Ref: JUMP-IST-153-2
Date: 14/9/2017

JUMP: Modelling and Simulation of Cyber Resilience for Mission Impact Assessment

Principal author:

Tim Dudman: Senior Principal Consultant, Riskaware, Colston Tower, Colston Street, Bristol BS1 4XE, UK, +44 (0)117 929 1058, tim.dudman@riskaware.co.uk, www.riskaware.co.uk

Co-author:

Antony Waldock: Principal Systems Analyst, BMT Defence Services, Maritime House, 210 Lower Bristol Road, Bath, BA2 3DQ, UK, +44 (0)1225 473600, awaldock@bmtdsl.co.uk, http://www.bmtdsl.co.uk/

MOD contact:

Steve Barrington: Principal Scientist, Cyber & Information Systems Division, Dstl, Porton Down, Salisbury, Wiltshire, SP4 0JQ, UK, +44 (0)1980 956877, sjbarrington@dstl.gov.uk, https://www.gov.uk/government/organisations/defence-science-and-technology-laboratory/

Overview

The Joint User cyber Mission Planning (JUMP) application is a concept demonstration environment to understand the impact of land, air and sea activities on cyberspace and vice versa for various defensive and offensive joint force missions using state-of-the-art analysis algorithms and interactive visualisations. The scope of this work is to develop a concept demonstrator framework for visual analytics, Virtual Reality (VR) and Augmented Reality (AR) tools that can be employed for Cyber Mission Planning (CMP) with a view towards exploitation over the medium term (~5 years). JUMP will provide the defence community with much-needed confirmation that foundational theory can be implemented and applied within a coherent mission planning context. It will also provide prototype tools and techniques to de-risk the development of a capability that should ultimately support a military commander to accomplish a wide-range of mission-planning tasks including:

- Understand the impact of cyberspace activity on various mission Courses of Action (CoA) and the subsequent decision-making.
- Construct mission plans containing CoA.
- Evaluate the impact of CoA against the potential activities of adversaries, allies and neutrals.
- The use of cyber Search, Visualisation and Analysis (SV&A) technologies.
- Identify the critical points of our own, or adversary's, military cyber-dependent systems and understand their status.
- Integrate understanding of the Cyber and Electro-Magnetic Activity (CEMA) environment into cyber-operational planning, exploiting synergies with MOD projects (e.g. Landseeker, Airseeker and Seaseeker).
- Fuse Land, Air, Sea, Electro-Magnetic (EM) and cyber environments for a joint picture.

In addition to mission planning, JUMP could also be applied to support mission rehearsal immediately ahead of the mission to confirm that plans are feasible, re-planning during the live mission, and following the mission as part of de-briefing.

JUMP is being developed for the UK MOD by a consortium of BMT Defence Services, Riskaware and Cyberlytic; running from December 2016 to reach Technology Readiness Level (TRL) 6 by March 2019. It will help to communicate implications of the cyber battle to non-cyber commanders and give cyber staff awareness of the wider factors affecting the mission. End users interact with 2D and 3D maps of both

physical and cyber entities that provide a range of views supporting planning activities across the physical and CEMA spectrum. The analysis and insight developed from these views allows users to extract implications on the mission.

An agile development approach is being employed while engaging with MOD users and stakeholders to run experiments and integrate research outputs. Exploitation is via demonstrations, workshops with users and engagement with relevant personnel during military exercises, including Joint Venture 2017 and potentially Cyber Warrior 2018.

Defence of Critical National Infrastructure

JUMP aims to support military effects-based planning within a CEMA environment. It extends the existing symbology, language and visualisation of traditional land-based planning tools to include CEMA and form a single view such that the risks and benefits of actions in two domains can be considered side-by-side.

An example scenario would be the defence of Critical National Infrastructure (CNI) in a foreign friendly nation that is experiencing insurgence supported by a larger nation state. The nation state is known to have a cyber-capability, and intelligence has been gathered to indicate that CNI is a target. Preparation for such a mission would require an understanding of the geographic environment in and around the CNI, but also awareness of the cyber infrastructure to defend in relation to the enemy's capabilities.

JUMP extends the joint user mission planning environment to allow cyber units to be modelled in existing NATO standards and for cyber devices relevant to the mission to be associated. JUMP draws on data from Geographic Information Systems (GIS), Cyber Vulnerability Investigations (CVI) and Network Information Systems (NIS) to analyse the risk associated with the cyber infrastructure under protection. For example, a CVI may indicate that a particular building contains a device that is exposed (both physically and from a network security perspective) and plays a critical role in the operation of the CNI. JUMP allows the cyber analyst to understand the risk associated with operating the device in the wider context of the mission. For example, if the device vulnerable to attack from a remote location or an employee with elevated privileges. The options available to the commander to secure the device in the building and maintain operation of the CNI are available within JUMP, both in terms of infrastructure updates (patching and firewalling) or by physically securing the location to reduce the risk associated with the mission.

Cyber Resilience and Mission Impact Assessment

In order to represent the impact of cyber warfare for campaign and mission-level operations, JUMP leverages Riskaware's previous Centre for Defence Enterprise (CDE) research. In 2014, Riskaware developed the Rapid Evaluation of Disablement Action (REDACT) system to model the resilience of industrial processes to kinetic effects. This work pioneered the integration of connected-graph process modelling, 3D plant and blast modelling and visual analytics. The result was that the performance degradation of parts of the plant due to the impact of kinetic-attack could be modelled and visualised, along with the downstream impact on plant output.

In 2015 Riskaware built on this research, and the REDACT platform, to model the cyber resilience of military missions in the Cyber Operational Mission Mapping, Visualisation and Analysis Tool (COMMVAT). Missions were modelled as a dependency-based connected-graph, and the 3D plant and blast model was replaced with a cyber-attack model. The cyber model included a topological representation of a network, stored in a scalable connected-graph database, and algorithms to perform Topological Vulnerability Analysis (TVA) [1] and weakest attack path analysis. As with the previous industrial process resilience modelling, performance degradation of parts of the mission due to the impact of cyber-attack could be modelled and visualised, along with the resulting impact on mission objectives. In addition, the effect of patching mission-critical device vulnerabilities could also be assessed.

This existing cyber Mission Impact Assessment (MIA) capability is now being re-developed for integration into the service-based JUMP architecture and for use within the JUMP-hosted NATO mission planning process [2]. Additionally, the scalability of the algorithms and underlying technologies is being enhanced to support multiple missions and hybrid network topologies.

Unified Connected-Graph Data Model

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. Completely built on open-source, scalable connected-graph database technology, JUMP can model cyber-dependent missions with varying levels of fidelity in order to represent the impact of cyber phenomena on operations.

Computer networks are modelled as a topology of devices and physical connections in logical groups as shown in Figure 1. Device software is also modelled, along with known vulnerabilities and cyber threats. The intention is that this data will be generated through detailed Cyber Vulnerability Investigations (CVI) and network scans. In the interim, the latest Common Vulnerabilities and Exposures (CVE) are looked-up online from the US National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) [3] using web services such as the Computer Incident and Response Centre Luxembourg (CIRCL) [4].

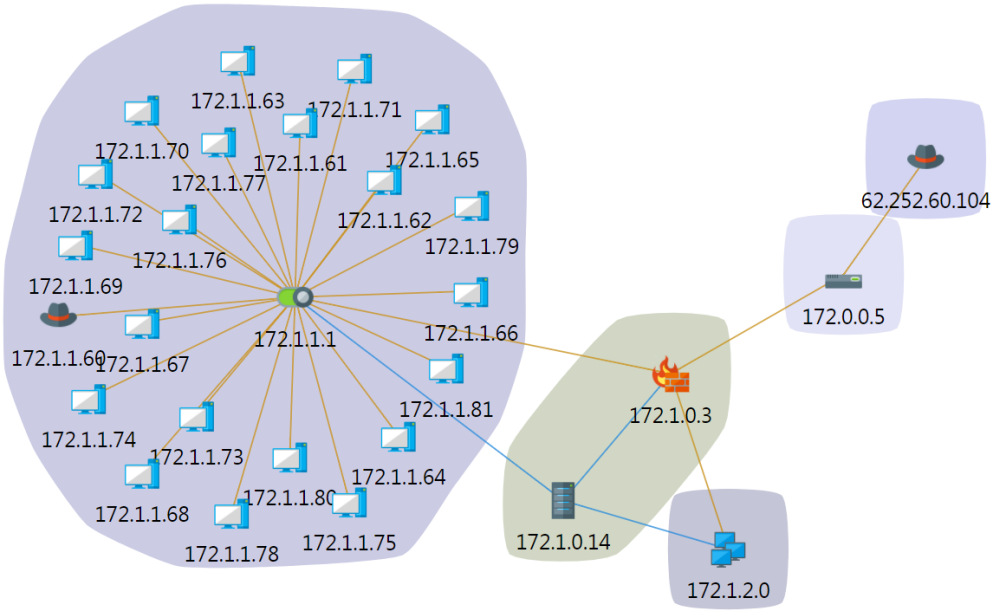

Figure 1: Connected-graph showing network topology

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 recovery time can also be modelled.

Mission vignettes are built behind the scenes within JUMP based on CVI information and user interaction with the map, or by importing Unified Modelling Language (UML) Cyber Mission Impact Assessment (CMIA) models that are then interactively augmented by a cyber analyst.

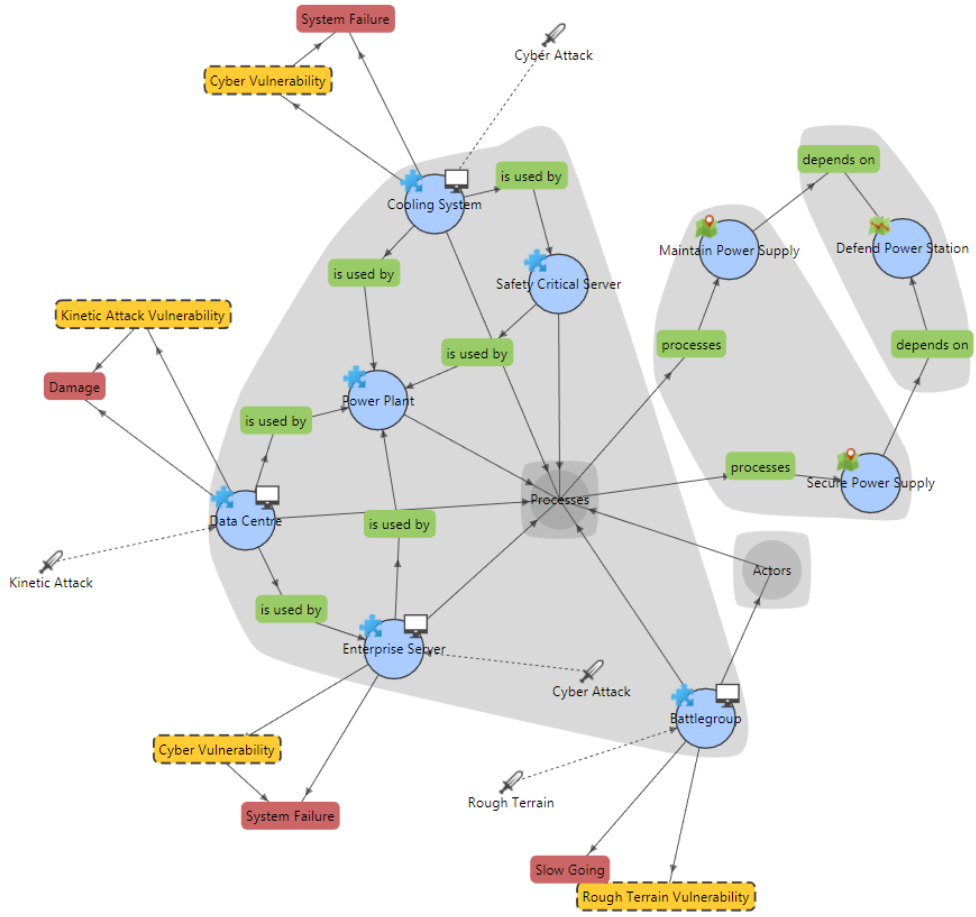

Figure 2: Connected-graph showing a mission vignette

The example mission vignette shown in Figure 2 models the protection of CNI. A blue forces battlegroup defends a power plant to secure the power supply. The battlegroup is reliant on a military network for communications, and the power station is dependent on both a safety-critical Supervisory Control and Data Acquisition (SCADA) network, as well as an enterprise network. Each network is modelled separately (the SCADA and enterprise networks are air-gapped), and critical devices are associated with mission components. The mission vignette models these assets along with military units, plant processes (such as cooling and control) and mission objectives. Mission vulnerabilities and events are also modelled to represent rough terrain, kinetic effects and cyber-attack. The cyber-attack surface is modelled by both mission-level vulnerabilities and cyber threats in the network topology. These simulate both external hackers and insider threats with different authentication capabilities.

Topological Cyber Vulnerability Analysis and Mission Impact Assessment

Graph-based analysis techniques can simulate both offensive and defensive entities within the mission and cyber domains. The modelling considers the impact of cyber threats and the consequences of mitigations such as firewalling and patching. The progression of chained cyber-attacks is modelled through a simplified and highly-optimised TVA approach; a process whereby all possible attack paths through the logical network are calculated. The algorithm involves the following steps:

1. Exploits are created from applicable vulnerabilities based on pre- and post-condition Common Vulnerability Scoring System (CVSS) [3] metrics:
    a. Access vector

   b. Impact
2. Device statuses are then created for the highest impact exploits, based on:
   a. Integrity impact
   b. Availability impact

Following the TVA stage, MIA is performed in order to predict the likely impact of all events (both cyber and conventional) on the mission. During MIA, the time-based performance degradation and recovery of mission components is calculated as follows:

1. The mission vignette is topologically-sorted using Kahn's algorithm [4]
2. Weakest attack path analysis from attacker locations in the network to critical devices is performed using Dijkstra's algorithm [5], based on CVSS metrics:
   a. Authentication
   b. Access complexity
3. The time-based impact of all events is assessed, considering all known vulnerabilities, resulting in the calculation of:
   a. Performance degradation and recovery
   b. Collateral damage
4. Cyber impact is mapped to mission impact through consideration of:
   a. Device status
   b. Redundancy rules
5. Dependency degradation is tracked through the graph, based on:
   a. Sensitivity to upstream mission components
   b. Combination rules where there are multiple dependencies, covering cases such as those in which all dependencies must work, through to cases where only one need work, via various intermediate cases

The topological dependency-based mission graph allows resilience to cyber-attack to be seen at each mission component, as well as aggregated at the mission objective level.

Visual Analytics

Visual representation of modelling and simulation results and adversary actions is a key element of the JUMP system and is critical for assessing mission resilience and responding to cyber-attacks in a targeted manner that maximises mission success. Web-based visual analytics support interactive views that improve situational understanding and convey the implications of cyber-attacks for mission objectives, allowing damage assessment and mitigation strategies such as patching to be proposed and assessed.

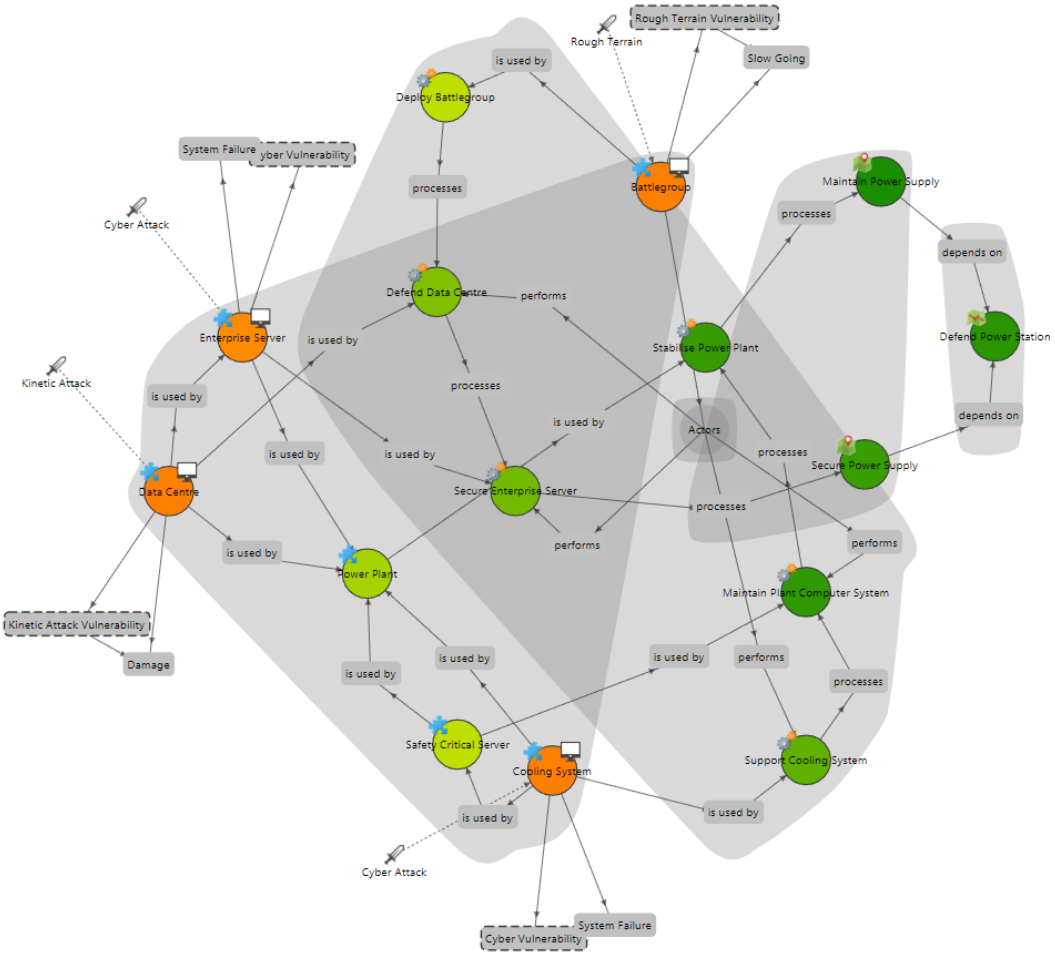

Figure 3: MIA showing time-based performance degradation and recovery

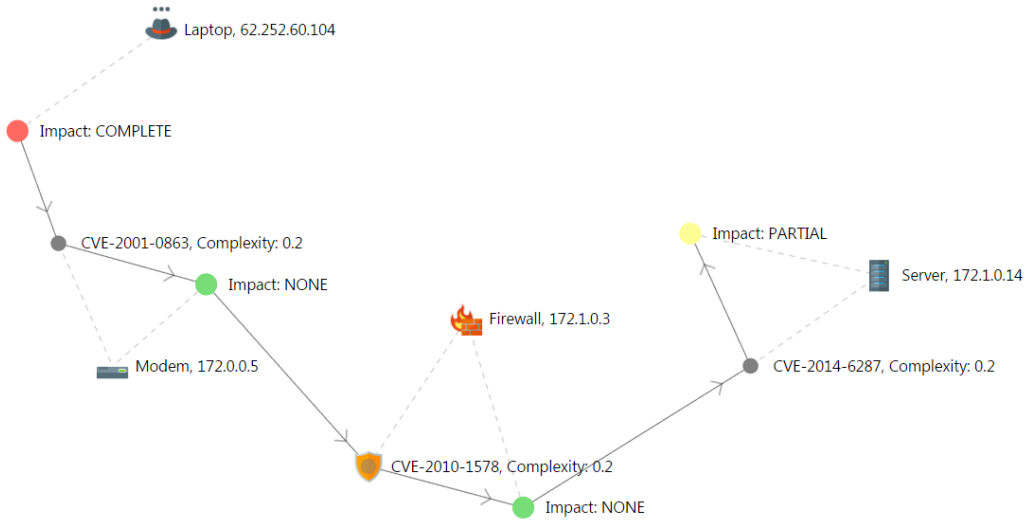

Figure 4: Weakest cyber-attack path analysis and patching

In the simulation results shown in Figure 3, the impact of physical and cyber effects has been quantified, along with the increased cyber resilience gained from actions such as patching mission-critical software vulnerabilities as shown in Figure 4.

Detailed cyber resilience information is presented in a separate JUMP screen for cyber analysts. The highly-interactive visual analytics are powered by industry-leading open-source technologies including Data Driven Documents (D3) [6], Facebook's React framework [7] and Bootstrap (originally Twitter Blueprint) [8]. Redux [9] is being used to implement Facebook's Flux architecture [10] for building client-side web applications.

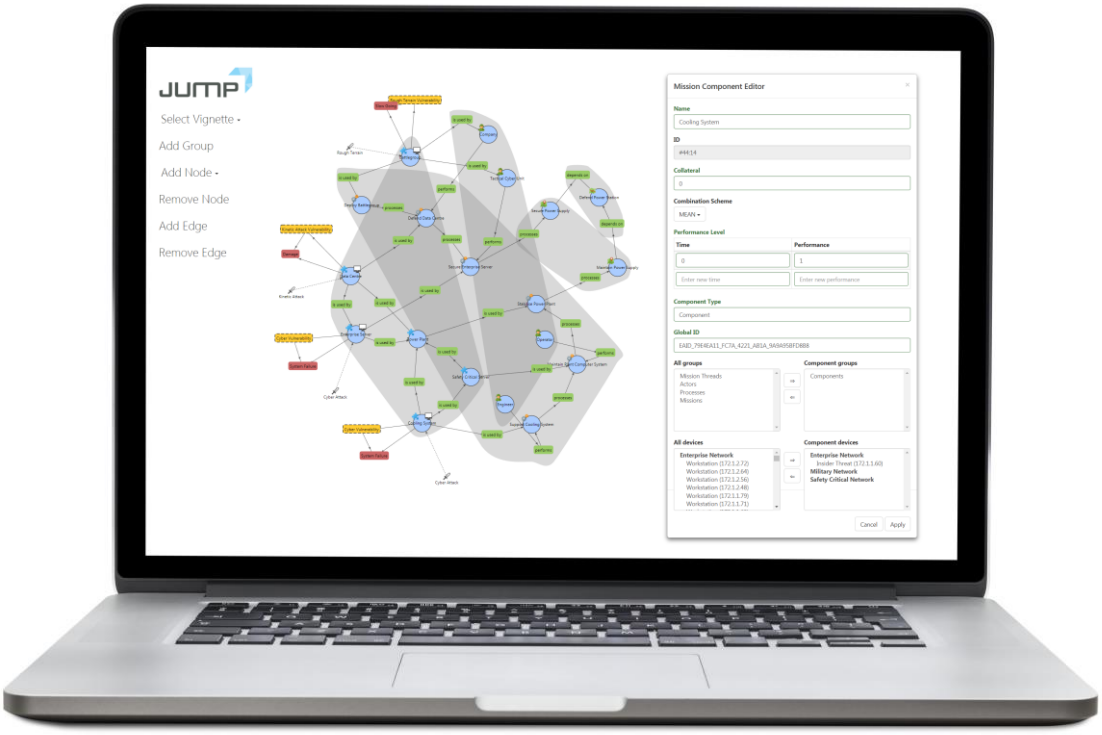

Figure 5: JUMP cyber analyst screen

The cyber analyst screen shown in Figure 5 supports full topological mission vignette editing, as well as views that allow interactive exploration of network vulnerabilities, assignment of network threats, data analytics and cyber resilience simulation. It also allows cyber-attack mitigations such as network hardening or patching of critical vulnerabilities to be staged and assessed.

Further Research

At the time of writing, the JUMP project has already completed Situational Understanding, Mission Objectives and CoA epics. The remaining Year 1 development epics concern CoA Evaluation, Red Teaming and CoA Decision-Aid Analysis. Planned enhancements to the functionality presented in this paper include what-if analysis, high impact – low probability analysis, alternative futures analysis and integration with the MOD's Cyber Situational Awareness Fusion Architecture (CySAFA).

References

[1] S. Jajodia and S. Noel, "Topological Vulnerability Analysis," *Advances in Information Security,* vol. 46,

pp. 139-154, 2009.

[2] "Staff Officers' Hand Book," British Army, 2014.

[3] National Institute of Standards and Technology, "National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/.

[4] Computer Incident Response Center Luxembourg, "cve-search Common Vulnerabilities and Exposures (CVE)," [Online]. Available: https://www.circl.lu/services/cve-search/.

[5] Forum of Incident Response and Security Teams (FIRST), "Common Vulnerability Scoring System," [Online]. Available: https://www.first.org/cvss/.

[6] A. B. Kahn, "Topological sorting of large networks," *Communications of the ACM,* vol. 5, p. 558–562, 1962.

[7] E. W. Dijkstra, " A note on two problems in connexion with graphs," *Numerische Mathematik,* vol. 1, p. 269–271, 1959.

[8] M. Bostock, "Data-Driven Documents," [Online]. Available: https://d3js.org/.

[9] Facebook, "React," [Online]. Available: https://facebook.github.io/react/.

[10] Bootstrap Core Team, "Bootstrap," [Online]. Available: http://getbootstrap.com/.

[11] Redux, "Redux," [Online]. Available: http://redux.js.org/.

[12] Facebook, "Flux," [Online]. Available: https://facebook.github.io/flux/.