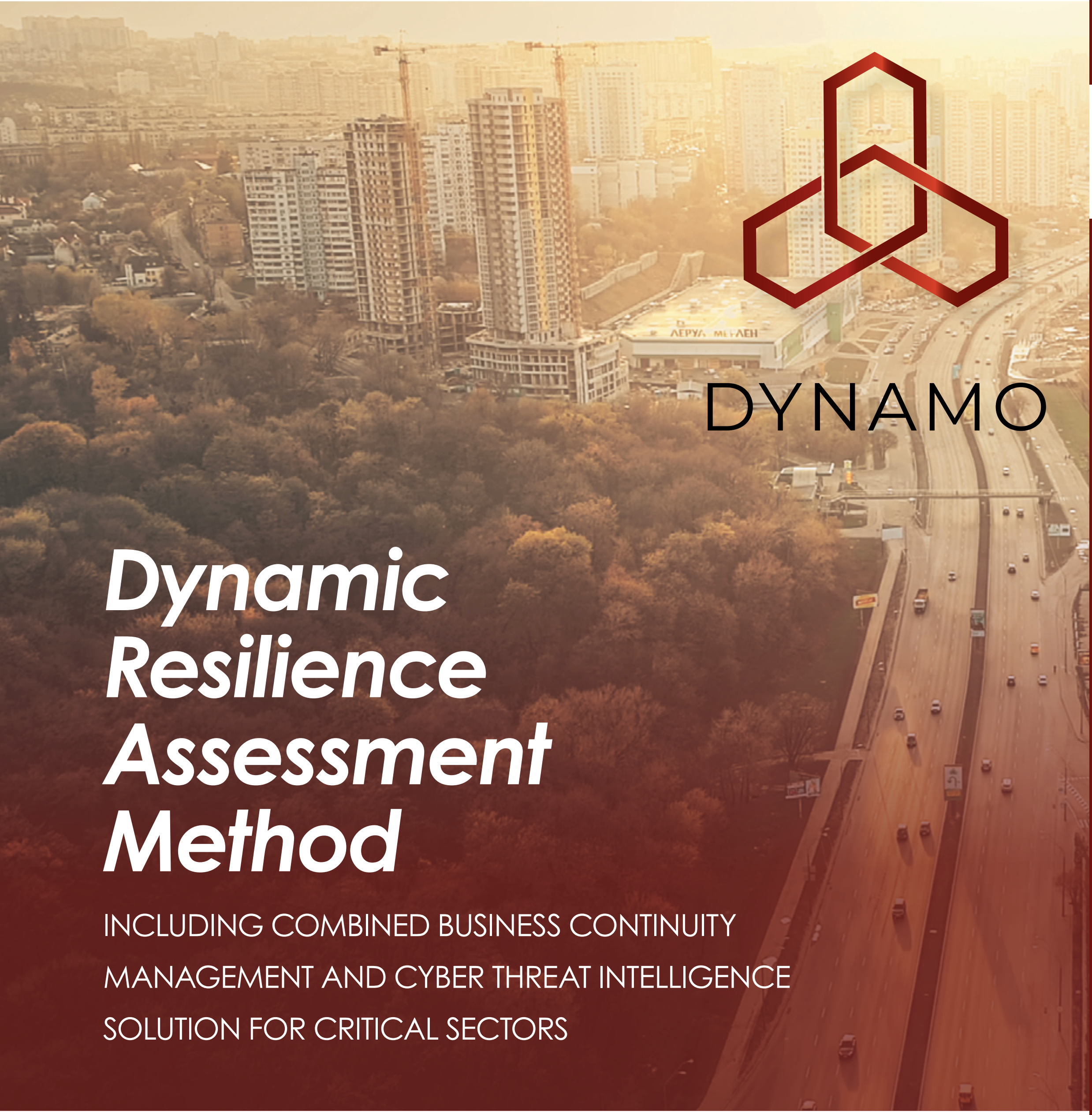

DYNAMO

Dynamic Resilience Assessment Method

INCLUDING COMBINED BUSINESS CONTINUITY MANAGEMENT AND CYBER THREAT INTELLIGENCE SOLUTION FOR CRITICAL SECTORS

Issue 04
Jan 2025

Prevent, Respond, Recover

DYNAMO Newsletter – aims at launching a new channel of communication to provide updates on project progress while discussing and highlighting insightful topics relevant to the DYNAMO project.
For more detailed information about the project, we invite you to visit our project website, which is continuously updated with the latest project news: **horizon-dynamo.eu**.

DYNAMO Overview

The current situation regarding potential cyber threats has increased the complexity of critical sectors and infrastructure such as energy, health and maritime. With increasing digitalisation and ever-evolving cyber threats, this represents an important challenge for business continuity. DYNAMO intends to develop and refine selected tools and bring them together in a single integrated platform. The knowledge generated by DYNAMO will help to improve and speed up the evaluation, response and recovery processes, by incorporating infrastructure-specific cyber threat intelligence, while also providing mitigation plans and tailored training. More information about DYNAMO and its vision, motivation and objectives can be found in the **project leaflet** and the **elevator pitch**.

Funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

horizon-dynamo.eu

@DYNAMO_HEU

dynamo-horizon

Project Coordinator

Fraunhofer Institute for
High-Speed Dynamics
Ernst-Mach-Institute
(Fraunhofer EMI)

Project Coordinator Support

Technikon Forschungs- und
Planungsgesellschaft mbH
technikon@horizon-dynamo.eu

Budget

€ 5 Million
100% EU-funded

Consortium

15 Partners
10 countries

Duration

36 Months
10/2022 - 09/2025

... what has happened by now?

- DYNAMO Review Meeting
- Successful 3rd General Assembly Meeting
- Organization and holding of the DYNAMO BCM Conference
- Publication of DYNAMO Papers
- Successful completion of the Horizon Results Booster Module B an C
- Production of numerous Communication & Dissemination material
- Participation on various conferences
- Organisation of our Stakeholder Reference Group Introduction Call

As you can see, DYNAMO's second project year was very successful and exciting, and these are just a few of the highlights we had. Therefore, follow the project on **LinkedIn** and **X** to not miss the latest updates about our work and to stay up to date.

DYNAMO Conference: Future-proofing Your Organisation through BCM and Sustainability

On the 12th June 2024, the University College Cork hosted the highly anticipated DYNAMO Conference, a landmark event focused on „Future-proofing Your Organisation through Business Continuity Management (BCM) and Sustainability." This groundbreaking conference was a collaborative effort organized by University College Cork (UCC) and KPMG Future Analytics, our esteemed partners dedicated to advancing knowledge and practices in business continuity and sustainability.

The DYNAMO Conference brought together a diverse group of professionals from various sector. This one-day event served as a dynamic platform for exchanging ideas, sharing best practices and lessons learned, and exploring innovative solutions aimed at ensuring organisational resilience in the face of evolving challenges.

Attendees had the opportunity to participate in a series of high-level presentations and an engaging panel discussion, each designed to provide practical knowledge for implementing effective BCM and sustainability practices.

The DYNAMO Conference also provided ample opportunities for networking and collaboration. Attendees engaged in meaningful conversations during networking breaks, fostering connections that are crucial for future collaborations.

As the conference concluded, the enthusiasm and commitment of the participants were palpable. The discussions and ideas generated during the DYNAMO Conference have undoubtedly sparked new initiatives and strengthened the resolve of organizations to prioritize resilience and sustainability in their strategic planning.

DYNAMO's General Assembly Meeting Highlights in Cork

The city of Cork served as the setting for the DYNAMO General Assembly, which took place on June 13-14, 2024. This important gathering of the DYNAMO consortium followed on from the successful DYNAMO conference and continued the momentum with strategic discussions and joint planning sessions.

Strategic Vision and Collaborative Efforts

The General Assembly Meeting was a significant event that brought together representatives from the partner organisations. The primary focus was to review DYNAMO's progress, set strategic priorities, and foster collaboration among members to drive forward the shared mission of developing a platform that will be able to improve organisational resilience.

Day 1: Progress, Tools and Dissemination

The first day began with a warm welcome by representatives from UCC and Fraunhofer, setting the stage for a productive meeting. A comprehensive overview of upcoming deliverables and milestones emphasized DYNAMO's forward momentum.
Fraunhofer led discussions on key outcomes and feedback from the Midterm Review Meeting. The integration and alignment of evaluation methodologies across WP2 and WP6 were highlighted, focusing on collaboration between technical leaders. Later, discussions centred on KPIs and the operational launch of WP6, reinforcing how technical and non-technical metrics will drive success. WP3 Task Leaders delivered a dynamic session, showcasing progress in Business Continuity Management, human resilience development, and AI-based disaster recovery methodologies. In the afternoon, KPMG FA presented DYNAMO's dissemination achievements, underlining the project's expanding presence through publications and outreach efforts. The day concluded with a banquet dinner, offering attendees an informal setting to network and discuss insights.

Day 2: Workshops and Innovations

The second day opened with a workshop led by WP4 Task Leaders, featuring demonstrations of innovative tools contributing to the overall project's objectives. The session provided practical insights into DYNAMO workflows, including real-world examples of how DYNAMO's components could support the defined project's use cases. CERTH presented cutting-edge demonstrations, showcasing the detection and forecasting capabilities of the developed DYNAMO tools, including abnormality identification and mitigation suggestions, advanced CTI correlation and analysis solutions, as well as secure and effective CTI sharing components. These sessions emphasized DYNAMO's technological advancements and their applicability in diverse scenarios. WP5 discussions focused on the development and deployment of the solutions comprising DYNAMO's architecture, exploring challenges and timelines. Participants reviewed the progress of the DYNAMO's GUI, which aims to enhance user experience through intuitive design and functionality. The event concluded with an interactive session on mapping tools to specific use cases and gathering end-user feedback on KPIs and functionalities.

Looking Ahead

The DYNAMO General Assembly in Cork proved to be a milestone event, reflecting the dedication and collaboration of all partners.

Successful Completion of the SRG Introduction Call

We are pleased to announce the successful completion of the DYNAMO Stakeholder Reference Group (SRG) Introduction Call held on 29th November 2024. The session marked an important milestone in guiding the collaborative development of a cybersecurity platform tailored to critical sectors, including maritime (transport), energy, and healthcare.

Key Highlights of the SRG Introduction Call:

1. *Purpose and Expectations:* The SRG will play a pivotal role in ensuring that the DYNAMO platform meets sector-specific needs, delivering practical and impactful solutions for end-users.
2. *Benefits of Participation:* Participants were introduced to how they can actively contribute to and benefit from the

platform's development, ensuring both relevance and usability.

3. *Collaboration and Next Steps:* Stakeholders were encouraged to engage with upcoming activities, including platform design discussions, evaluations, and pilot initiatives.

We would like to extend our gratitude to all participants for their valuable input, enthusiasm, and commitment to making DYNAMO a success. Your contributions are critical in shaping a solution that enhances business continuity and cybersecurity resilience across industries.

What's Next?

Stay tuned for further updates, including the outcomes of the SRG meetings and progress on the DYNAMO solution's development and pilot evaluations. For any follow-up questions or additional information, feel free to contact us or visit our website

Fraunhofer EMI at IEEE CSR 2024: Shaping the Future of Cyber Resilience

Fraunhofer EMI proudly represented our project at the IEEE International Conference on Cyber Security Resilience (CSR) 2024, held from September 2nd to 4th in London. This renowned global event brings together leading researchers, industry experts, and practitioners to explore the latest advancements in cybersecurity and resilience strategies.

As cyber threats continue to grow in scale and sophistication, the importance of building robust, secure, and resilient systems has never been more pressing. Fraunhofer EMI's participation underscores its dedication to developing cutting-edge security solutions that address today's challenges and anticipate tomorrow's needs.

During the conference, Fraunhofer EMI representatives took an active role by participating in panel discussions, presenting technical papers, and hosting interactive workshops. Their contributions provided valuable insights into emerging trends and showcased EMI's pioneering research in creating secure and reliable infrastructures.

The IEEE CSR conference also offered attendees a unique opportunity to engage with experts and gain a deeper understanding of the innovative work shaping the future of cyber resilience.

Unveiling Insights: New Project Publications

We are delighted to announce the release of several new publications stemming from our collaborative efforts in DYNAMO. These publications represent the culmination of months of hard work, dedication, and collaboration among our team members, and we are thrilled to share our insights and findings with the broader community.

Highlighting Key Publications:

Cybersecurity Through Thesis in Laurea University of Applied Sciences: The publication discusses the integration of cybersecurity topics into thesis work at Laurea University. It highlights how students engage in practical research to address real-world cybersecurity challenges, thereby enhancing their skills and contributing to the field. The paper emphasizes the importance of applied research in developing effective cybersecurity solutions and preparing students for professional roles in the industry.

Engagement of Actors in Expert Communities: The paper examines how individuals participate and interact within specialized professional groups. It explores the dynamics of engagement, factors influencing active involvement, and the impact of such participation on knowledge sharing and community development. The study provides insights into fostering collaboration and enhancing the effectiveness of expert communities.

Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity: The paper explores how Open Source Intelligence (OSINT) can enhance cybersecurity within financial institutions. It presents a case study demonstrating the effective integration of OSINT tools to identify and mitigate potential threats, thereby strengthening the organization‘s overall security posture. The study underscores the importance of leveraging publicly available information to proactively address cybersecurity challenges in the finance sector.

Utilization and Sharing of Cyber Theat Intelligence Produced by Open-Source Intelligence: The publication discusses the use and dissemination of cyber threat intelligence derived from open-source intelligence (OSINT). It highlights challenges in integrating OSINT effectively, emphasizing the importance of reliable, timely data sharing among stakeholders to strengthen cybersecurity measures. The paper proposes strategies for optimizing OSINT's role in threat detection and response, enhancing collective cyber resilience.

Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals: The paper highlights the role of the DYNAMO in enhancing cyber resilience across critical sectors like healthcare, energy production, and marine transport. By integrating artificial intelligence with cyber threat intelligence (CTI) and business continuity management (BCM), DYNAMO supports proactive decision-making and regulatory compliance. A key focus is on CTI sharing in healthcare, particularly under GDPR and NIS2 regulations, using a phishing attack on a hospital as a case study. The findings emphasize the challenges of managing sensitive data and aligning regulatory frameworks while providing actionable guidelines for improving cyber threat responses.

Business Model Canvas and Competition to Understand Exploitation of Cybersecurity Project Results: The publication introduces an enhanced Business Model Canvas (BMC) framework, termed BMC&C, which incorporates a ‚Competition‘ element to better assess an organization‘s position within the market. This addition aims to help organizations, particularly those involved in EU-funded cybersecurity projects, to effectively strategize the exploitation of their project results by considering competitive dynamics. The study demonstrates the practical application of BMC&C through workshops analysing the ECHO project‘s Early Warning System, highlighting its utility in fostering co-creative discussions and strategic planning. The authors conclude that BMC&C is a valuable tool for understanding market competition and enhancing the impact of cybersecurity innovations.

The Social Domain: Resilience of Information-Sharing Networks: The paper explores the critical role of social networks in enhancing the resilience of information-sharing systems. It emphasizes the importance of collaboration and trust between network members in improving response capabilities during crises. The study examines strategies for strengthening information-sharing practices and mitigating risks in digital and physical environments, highlighting the potential for more effective, adaptive systems in the face of emerging threats.

E-EWS-based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector: The publication presents a governance framework for sharing cyber threat intelligence (CTI) in the energy sector, utilizing an Early Warning System (E-EWS). It aims to enhance collaboration and information-sharing between organizations to improve cybersecurity resilience in the energy industry. The framework focuses on ensuring timely, effective, and secure data exchange to mitigate risks from cyberattacks. It emphasizes the importance of trusted partnerships and standardized processes to strengthen the sector‘s overall defense against evolving threats.

Measuring Social Impacts of Cybersecurity: The paper discusses frameworks for assessing the broader societal implications of cybersecurity beyond technical aspects. It highlights how cybersecurity affects not only organizational resilience but also societal well-being, trust, and economic stability. The authors propose metrics for evaluating these impacts and stress the importance of integrating social factors into cybersecurity decision-making. The paper underscores the need for a holistic approach in understanding the far-reaching consequences of cybersecurity policies and actions.

CTI Sharing Practices and MISP Adoption in Finland's Critical Infrastructure Protection: The publication explores the practices of Cyber Threat Intelligence (CTI) sharing and the adoption of the MISP (Malware Information Sharing Platform) in Finland's Critical Infrastructure Protection (CIP) efforts. It examines the importance of effective CTI sharing for enhancing cybersecurity resilience in critical sectors and how MISP facilitates collaboration between organizations. The study highlights the benefits of sharing threat data and the role of MISP in improving situational awareness, allowing for a more proactive approach to mitigating cyber threats.

These new publications not only showcase the depth and breadth of our team‘s expertise but also contribute to the broader academic discourse and industry knowledge in our field. By sharing our research findings and insights with the global community, we aim to stimulate discussions, inspire further inquiry, and drive innovation in the cyber security area. We encourage you to **explore these new publications** and share them with your colleagues, peers, and networks.

The work continues, ... so more to come!