demonstration of the capability at various UK MOD exercises to steer future research.

# 2.0 INTERFACES

JUMP has been designed around two key users; the Cyber Commander and the Cyber Analyst:

> ***Cyber Commander:*** *As staff officer who is responsible to the Joint/Mission Commander for planning and co-ordinating cyber effect. A member of the planning group, works to the Mission Commander's intent, ensures cyber effect is synchronised to support/enhance mission success. Has command responsibility for a number of Cyber Analysts.*
>
> ***Cyber Analyst:*** *A technical expert in the production and execution of cyber effect. Tasked by the Cyber Commander to deliver cyber effect in support of the overall mission. Roles include understanding networks and identifying key vulnerabilities and critical nodes/pathways, identifying possible Courses of Action (CoA) for protection/exploitation of cyber systems, articulating potential cyber risk to the Cyber Commander.*

The Cyber Commander is responsible for contributing to the definition of CoA which defend against, and exploit, cyber vulnerabilities. The Cyber Commander interacts with the Mission Commander to inform them of the opportunities and risks associated with cyber operations. The Cyber Analyst is responsible for building and analysing models of the cyber infrastructure to identify weaknesses and criticalities, and to propose possible solutions [4].

The technologies used provide web-based interfaces to the Cyber Commander and Cyber Analyst, as well as a service-based architecture that will facilitate interoperability with other NATO systems.

## 2.1 Cyber Commander

The Cyber Commander is responsible for providing cyber situational awareness, cyber directions and for contributing to the definition of CoAs within a mission. This role needs to access and analyse a broad range of cyber and physical information in order to make informed decisions and explore suitable trade-offs when defining CoAs.

In this context, JUMP supports a Cyber Commander's activities by providing a rich set of touch-enabled integrated views, including:

- A map view which utilises the NATO Core Geographic Services System [5] to provide geographical insights;
- A cyber view displaying the cyber infrastructure of relevance in respect to physical location;
- A network view displaying device technical information and topological layout; and
- A CoA view for mission risk and CoA trade-off analysis.

Figure 1 shows examples of map views, along with incremental details of geographical areas of relevance to a mission and underlying infrastructures.


*Figure 1 Examples of map views and NATO iconography showing aerial imagery and red/blue force locations*

The Cyber Commander can drill down to details of units using graphical overlays and correlate geographic information with cyber information, for example specific buildings and underlying networking and Information Technology (IT) systems hosted in these locations.

JUMP utilises NATO Joint Military Symbology APP-6 [6] and MIL-STD-2525D [7] to represent relevant entities on the geographic map along with an extension of these symbols to represent cyber elements. Figure 2 provides an example of the cyber view and additional annotations, aiming at mapping a network and devices to their geo-locations.

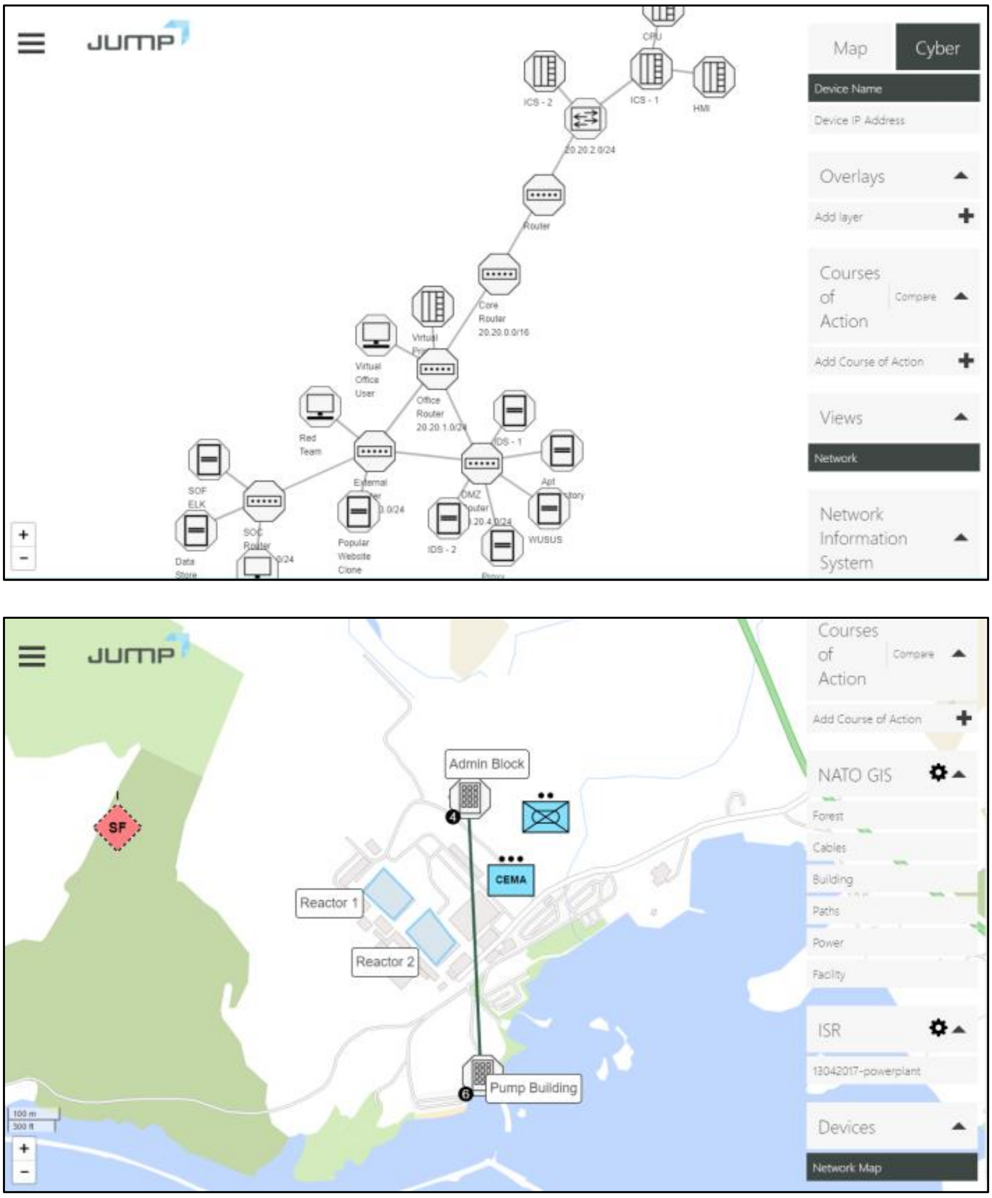


*Figure 2 Examples of cyber view and network map showing network topology and geographic connectivity*

In general, the content of these maps is automatically populated by ingesting, processing and analysing a wide range of data sources, both from the geographic and cyber domains, including outcomes from automatic network scanning and system-of-system architectures.

JUMP aims at enabling a Cyber Commander not only to visualise, analyse and consume this information but also to interactively and dynamically update this data based on intelligence feeds and an evolving situational awareness. For example, Figure 3 illustrates additional capabilities provided to Cyber Commanders to annotate cyber views with overlays which locate cyber components with geographical/physical areas and to update, correct or add technical details.

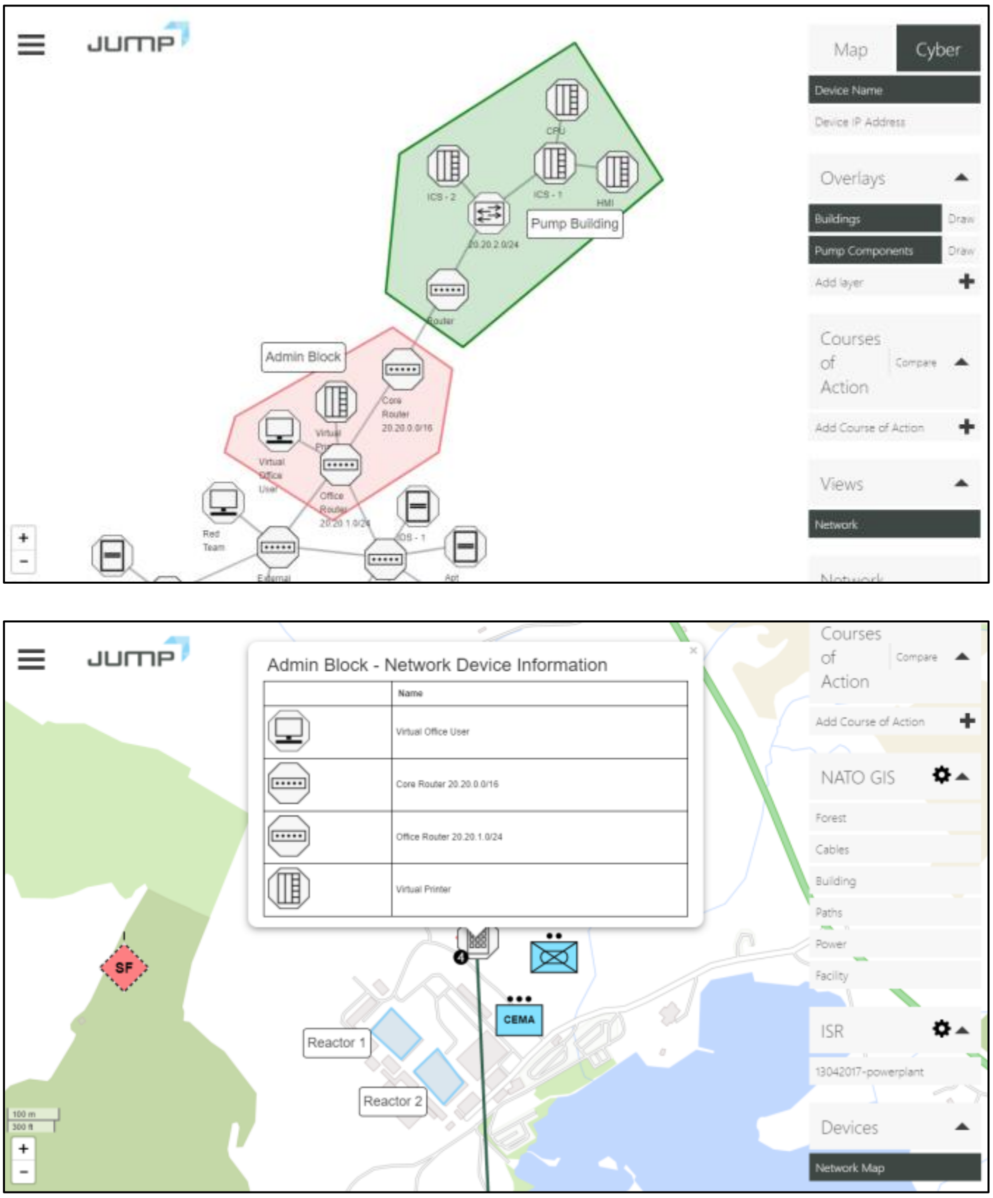


*Figure 3 Examples of cyber views annotation with overlays and network device details*

Finally, JUMP supports a Cyber Commander's objective of creating and analysing CoAs in the context of a mission. In JUMP, a CoA consists of a group of tasks such as military effects including UNDERSTAND, SECURE, MOVE, etc. It can also be assigned to a cyber/military unit to carry out, has a start and end time and is applied to an objective such as a cyber-asset or function. Depending on the Cyber Commander's objectives and analytical goals, JUMP supports the creation and authoring of CoAs in the context of both geographic maps and cyber views. Figure 4 shows examples of the JUMP interface where tasks are added to a CoA and associated effects are visible on a map.

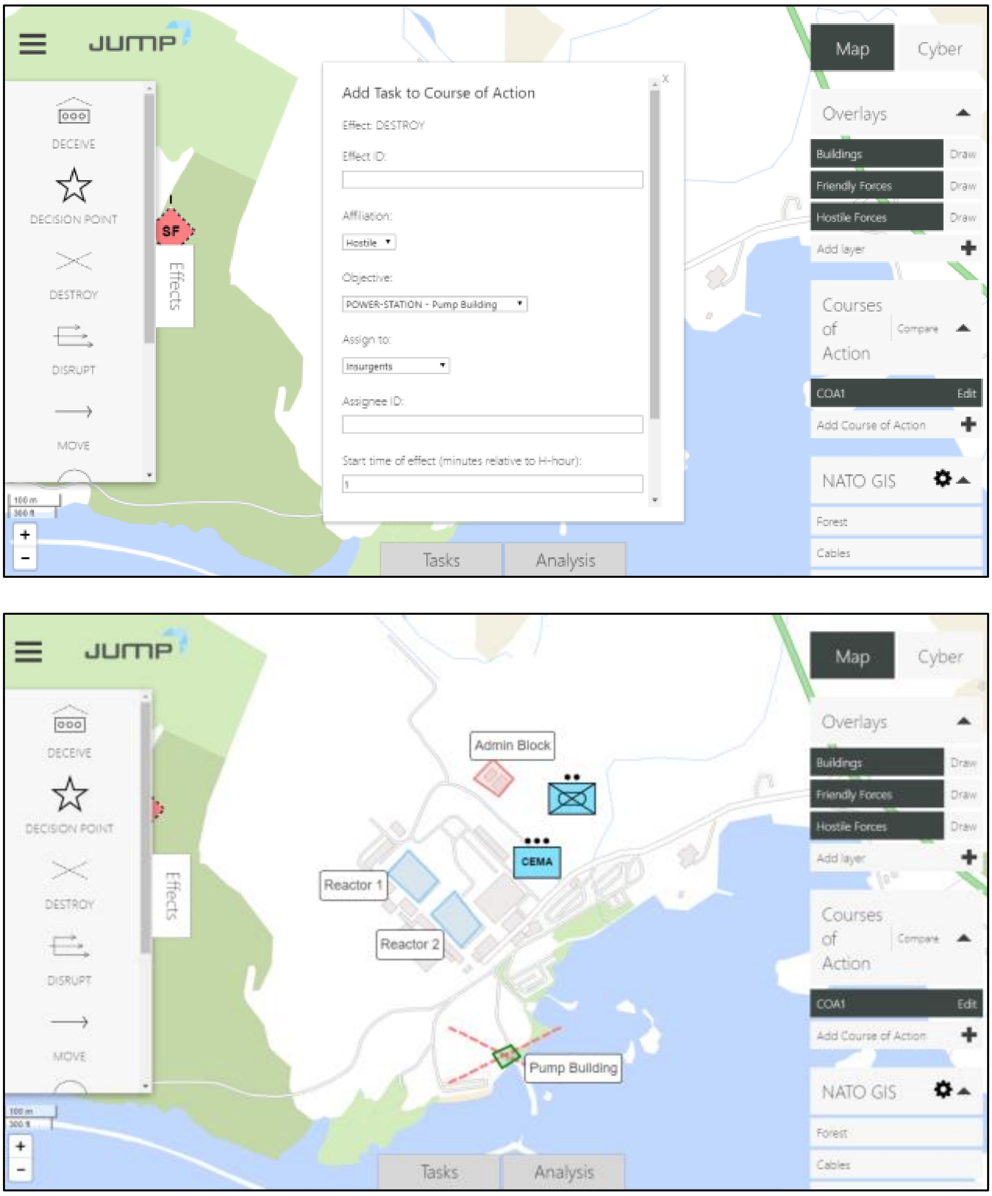


*Figure 4 Examples of adding tasks to a CoA and visualization of cyber effects*

## 2.2 Cyber Analyst

Visual analytics enable the Cyber Analyst to interactively construct and analyse the mission impact of cyber-attacks on the underpinning cyber infrastructure. The Cyber Analyst can model complex mission objectives, supporting processes and component hierarchies while visually interrogating the results of simulated threats, both at the network and mission level. Figure 5 shows two screens on the Cyber Analysis interface, whereby the analyst can compare results to better understand the relationship between both domains. For example, what is the mission impact of a cyber-attack on my Reachback support's information system and how should I prioritise security measures? This enables a Cyber Analyst to convey the tactical implications of cyber-attacks to the Cyber Commander and propose risk and damage assessment, and mitigation strategies such as software patching or physical controls. The Cyber Analyst can also challenge current system assumptions through further analysis.

*Figure 5 Cyber analyst interface showing MIA and cyber-attack path visual analytics*

## 3.0 ANALYTICS

JUMP reduces the workload of Cyber Commanders and Cyber Analysts through interactive CoA evaluation, Mission Impact Assessment (MIA) and cyber-attack analytics. In addition, these capabilities support tactical mission planning by providing insight into complex scenarios that bridge the cyber and physical domains.

### 3.1 Evaluating Courses of Action

JUMP aims at enabling a Cyber Commander to analyse and evaluate a CoA for a given mission, by computing and providing multiple metrics, including performance, cost and time, risk and impact of mitigations, and the likelihood of tasks succeeding.

An extensible library of analytics computes these metrics within JUMP, which factor in physical, geographic and cyber information from ingested mission and network models, and from interactive mission planning using the JUMP user interface. For example, the analytics identify critical assets for a given cyber network or mission; compute the performance of a CoA by performing MIA, identifying the cost and time for given tasks; and by means of cyber risk analysis based on risk level, deployed mitigations, controls and countermeasures.

Figure 6 shows examples of how CoA evaluation is conveyed to a Cyber Commander, with regard to the likelihood of success of CoA's tasks and overall performance.


*Figure 6 Examples of JUMP CoA task analysis and performance evaluation*

In general, JUMP's objective is to support Cyber Commander's what-if analysis for CoAs, by visually comparing and contrasting the impact of different (cyber) decisions, both at the task level and across multiple CoAs.

## 3.2 Mission Impact Assessment

A unified connected-graph model-driven approach allows JUMP to represent the cyber terrain and mission in a single, coherent data model, bridging the gap between operational decision makers and cyber analysts. The mission is modelled as a topological vignette of interdependent mission components. These can represent mission threads, actors, processes and other mission-critical assets. Each has an assigned sensitivity to the combination of performance degradation of any dependencies. Mission components can be associated with network devices, and have time-based events, vulnerabilities and impacts associated with them to allow the mission impact of both conventional and cyber events to be modelled. Complex rules such as device redundancy and impact time profiles can also be modelled.

Mission vignettes are built automatically within JUMP based on Cyber Vulnerability Investigation (CVI) information and Cyber Commander interaction with the map, or by importing Unified Modelling Language

(UML) Cyber Mission Impact Assessment (CMIA) [8] models, that are then interactively augmented by a Cyber Analyst [9]. Key operations are the construction of mission risks (events, vulnerabilities and impacts) and the association of mission-critical network devices known as Operational Technology (OT).

MIA involves topologically sorting the mission vignette, followed by assessing the time-based impact of all events, considering the results of any cyber-attack analysis. The output of the MIA calculation is a detailed performance time series at each level of the mission. Following MIA, mission performance information is available to both the Cyber Commander and Cyber Analyst. It is then possible to perform red teaming [10] analyses, including what-if analysis to look at the impact of each event in isolation, high-impact analysis that filters the what-if results to show the highest impact and highest probability events only, and alternative futures analysis that generates mission outcome realisations based on sampling from multivariate distributions for the highest impact and highest probability events.

### 3.2 Cyber-Attack Analysis

A computer network in JUMP can be analysed to display viable cyber-attack paths that could be used by a cyber threat during an attack. Device inter-relationships are modelled, and software vulnerabilities analysed to see how a cyber threat could traverse a network to a given mission-critical device. A cyber threat actor can be graded in capability and positioned topologically given operational intelligence to best simulate the logical attack origin. In addition, attacks from multiple threat actors can be simulated simultaneously with varying levels of capability, and human-facilitated attack vectors can be modelled. Additional R&D work will complement this assessment with cyber risk analysis (based on estimated likelihood of threats and their impacts) along with an assessment of costs and time of deploying different countermeasures and controls.

Network topologies in JUMP can be built by importing raw Nmap [11] scans that are then augmented interactively by a Cyber Analyst. Known software vulnerabilities can be automatically mapped to detected software during ingest. These software vulnerabilities form the basis of the cyber-attack analysis and are an abstraction of the vulnerabilities present in the National Vulnerability Database (NVD) [12]. The Common Vulnerability Scoring System (CVSS) [13] outlines the specification for these vulnerabilities and is a system for categorising key exploitation features, including Confidentiality (C), Integrity (I) and Availability (A) impacts.

In JUMP, all possible attack paths through the logical network are calculated using a simplified but highly-optimised Topological Vulnerability Analysis (TVA) [14] approach. Each software vulnerability is processed to determine the pre-conditions required to exploit it, and the level of impact realised if successful. Socio-technical analysis is supported with the introduction of CVSS Version 3 properties [15], which include physical attack vectors (e.g. USB or jailbreak attack) and user interaction (e.g. a user clicking on a malicious executable).

The attacker's physical location as depicted in the Cyber Commander's interface is used to deduce the ability for a physical pre-condition to be satisfied during exploitation. Non-malicious threat actors can also be assigned to devices to model instances of a potential operator being able to inadvertently satisfy a required user interaction pre-condition.

The resultant technical impact of an attack on OT is determined during MIA to give it tactical context in the mission model.

## 4.0 SUMMARY AND CONCLUSIONS

This paper has provided a high-level overview of just some aspects of the JUMP application R&D - how it is providing underpinning research to the defence community and where analytics and visualisation can be implemented to best effect within a coherent tactical mission planning context. To date JUMP has been used for interactive CoA evaluation, MIA and cyber-attack analytics that provide insight into scenarios that bridge the cyber and physical domains. Feedback from stakeholders and users at demonstrations has indicated that it has utility at both the tactical and strategic level, especially if limitations concerned with advanced cyber-attack modelling, uncertainty and EM capabilities are addressed.

Current research efforts for 2018/2019 are focused on addressing these limitations by enhancing the modelling of socio-technical cyber risks and controls (including threat actor goals and techniques), modelling temporal device connectivity and network uncertainty, modelling EM effects (including the defence of mesh networks) and optimising task cost and time calculations for CoA evaluation.

*The contents of this paper/presentation should not be interpreted as representing the views of the UK MOD, nor should it be assumed that they reflect any current or future UK MOD policy. The UK MOD contact for the JUMP programme is Steve Barrington, Dstl, Salisbury, UNITED KINGDOM, sjbarrington@dstl.gov.uk.*

# References

[1] "BMT," [Online]. Available: https://www.bmt.org/.

[2] "Riskaware," [Online]. Available: http://www.riskaware.co.uk/.

[3] S. Noel, T. Dudman, P. Trepagnier and S. Badesha, "Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153," US Army Research Laboratory, Adelphi, MD, USA, 2018.

[4] A. Waldock, T. Dudman, S. J. Harold and M. Cobley, "JUMP Phase 1 Final Report," BMT Defence Services, Bath, UK, 2018.

[5] ESRI, "The NATO Core Geographic," ESRI, Redlands, CA, USA, 2014.

[6] NATO, "NATO JOINT MILITARY SYMBOLOGY APP-6(C)," NATO, 2011.

[7] Department of Defence, "JOINT MILITARY SYMBOLOGY," Defense Information Systems Agency, Ft. Meade, USA, 2014.

[8] C. Lang and B. Madahar, "Understanding the Mission Impact of a Cyber Attack in a System of Systems Environment," in *NATO IST-156: Cyber Modelling and Simulation Workshop*, Portsmouth, UK, 2017.

[9] T. Dudman and A. Waldock, "JUMP: Modelling and Simulation of Cyber Resilience for Mission Impact Assessment," in *NATO IST-153: Cyber Resulience Workshop*, Munich, GERMANY, 2017.

[10] Ministry of Defence, "Red Teaming Guide Second Edition," Ministry of Defence, London, UK, 2013.

[11] G. Lyon, "Nmap," [Online]. Available: https://nmap.org/.

[12] NIST, "National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/.

[13] FIRST, "Common Vulnerability Scoring System v3.0: Specification Document," FIRST, Morrisville, NC, USA, 2017.

[14] S. Noel and S. Jajodia, "Topological Vulnerability Analysis," *Advances in Information Security*, vol. 46, pp. 139-154, 2009.

[15] FIRST, "Common Vulnerability Scoring System v3.0: User Guide," FIRST, Morrisville, NC, USA, 2017.