Governance and Management Information System for Cybersecurity Centres and Competence hubs

Jyri Rajamäki and Janne Lahdenperä
Laurea University of Applied Sciences, Espoo, Finland

jyri.rajamaki@laurea.fi
janne.lahdenpera@student.laurea.fi

Abstract: Information sharing allows organizations to leverage the collective knowledge, experience, and analytical capabilities of their sharing partners in a community of interest. Sharing information is made easier with the help of a suitable information system. The DYNAMO project (10/2022-9/2025) creates tools for the cyber situational picture to support decision-making. One task of its mode of operation is to continue the development of the assets designed in the ECHO project (2/2019-2/2023). This article examines the design of ECHO's governance and management information system and how it can be applied to support the organisational processes and information-sharing needs of the collaborative network as a part of the DYNAMO project.

Keywords: Cybersecurity centre, Competence hub, Governance model; Data governance; Management information system

1. Introduction

The European Cybersecurity Competence Centre (ECCC) increases Europe's cybersecurity capacities and competitiveness. Each Member State should nominate one National Coordination Centre (NCC) and the Community formed from this would involve a large, open, and diverse group of actors involved in cybersecurity technology. ECCC will work together with NCCs to build a strong cybersecurity community. ECHO (2022), CONCORDIA (2022), SPARTA (2022), and CyberSec4Europe (2022) were the EU pilot projects launched to prepare the European Cybersecurity Competence Network that will be achieved through multiple different concepts, such as a governance and management model.

Cooperation and information sharing between different information security operators are based on heterogeneous data, models, and forecasts. The management of the information flows is an important area of successful governance of the European Cybersecurity Competence Network. The scope of DYNAMO (2023) is to generate a cyber situational picture for decision support. The DYNAMO approach is based on the refinement of the existing solutions of the ECHO project. This design science research (DSR) deals with the development of governance and management information systems (GMIS) for cybersecurity centres and competence centres. The extension of the ECHO GMIS system would enable information sharing and cooperation within the network. This study focuses on the conception, structure, and application of information-sharing and management systems for cybersecurity centres and competence hubs where the ECHO GMIS is based.

This design science research (DSR) follows the DSR framework and the DSR checklist questions (CQ) (Hevner & Chatterjee, 2010). These DSR CQs are mapped to this paper as follows:

- *DSR CQ1 - What is the research question (design requirements)?*
  The main research question: *What kind of information system best supports the operation of a collaborative network organization?*
- *DSR CQ2 - What is the artifact? How is the artifact represented?*
  Section 4 describes the platform of the information system and its most important functions.
- *DSR CQ3 - What design processes (search heuristics) will be used to build the artifact?*
  Section 4 presents the heuristic design cycles of the artifact.
- *DSR CQ4 - How are the artifact and the design processes grounded by the knowledge base? What, if any, theories support the artifact design and the design process?*
  Section 2 deals with the knowledge base of this study.
- *DSR CQ5 - What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle?*
  Section 4.4 discusses the self-evaluation of the artifact.
- *DSR CQ6 - How is the artifact introduced into the application environment and how is it field tested? What metrics are used to demonstrate artifact utility and improvement over previous artifacts?*
  Section 5 deals with the implementation of the artifact.

- *DSR CQ7 - What new knowledge is added to the knowledge base and in what form (e.g., peer-reviewed literature, meta-artifacts, new theory, new method)?*
  Section 'Discussions' discusses these items.
- *DSR CQ8 - Has the research question been satisfactorily addressed?*
  'Conclusions' answers to the research question.

2. Groundings to the Knowledge Base

2.1 Governance and Management Information Systems

Organization's governance function is responsible for determining its strategic direction. Chartered Governance Institute UK & Ireland (2022) defines corporate governance as "the system of rules, practices and processes by which a company is directed and controlled." They also add that corporate governance is a toolkit with which management and board are able to deal with the challenges of running a company more effectively. One function of corporate governance is ensuring that businesses have appropriate controls and decision-making processes in place so that the interests of all stakeholders are balanced. Corporate governance is also very important when meeting the requirements of laws and regulations such as the General Data Protection Regulation (GDPR) or the Network and Information Security (NIS) Directive.

Information governance involves the overall strategy for information, it handles information in the context of policies, systems, people, and processes. Utilizing its different elements can help us to create and maintain applicable policies and procedures that help meet the requirements for our data privacy. Information governance balances the risk that information presents with the value that information provides. Issues covered by information governance include information security and protection, compliance, data quality, data governance, electronic discovery, risk management, privacy, data storage and archiving, knowledge management, business operations, and management, audit, analytics, IT management, master data management, enterprise architecture, business intelligence, big data, data science, and finance.

The management functions of an organization take the strategic direction and translate it into actions that bring the organization closer to achieving its strategic goals. A management information system (MIS) is an information system used for decision-making, and the coordination, control, analysis, and visualization of information in an organization. The study field of MIS involves people, technology, and processes in an organizational context. In corporations, the goal of the use of MIS is to increase the value and profits of the business through IT tools used to support processes, operations, and intelligence. Information sharing is considered one of the most important ways to increase organizational efficiency and performance (Yang & Maxwell, 2011).

2.2 Information System Design Theories

The main function of any implemented information system is to improve the efficiency, effectiveness, and cyber resilience of the organization where it is implemented. For designing information systems with design science, Hevner, et al. (2004) present seven guidelines to follow. These guidelines are not to be adhered to too literally, but during the design process, each of them should be assessed at least somewhat. The guidelines are:

1. Design as an Artifact – The outcome of the research should be an IT artifact that focuses on a specific problem related to the organization.
2. Problem Relevance – It is important for information system research to address the problems that arise in the environment it is applied.
3. Design Evaluation – To demonstrate the quality of the design artifact, well-executed evaluation methods should be used.
4. Research Contributions – It is important to provide clear contributions in the area of the research artifact.
5. Research Rigor – The application of rigorous methods is required in both the construction and the evaluation of the designed artifact.
6. Design as a Search Process – The target of finding an effective solution to a problem is an inherently iterative search process.
7. Communication of Research – It is important to present the research results in a form that is easily understood both by management-oriented and technology-oriented audiences.

When designing an information system, it is also very beneficial to define different roles and responsibilities within the system right from the beginning. One way to accomplish this is to use a responsibility assignment matrix, also known as RACI matrix (RACI Chart, 2022). RACI matrix defines the different roles as responsible, accountable, consulted, and informed. One critical part of information system design is to follow an architectural approach first presented by Zachman (1987) with specific aspects developed for the web-based systems presented by Molnár and Tarcsi (2013). We adapt these approaches starting from the operational view through the system view, down to the technical view for the web-based GMIS for ECHO with a focus on information sharing and the need for migration from the ECHO Project Information System to ECHO Collaborative Network Organization GMIS.

2.3 Information Sharing

A key part of any organization's data management is information sharing, without effective data sharing operational capacity and decision-making may be disturbed. The system used for information sharing should be compatible with the whole organization, otherwise, it can lead to unnecessary transcribing and rekeying of the information when it is transferred between systems. Other important requirements for information-sharing systems are ease of access and fast data search. If the needed information is not readily accessible, it can cause frustration and reduce organizational effectiveness. (Gordon, 2013)

Information sharing can be divided into two separate categories, internal and external. Interactions in the work community can lead to a higher level of cooperation and better work performance (Peters & Manz, 2007). Effective internal communication increases inspiration, engagement, and productivity, but it is not easy to find the correct internal communication system for the organization and its culture. Newsletters and emails are not effective communication. It is important that the internal channels are immediate, fast, targeted, measurable—and mobile. An organisation's internal communications can for example include different mailing lists, where each department (ECHO CNO entity) has its own list. For the purposes of internal information sharing, an efficient tool is an organization-wide intranet, where all needed information is easily accessible when needed. With external information sharing, one commonly used method is the organization's web page. Any news or other shared information can be easily accessed by all visitors through a www-site. Building a specific extranet for the organization's various partners can also be beneficial, so they can easily communicate without having access to the intranet. Smooth communication channels are extremely useful in building stakeholder engagement and ensuring effective end-user collaboration (Ruoslahti & Tikanmäki, 2019).

Sharing cybersecurity information between different organizations can be very helpful. It can improve response to threats, help to defend against potential attackers, and mitigate damages. Information sharing can also help to improve relations and build trust between organizations. Information sharing is not without any challenges, legal issues may arise when different countries have different definitions of protecting classified information. Therefore, it is very important to use the right information-sharing models and frameworks to achieve efficient data sharing between organizations (Rajamäki & Katos, 2020).

2.4 Information System Migration

As information systems grow older, they can become outdated and may no longer serve their intended function. Thus it is often very important for an organization to migrate to a more evolved and modernized platform that can provide all the needed services. Information System Migration projects can be very complex, as they should be completed without any loss of data or functionalities, and access to the system should be available during the migration process (Klettke & Thalheim, 2011). Some factors that may further increase the complexity are dealing with legacy information systems (Limaj, et al., 2020) and migrating on-premises data to a cloud platform (Alharthi, 2023).

For IS migration Klettke and Thalheim (2011) present three different strategies, each with its own strengths and weaknesses. Choosing the right strategy to use depends on system complexity, modularization of the legacy system, frequency of the data changes, amount of data in the database, and accepted delay time of the system.

- Big bang – In this strategy, a completely new system is developed at once. During the development process, the legacy system serves as the operating system. Although the migration process can be easy to manage, development times are usually long, and there is no system availability during the transition.

- Chicken little – In this strategy, the system is modularized, and all components are migrated separately. System availability is high through the transition and the individual development and migration times are short. This strategy requires two parallel systems to exist at the same time, which can prove problematic when they must interact with each other.
- Butterfly – Combination of both previous strategies. In this strategy, the focus is on the migration of the database. The legacy system is designated as read-only storage and all the required changes are done to the new system. This mitigates the risk of possible data loss, and it provides a lot of already available data with which to test the new system. Although this strategy can lead to long development times and the design of the old system has a big impact on the new one.

3. Environment and the Relevance Cycles

The relevance cycle initiates design science research with an application context that not only provides the research with requirements as inputs but also defines the acceptance criteria for the final evaluation of the research results (Hevner & Chatterjee, 2010). In this study, the application domain deals with the ECHO project and its information systems, the planned ECHO collaborative network organisation (CNO), and the requirements for the GMIS coming from the environment.

3.1 The ECHO Project

European network of Cybersecurity centres and competence Hub for innovation and Operations (ECHO) is a European Union project founded under European Commission's Horizon 2020 Program. The aim of ECHO is to develop a unified cyber defence ecosystem for the European Union and improve the secure cooperation of its members. This is achieved through multiple different ECHO concepts, such as ECHO Governance model for managing current and future partners, ECHO Federated Cyber Range for cyber simulation training, and ECHO Early Warning System for secure sharing of cyber threat information. One of the goals of ECHO is to raise EU citizens' cybersecurity awareness, helping everyone to be more informed about potential threats. This education is also expanded into different industry fields to help them mitigate possible attacks. Creating an EU-spanning network of cybersecurity hubs is the main challenge of the project, which it aims to complete in the near future. (ECHO, 2022)

The information system of the ECHO project consisted of the following parts:

1. Websites that share public deliverables, scientific publications, newsletters, and other information intended for general distribution. They also included a service related to supporting partnership engagement.
2. Internal SharePoint, Teams, and One Drive for Business platform which included project repositories for contract documents, changes, review-related documentation, reporting documentation, contact information, templates, work documents for deliverables, final versions of all deliverables, internal work documents, agendas, minutes, etc. The project's telephone conference system was also implemented using this.
3. Zenodo open repository used for open datasets.

3.2 Transitioning from project to network

One of ECHO's big milestones is the transition from the initial ECHO project into the complete ECHO CNO. This transition can be summarized as moving from the Current Operating Model (COM) to the Target Operating Model (TOM) (Mladenova, et al., 2022). The final goal is to build CNO that have Central Hubs, National Hubs, and Service Groups (Penchev, 2021). Central Hub is ECHO CNO's overall management (including the governing level of boards/councils) body. National hubs are established on a national level and serve as contact points between the Central Hub and national authorities and organizations. Service groups are formed around the delivery of specific services, such as the ECHO Federated Cyber Range (E-FCR) or the ECHO Early Warning System (E-EWS). The ECHO GMIS is mainly intended for internal use within the organization. The Catalogue (Market Place) is intended for service providers (Service Groups) and their customers, and the web pages serve all stakeholders. (Penchev, G. et al., 2021, p. 45):

To ensure sustainability after the end of the ECHO project, the need for a transition plan was implemented. As project partners have varying levels of commitment, capabilities, resources and, experience, the plan must take into account the capacity of individual organizations to change. Figure 1 shows the approach used in transition

planning and change management, where Initial Operating Capability (IOC) is achieved in the first phase, then plans are implemented in the second phase and the CNO can move to Final Operating Capability (FOC). The goal is to reach the IOC by the end of the ECHO project in February 2023 (Mladenova, et al., 2022).

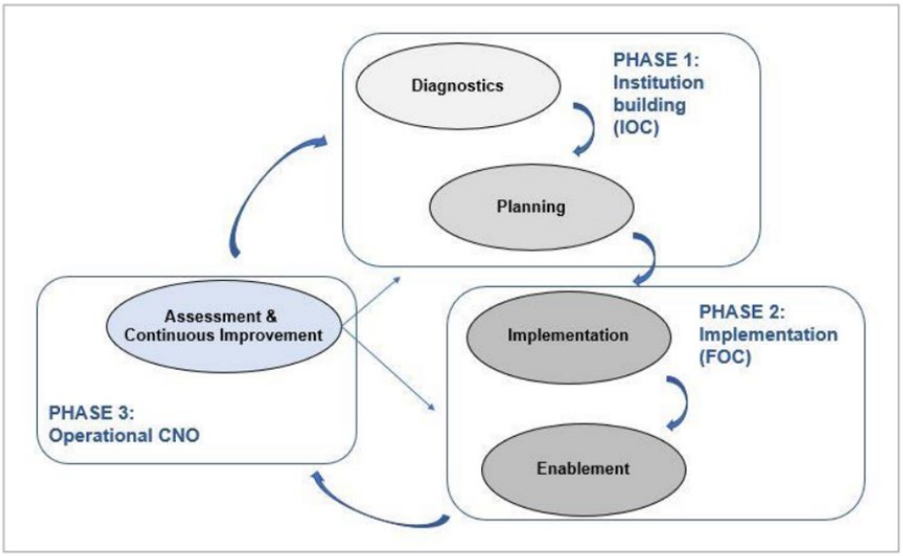

Figure 1: Approach to transition planning and managing change (Mladenova et al. 2022, 134)

3.3 ECHO GMIS Requirements

Deliverable ECHO D3.13 defines the high-level requirements for GMIS: (1) support processes, (2) ensure efficient information sharing, and (3) help to meet the requirements of laws and regulations. The ECHO CNO's core processes are strategic planning, partnership development, innovation management, and catalogue and customer relations, and other processes are HR management, financial management, data management including document handling, portfolio management, continuity management, and external relations management (Penchev, et al., 2021).

Communication between different partners is a key factor in the governance of collaborative networked organizations. The ECHO GMIS should solve this by having a communication platform that is community-based and accessible to all different ECHO members and partners. The platform will include, for example, an intranet, extranet, web pages, calendar management, and document repositories.

The ECHO CNO provides services through an electronic marketplace, which is a digital service that allows individuals or merchants to enter into sales or service contracts with merchants. This means that the Directive on Security of Network and Information Systems (NIS/NIS 2 Directive) applies to GMIS. The General Data Protection Regulation (GDPR) applies to all personal data. This means that GMISs must define controllers and processors who demonstrate compliance with its requirements with specific documents, including relevant logs, policies, and procedures. In addition, the national legislation of the countries where ECHO CNO operates must also be observed.

4. Design Cycle

It has been decided to implement GMIS with Microsoft SharePoint. Next, with the help of blogs found on the internet, etc., we will investigate what the future platform should be like, how internal communication should be implemented, how to ensure compliance with laws and regulations, and how to carry out self-evaluation.

4.1 Platform planning

Microsoft (2022) describes SharePoint as a portal, where you can engage, learn, and collaborate. It consists of portals, sites, and pages. SharePoint as an internal communications tool has many possibilities and solutions. It is part of Microsoft 365 and is possible to combine it with Teams for chats and meetings, Yammer with live events, Outlook for emails, Stream for channels to follow, and Viva for connecting. You can have a portal with

news, connecting, events, sharing, announcements, networking, communicating, training, and learning, employee onboarding, measuring of engagement, good user experience and much more.

According to Microsoft, an intelligent intranet is made of rapid deployment, has been built with user-experience in mind, has a personalized experience, and has software as a service, which means that it is updated automatically and always has the latest technology. Modernizing the intranet is a big job that needs resources but will be worthwhile because it makes the intranet dynamic and scalable, it can target the audience and works on any device, there is central governance of permissions, security, and sharing grows the adaption due to relevant content, user-friendliness, and responsiveness. A modern intranet is where you start your day, it promotes collaboration and has everything in one place. SharePoint has an intuitive discussion board that can be used by the employees to discuss work subjects or give opinions. It is fast to create and can be embedded on the intranet or on the departmental home pages. Discussions can also be highlighted so they are shown under the featured view (Jones, 2014).

There are Wiki pages, where a document library can be edited or added to by anyone. Existing pages can be linked together, and it is possible to link to new pages or create pages. You can use Announcement lists for announcements that expire on a specific date and are shown on the intranet landing page or any other page. You can search in it and add alerts to show when a new announcement is made. If you need an opinion, you can use a survey for input. They can come as a pop-up, be exported to Excel, and get stored as SharePoint list. It is an easy way to gather data through information and replies. There is an alert possibility for changes in contents, a community site template for social networking around a given subject with gamification giving points for completing tasks, discussion forums and an activity view of the members, you can add a web part to wiki or content pages for video on the intranet with a thumbnail and create a blog site template where you can add and manage your posts, comments, and categories. You can also use Yammer as social networking almost like Facebook.

There are add-ons for DocRead for tracking and distributing tasks and DocSurvey for mandatory quizzes. And you can use Delve for monitoring usage inside SharePoint (Jones, 2014). The content tagging. It is almost like Hash tagging used in Twitter but is a Tag cloud that is larger when it is a popular tag and it can be clicked to see the tagged content, to follow a tag, to add notes, and to view people who are following the tags. SharePoint also has a mobile-friendly version that works on SharePoint Online and Microsoft has created a mobile app for iOS and Android.

SharePoint Team site can be used for communication and collaboration, like for projects, tracking status, planning events, etc. Or you can use Communications site for communicating messages to a wide audience, where there are a few content creators and a wide audience for content like HR-related, guidelines, policies, micro-sites, etc. Or a hub site that shows what is happening across sites, is searchable, and creates cohesion with shared navigation, look and feel (Shareknowledge, 2020). Even though there seem to be many ways to use SharePoint as an internal communications tool there are opinions about it not being good enough for that purpose. SharePoint is lacking user engagement when it is used for enterprise communications being a document management and storage system promoting collaboration, but it is not a communications platform and cannot compete with modern employee experience platforms (Unily, 2022). They reference to a Forrester survey of business leaders using SharePoint from 2013 where 64% of business leaders could not see the expected degree of adoption, 62% meant it was difficult to use, 49% preferred other tools, 44% could not see any added benefits and 44% meant that it did not reach the functional requirements. SharePoint is a solution that is often chosen by IT because it is an easy choice in a Microsoft-led organization and will integrate with the existing Microsoft solutions they already have. Unily (2022) lists five reasons why SharePoint doesn't cut it for internal communication:

1. SharePoint is lacking essential communications functionalities such as engaging, meeting expectations, personalisation, availability on any devices, and delivery through many channels and in many formats.
2. SharePoint cannot unite communication channels such as integrating to other than Microsoft solutions. One example is Slack and meeting employees on channels they use daily.
3. SharePoint means relying on IT resources, where all changes need to be done by IT.
4. The lack of measurement and analytics capabilities; there will be no possibility to see what employees are engaging with, and when and how they are doing it.
5. It fails for frontline workers as they do not have access to computers, and it is not working optimally on mobile.

Harris (2022) gives a broader view of why SharePoint is chosen in organizations and if it is a good choice. SharePoint is a natural choice for organizations that are using Microsoft 365 even though it doesn't always meet managers' needs as they are today. The benefits of SharePoint are document management, centralizing policies and procedures, collaborations, sharing, storing, and organizing information. It is natively integrated with Outlook, Teams, Yammer, and OneDrive. It allows to access information from anywhere through SharePoint online and offers enhanced security with access management and encryption. It has a good content management system and approved content can be published on the internet and social media platforms. There are possibilities to automate and streamline processes and business operations, and it can be integrated with applications, email programs, and browsers giving a good user experience. The negative side of SharePoint is that it is mostly for top-down communications, it could be integrated with Teams for better employee engagement and collaboration in decision-making but is not designed for two-way internal communication. SharePoint is not good for frontline workers due to the need for Microsoft 365 license. Information overload is one issue as it is difficult to send the correct information to the correct people unless they are using targeting, which still can be improved in SharePoint. SharePoint also needs a third-party solution if branding is important as SharePoint alone will look like Microsoft intranet. Also, the engaging features are limited and to meet employee expectations third-party solutions with more features like employee advocacy, desk booking, and more is recommended (Harris, 2022).

4.2 Internal communications

The intranet needs to be well-designed, user-friendly, responsive, and full of engaging information which the users require (Pocketstop, 2018). Internal communication best practices to give the employees the feeling of importance and purpose, remove the hierarchical information flow, and avoid gossip and rumours include (Pocketstop, 2018):

1. Internal communications strategy – think, strategize, and Plan
2. Use the right internal communications tools
3. Use visual communication – screens, SOME, motivational quotes, goals, accomplishes
4. Provide channels for feedback and ideas
5. Encourage to give feedback
6. Avoid communication overload – brief, to the point, relevant, automation of key messages
7. Promote employee resources and training
8. Encourage cross-departmental communication and collaboration

According to Temkin and Lucas, the five I's that drive employee engagement are to inform, inspire, instruct, involve, and incent (Temkin & Lucas, 2018). These can also be used as guidance for internal communication. Strachan (Strachan, 2022) lists six best practices to build a successful intranet and recommends considering the three E's: engagement, enablement, and empowerment. He also says that intranet should have relevant and encouraging information. The best practices include defining intranet with strategic goals, where you can measure the KPIs for Employee adoption through how many are using it, time to access knowledge through the time from search to result, average click rank through search engine effectivity and employee satisfaction through feedback surveys. The second part is about consulting the employees to find out what is most important about the corporate intranet, what they like/ do not like of the intranet, what information they want to/do not want to see, what user experiences would increase the usage of intranet. The third part is to unify the content across the company. The fourth part is to personalize the experience through using location, departments, roles, tenures, projects, product lines and markets. The fifth part is about having a balance between business and personalized content. And the last is about improving the employee experience.

4.3 Compliance with Laws and Regulations

As ECHO's operating environment is the European Union, there are couple of directives we have to be compliant with. The first one is the General Data Protection Regulation (GDPR), which requires all organizations to have rigorous data handling policies with data controllers and processors. The other one is the Network and Information Security (NIS) Directive, which is an EU-wide legislation on cybersecurity, with a specific aim to achieve a high common level of cybersecurity across the Member States. This Directive applies to ECHO GMIS, as the platform will have an online marketplace for the services offered by various partners.

The following sections of the NIS directive need to be addressed when designing the future GMIS (ENISA, 2022):

- Human resource security – security training programs are required for employees with CIS related responsibilities.
- Information system security risk analysis – during the designing process, regular risk analysis are conducted so possible risks are assessed as early as possible.
- Information system security audit – taking account the regularly updated risk analysis, all critical assets are frequently audited to ensure compliance with regulations.
- Ecosystem mapping – during the design process, all documentation of GMIS ecosystem is frequently updated.
- Information system security policy – building up to the risk analysis, an information system security policy will be established and maintained.
- Ecosystem relations – the interfaces between ECHO GMIS and third parties are designed so that potential risks are mitigated.

As the EU is a very diverse area, there are also various national laws and regulations concerning data privacy and handling. All of this has to be taken into consideration when building the ECHO GMIS.

4.4 Self-evaluation

During the ECHO project, there have been several workshops (e.g., the ECHO WP3 Workshop, 10-11 Nov. 2022) from which feedback has been received for further development of the project. As the future GMIS will have multiple national and international shareholders, this feedback has been very beneficial for the clarifications and confirmations it has provided. Self-evaluation and gathering feedback will continue until the end of the project.

5. Implementation plan

The overall migration is a key effort to move from ECHO Project to ECHO CNO. A big challenge is to figure out how to transfer all ECHO Project materials to the new GMIS or other repositories. The transferred material can be any digital material, such as a document, image, video, folder, or entire folder structure with documents. Once the material to be transferred is defined, a digital object is formed from it. In this context, it is given a persistent ID and the desired metadata is defined. After this, the transfer to the desired new location is performed.

The first step was to design a new folder structure for the old SharePoint. One big change between ECHO Project's SharePoint portal and the future GMIS is the access and user rights. In the project's portal all users had access to everything, but as CNO partners are not the same as ECHO project partners, this should be changed. Even after the project, the project partners have to be guaranteed access rights to the project outputs. As some of the project folders contain confidential information, not all members of the future CNO can be automatically given access to them. Folder access and user rights should be determined using the RACI matrix.

Creating and implementing a new information system is a major task that must be planned carefully and in sufficient time. With the ECHO project ending, there is no time to build a completely new system before the CNO starts operating, so we have to make do with the old system at first. The main thing is that the system starts small and grows with the Central Hub. GMIS and web visibility should be outsourced and in the first phase, the continuation of their maintenance is agreed upon year by year for a maximum of 5 years with the current administrators. A lot of additional work will be required during the transition, as CNO partners are not the same as the project partners and may have different levels of access and user rights. Once the CNO's operations are established, the GMIS planning project can be initiated. The size of this information systems development project depends on the scope and scale of the CNO's operations.

6. Discussion and Conclusions

The DYNAMO project (10/2022-9/2025) creates tools based on the refinement of the existing solutions of the ECHO project for a cyber situational picture to support decision-making. Information sharing allows organisations to leverage the collective knowledge, experience, and analytical capabilities of their sharing partners in a community of interest, improving the cybersecurity of multiple organisations. Towards this goal, the tools developed in DYNAMO convert heterogeneous data into common formats and protocols, which enables automation and allows organizations to quickly exchange information. Privacy preservation techniques are used to protect sensitive and classified information without preventing access and sharing of information. This paper examines the design of the ECHO governance and management information system and describes

the structure of such an information system, which best supports the organisational processes and information-sharing needs of the collaborative network.

Acknowledgements

Acknowledgement is paid to DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

Alharthi, D., 2023. Secure Cloud Migration Strategy (SCMS): A Safe Journey to the Cloud. *Vol. 18 No. 1 (2023): Proceedings of the 18th International Conference on Cyber Warfare and Security*, pp. 1-6. DOI: https://doi.org/10.34190/iccws.18.1.1038 [Accessed 10 March 2023].

CONCORDIA, 2022. *CONCORDIA - Home*. [Online] Available at: https://www.concordia-h2020.eu/ [Accessed 13 December 2022].

CyberSec4Europe, 2022. *Cyber Security for Europe - Home*. [Online] Available at: https://cybersec4europe.eu/ [Accessed 13 Dec. 2022].

DYNAMO, 2023. *DYNAMO Project - Home*. [Online] Available at: https://horizon-dynamo.eu/ [Accessed 18 January 2023].

ECHO, 2022. *ECHO - Home*. [Online] Available at: https://echonetwork.eu/ [Accessed 13 December 2022].

ENISA, 2022. *Minimum Security Measures for Operators of Essentials Services*. [Online] Available at: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services [Accessed 19 January 2023].

Gordon, K., 2013. *Principles of Data Management - Facilitating Information Sharing*. Second Edition. Swindon: BCS Learning & Development Limited.

Harris, Y., 2022. *Is SharePoint a good internal communication tool?.* [Online] Available at: https://powell-software.com/resources/blog/sharepoint-internal-communication-tool/ [Accessed 19 January 2023].

Hevner, A. & Chatterjee, S., 2010. *Design research in information systems: theory and practice*. New York: Springer Science and Business Media.

Hevner, A., March, S., Park, J. & Ram, S., 2004. Design science in information systems research. *MIS Quarterly*, 28(1), pp. 75–105.

Jones, M., 2014. *11 Ways to Use SharePoint for Internal Communications*. [Online] Available at: https://community.aiim.org/blogs/mark-jones/2014/08/21/11-ways-to-use-sharepoint-for-internal-communications [Accessed 18 January 2023].

Klettke, M. & Thalheim, B., 2011. Evolution and Migration of Information Systems. In: Embley, D., Thalheim, B. (eds) *Handbook of Conceptual Modeling*. Heidelberg: Springer, pp. 381–419.

Limaj, E., Bernroider, E. & Ivanova, M., 2020. Facing Legacy Information System Modernization in Scaling Agility in the Banking Industry: Preliminary Insights on and Non-technical Barriers. In: Joey George, Paul, Rahul De' (Ed.), *Proceedings of the 41st International Conference on Information Systems (ICIS)*. AIS Association for Information Systems, pp. 1–9.

March, T. & Smith, G., 1995. Design and natural science research on information technology. *Decis Supp*, 15(4), pp. 251-266.

Mirosoft, 2022. *Step 2: Review Microsoft 365 communication tools*. [Online] Available at: https://learn.microsoft.com/en-us/sharepoint/review-communication-apps?source=recommendations [Accessed 19 January 2023].

Mladenova, I., Shalamanov, V. & Shalamanova-Filipova, A., 2022. Governance Consulting Services and Tools: Transition Planning and Implementation for Collaborative Networked Organisations in the Cyber Domain. *Information & Security: An International Journal*, 53(1), pp. 131-146.

Molnár, B. & Tarcsi, Á., 2013. Design and architectural issues of contemporary web-based information systems. *Mediterr. J. Comput. Netw.*, Volume 9, pp. 20-28.

Penchev, G. et al., 2021. *ECHO D3.3 GOVERNANCE MODEL DESCRIPTION*. [Online] Available at: https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D3.3.Governance-Model-Description.pdf [Accessed 18 November 2022].

Penchev, G., 2021. Planning and Implementing Change in Cyber Security Network Organisations. *Information & Security: An International Journal*, 50(1), pp. 89-101.

Peters, L. & Manz, C. M., 2007. Identifying antecedents of virtual team collaboration. *Team Performance Management: An International Journal*, 13(3/4), pp. 117-129.

Pocketstop, 2018. *Rethinking Internal Communications*. [online] June 15. [Online] Available at: https://pocketstop.com/blog/rethinking-internal-communications/ [Accessed 19 January 2023].

Pocketstop, 2018. *What Is an Internal Communication System?* [Online] Available at: https://pocketstop.com/blog/what-is-an-internal-communication-system/ [Accessed 19 January 2023].

RACI Chart, 2022. *RACI Chart*. [Online] Available at: https://racichart.org/ [Accessed 19 November 2022].

Rajamäki, J. & Katos, V., 2020. Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence. *Information & Security: An International Journal*, 46(2), pp. 198-214.

Ruoslahti, H. & Tikanmäki, I., 2019. Complex Authority Network Interactions in the Common Information Sharing Environment. In: Bernardino, Jorge; Salgado, Ana; Filipe, Joaquim (Eds.) *Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2019).* Setúbal: Science and Technology Publications, pp. 159 – 166.

Shareknowledge, 2020. *3 new ways SharePoint impacts communication in the workplace*. [Online] Available at: https://www.shareknowledge.com/blog/3-new-ways-sharepoint-impacts-communication-in-the-workplace [Accessed 19 January 2023].

Smallwood, R. F., 2019. *Information Governance*, 2nd Edition. John Wiley & Sons, Inc.

SPARTA, 2022. *SPARTA - Home*. [Online] Available at: https://www.sparta.eu/ [Accessed 13 December 2022].

Strachan, C., 2022. *6 Intranet Best Practices for a More Engaged Workplace in 2022*. [Online] Available at: https://www.coveo.com/blog/intranet-best-practices/ [Accessed 19 January 2023].

Temkin, B. & Lucas, A., 2018. *Employee Engagement Competency & Maturity Insight Report 2018.* [Online] Available at: https://www.xminstitute.com/research/2018-employee-engagement-maturity/ [Accessed 19 January 2023].

The Chartered Governance Institute UK & Ireland, 2022. *What is corporate governance?* [Online] Available at: https://www.cgi.org.uk/about-us/policy/what-is-corporate-governance [Accessed 18 November 2022].

Unily, 2022. *Why SharePoint doesn't cut it for internal comms*. [Online] Available at: https://www.unily.com/insights/blogs/why-sharepoint-doesnt-cut-it-for-internal-comms [Accessed 19 January 2023].

Yang, T. & Maxwell, T., 2011. Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, 28(2), pp. 164-175.

Zachman, J. A., 1987. A framework for information systems architecture. *IBM Systems Journal*, 26(3), pp. 276-292.