BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Lessons learned on cybersecurity project proposals for successful EU grant applications

Christine DEMETER, Ph.D.*
Dănuț MAFTEI, Ph.D.**

*National Cyber Security Directorate, Bucharest
e-mail: demeter.chris@gmail.com
**National Cyber Security Directorate, Bucharest
e-mail: dn.maftei@gmail.com

Abstract

This paper analyses the key aspects of successfully preparing cybersecurity project proposals to secure EU funding. It is structured around three major topics: (1) Global cybersecurity challenges, highlighting advanced cyber threats; (2) EU policies and funding mechanisms, analysing key regulations such as NIS2 Directive, the Cyber Resilience Act, and funding programs like Horizon Europe, Digital Europe, and CEF Digital, which support research, innovation, and digital security infrastructure; (3) Best practices for developing successful EU-funded projects, focusing on aligning proposals with EU priorities, building strong consortia, demonstrating impact, and avoiding common mistakes.

By integrating strategic alignment, policy frameworks, and effective project planning, this study provides actionable recommendations for governments, organizations, and cybersecurity professionals aiming to enhance digital resilience through EU-funded initiatives. The findings contribute to a better understanding of the complexities related to securing EU grants and developing sustainable cybersecurity solutions across Europe.

Keywords:

project proposal; strategies, regulations, policies, and legal framework on cyber issues; resilience; challenges; cyber security; risks; innovation; financing.

Article info

Received: 14 February 2025; Revised: 26 February 2025; Accepted: 12 March 2025; Available online: 2 April 2025

Citation: Demeter, C. și D. Maftei. 2025. "Lessons learned on cybersecurity project proposals for successful EU grant applications". *Bulletin of "Carol I" National Defence University*, 14(1): 136-153. https://doi.org/10.53477/2284-9378-25-09

As digital technologies become more and more deeply integrated into every segment of our society, cyber security is an increasingly critical concern worldwide, playing a central role in the smooth functioning of modern society.
In recent years, the European Union's (EU) increasing dependence on digital technologies has led to growing concerns about cyber security risks. Given the cyber challenges facing states, organizations, and citizens today, cyber security is no longer a matter of choice but a fundamental necessity to ensure the protection and resilience of EU societies and economies.

As a component of national security, the importance of cybersecurity cannot be underestimated (Romanian Government 2021). With the rapidly evolving digital landscape, a large number of states have become increasingly exposed to a wide range of cyber challenges targeting critical information infrastructures, disrupting key services and sectors such as finance, healthcare, transportation, energy, communication networks, and supply chains, all of which pose significant risks to national and international security, but also to economic, political, social stability, democracy and society at large. Such malicious activities can be used by state or non-state threat actors to conduct or support hybrid campaigns or activities specific to Foreign Intelligence Manipulation and Interference (FIMI).

Cyber resilience has become a cornerstone of the *EU Cyber Security Strategy for the Digital Decade* (European Commission 2020b). These are the EU's overarching cybersecurity objectives for critical information infrastructure and a secure digital future, with the European Union focusing on building a robust framework that can withstand and recover quickly from cyber incidents. Cyber resilience goes beyond simply preventing cyber attacks, as it involves preparing for potential disruptions, minimizing their impact, and restoring normal operations as quickly as possible.

Cyber issues and digital resilience are also key topics for the *EU's Union Security Strategy* (European Commission 2020a). The EU has prioritized the protection of its digital infrastructure (a critical area where cybersecurity plays a vital role), including energy networks, communications, supply chains, and financial systems, which are increasingly dependent on interconnected technologies.

Cyber security is essential for maintaining public trust in digital services and preventing unauthorized access to sensitive information. Privacy is another significant concern in the EU's cybersecurity framework. The European Union is a world leader in privacy protection, with a specific legal framework – the General Data Protection Regulation (GDPR) of 2016 (EUR-Lex 2016), which sets high standards for data security. The GDPR imposes strict rules for handling personal data, requiring organizations to implement robust cybersecurity measures to protect citizens' privacy. Breaching this law can lead to heavy fines and reputational damage. As more and more personal data is generated and stored digitally, ensuring the security of this data has become more important than ever.

It can be seen that the EU has put in place several strategies, regulations, policies, and legal frameworks to strengthen its cyber security. These focus on setting objectives to protect critical information infrastructures, create a secure digital space, strengthen cooperation between Member States, adopt stringent cybersecurity management standards in key sectors, or establish a framework for European cybersecurity certification schemes for ICT products, processes, and services. These efforts reflect the EU's commitment to building a united and secure digital ecosystem and further demonstrate the EU's proactive approach to cyber security.

In order to lay the foundations for a secure and prosperous digital future, in addition to existing cyber strategies, regulations, policies, and legal frameworks, submitting project proposals for EU grants can benefit **research, innovation, digital infrastructure development, capacity building in the cyber security sector, security of networks and information systems, international cooperation, exchange of information and experience, etc**.

Thus, the European Union has established several funding programs that align with its cybersecurity strategies, policies, and regulations to ensure a coordinated and strategic approach to cyber resilience, thus reinforcing the objectives outlined in the *EU Cybersecurity Strategy for the Digital Decade* and the *EU Strategy on the Security of the Union*.

Key funding instruments include the **Horizon Europe Programme** (European Commission 2021c), which prioritizes cybersecurity research and innovation, supporting projects that develop cutting-edge security technologies, and encouraging collaboration between academia, industry, and government agencies. Another important program, the **Digital Europe Programme** (European Commission 2021d), focuses on building digital capabilities, including cybersecurity resilience, through large-scale deployment projects and promoting digital skills training. In addition, the **Connecting Europe Facility - CEF Digital** (European Commission 2021a) is a key EU funding instrument to promote competitiveness, growth, and jobs through targeted infrastructure investments across the Union. It aims to stimulate public and private investment in digital connectivity infrastructures of common interest to the EU. In addition, the **EU Funding & Tenders Portal** (European Commission 2021b) is a key tool providing centralized and up-to-date information on available grants, eligibility requirements, and application procedures.

Developing and submitting a proposal for a cyber security grant project is a complex exercise that requires the strategic integration of European, national, and organizational priorities. Such alignment not only demonstrates the relevance of the project but also ensures that it responds to the real needs identified at all levels.
The current work will analyze the importance of cybersecurity proposals for ensuring the protection and resilience of EU societies and economies, as well as the key aspects of successfully developing cybersecurity project proposals for EU funding.

This research is relevant for national governments, the cybersecurity industry, academia, civil society, the legislature, as well as the EU institutions, as it identifies the specific challenges, lessons learned, best practices, success factors, and complexities involved in the successful development of EU cybersecurity project proposals.

The methodology used and research hypotheses

The study adopts an **analytical and exploratory** methodology, based on the following components: (1) **Desk review**: examining relevant EU directives and regulations, such as the NIS2 Directive, the Cyber Resilience Act, Horizon Europe, Digital Europe, and CEF Digital, which set the cybersecurity framework and requirements for obtaining EU funding; (2) **Benchmarking**: comparing EU strategies and policies with the requirements and challenges of funding applicants, to identify discrepancies and key success factors; (3) **Best practice review**: Identifying factors that have contributed to the success of previous project proposals in the field of cybersecurity and extracting lessons learned to optimize the application process; (4) **Actionable recommendations**: formulating concrete suggestions for effectively aligning projects with EU requirements, thus maximizing the chances of obtaining funding and successfully implementing cybersecurity projects.

The presented methodology provides a **practical and grounded insight** into the complexities of the funding application process, supporting stakeholders in improving their chances of success and contributing to the development of a robust framework for cybersecurity projects in Europe.

This article explores how cybersecurity projects can be optimized to obtain funding and contribute to the EU's digital resilience. The research aims to highlight the critical factors influencing the success of these initiatives, with a focus on compliance with European strategies and regulations, as well as the effectiveness of consortia and implementation mechanisms.

The study is based on the following research hypotheses:

1. Alignment with EU, national and organizational strategies, compliance with the legal framework, and prioritization of EU funding issues are key factors of the success of cybersecurity projects in obtaining funding and their contribution to strengthening digital resilience and critical information infrastructure protection;

2. A strategic and well-informed approach to cyber issues and project development ensures long-term sustainability and relevance;

3. Building strong consortia and demonstrating the impact of projects are key factors for the successful acceptance and implementation of cybersecurity project proposals.

Challenges related to cyber security, hybrid warfare, and FIMI around the world

According to the present research, the major challenges existing in the cyber security domain across the globe are currently related to:

- **The expanding range of IT devices, and the increasing sophistication of cyber attacks** (Spencer 2024), including state-sponsored, ransomware, phishing, advanced persistent threats, data breaches, terrorism, and cyber espionage attacks. They are harder to detect, harder to counter, increasing in frequency and sophistication. Such malicious activities can also be used by state or non-state threat actors to conduct or facilitate hybrid campaigns (European Union 2023) and specific FIMI activities.
- **FIMI**: One of its most damaging effects is the erosion of public trust in democracy and democratic institutions. At the same time, misinformation, fake news, and hate speech, including against ethnic, religious, and sexual minorities, widen social divisions in democratic states, lead to increased discrimination and violence, and fuel political and cultural polarization. Trust in institutions and traditional media is also being eroded, leading to increased scepticism and difficulties in distinguishing between real and false information (Maftei and Bogdan-Duica 2024).
- Malicious actors (especially non-state actors) **conduct hybrid warfare-specific operations**, including by exploiting vulnerabilities of social media platforms or using cyber-attacks, thus affecting children, girls, women, citizens, societies, economies, critical services, democracy, and national security (Maftei and Bogdan-Duica 2024). Researchers have observed the steady evolution of Russian information warfare doctrine, which has deep roots in Soviet practice (Giles 2016; Snegovaya 2015). Recent Russian military thinking emphasizes hybrid warfare as a new persistent reality, with the ”information sphere” and ”information warfare” as a critical battlespace.
- **Cybersecurity governance and coordination, appropriate strategies, policies, and legal frameworks on cyber issues are lacking or underdeveloped**. Several countries are faced with fragmented cybersecurity systems, where national efforts are not coordinated, and policies can differ widely. This can lead to ineffective responses against national and cross-border cyber threats, which requires better international cooperation and standardized approaches to cybersecurity.
- **Lack of implementation of national strategies, policies, and legal framework on cyber issues**. Although existing strategies, policies, and legal frameworks are well drafted, in some countries they are not properly implemented. The reasons could range from political interests to financial or human resources issues.
- **A low level of cybersecurity and cyberspace hygiene**.
- **Low level of cybersecurity education and culture and lack of adequate training** of network and information systems operators (Maftei 2024). Lack of

digital literacy and education on cyber issues leads to human errors that make IT systems and networks vulnerable (European Commission 2023).

- **Lack of qualified cybersecurity professionals**. The demand for qualified cyber experts outstrips the supply, making it difficult for organizations to effectively defend against attacks. This shortage of experts hinders the coagulation of a sufficiently qualified cyber security workforce (Maftei 2024). However, the EU is working hard to raise public and business awareness of cybersecurity risks and best practices. Educational programs and certifications are also being developed to close the cybersecurity skills gap in both EU institutions and private organizations.

- **Retention of human resources**. Governments, critical and important entities, or operators of critical information infrastructures face difficulties in retaining cybersecurity experts, who often leave the organization for better salaries. However, several states have identified ways to address such challenges. For example, in Romania, the National Cyber Security Directorate - DNSC - a specialized body of the central public administration, under the authority of the Government, responsible for ensuring the cyber security of national civilian cyberspace (DNSC 2022), has managed to multiply four (4) times the favourable conditions necessary for retaining cyber professionals within the organization: 1) by hiring the experts as contracted staff; 2) due to this type of contract, by allowing part-time work for other organizations (of course, the conflict of interest must be absent); 3) also, by allowing part-time work in externally funded cyber security projects; 4) by amending the legal framework necessary to increase the salaries of staff employed as cyber security experts.

- **Cyber resilience is often weak**, with some countries lacking the necessary cyber resilience capabilities. Cyber resilience refers to the ability to anticipate, respond and recover from cyber attacks. The ability to quickly restore operations after a cyber incident is critical to mitigating long-term damage and many states around the world have underdeveloped recovery plans or vulnerable cybersecurity infrastructures (CISCO 2025).

- **Privacy concerns** are a challenge as more and more personal and sensitive data is stored and shared digitally. Balancing the need for security with protecting citizens' privacy remains a delicate task, especially as laws and regulations such as the GDPR put pressure on organizations to comply with strict privacy standards.

- **National, regional, and international cooperation is not sufficiently developed**. Old mindsets and silo thinking (Gleeson 2013) still exist within some organizations. This has a particularly high negative impact on increasing trust between partners, the level of cooperation, information sharing and countering cyber incidents or other security challenges.

- **Public/private partnerships should be developed**. Only a few countries in the world could be presented as examples of this type of partnership. For example, in Romania, one of the five main objectives of the Cyber Security

Strategy for the period 2022-2027 is the *Pragmatic Public Private Partnership*. "A pragmatic public-private partnership between public authorities, private entities, academia, research and citizens is a necessity, given that cyber-attacks target a large number and broad spectrum of networks and information systems" (Romanian Government 2022). This demonstrates the government's focus on public/private partnerships.

- **Cyber incidents are underreported** by citizens, private businesses, critical information infrastructure operators, supply chain members or even state institutions, and the reasons can be different: lack of awareness or understanding; lack of clear regulations for incident reporting; fear of reputational damage; legal and financial consequences; fear of escalation of attacker threats; disruption of operations; government and regulatory pressure; internal divergences; cost and resource constraints, etc. (Maftei 2025). Improved cyber incident reporting enables governments to take informed, initiative-taking actions that protect national security, support economic stability, strengthen economic resilience, and contribute to the development of policies and regulations needed to improve cybersecurity in general.
- **Emerging trends in cybersecurity**. Today, there is an increasing use of artificial intelligence and machine learning both by cyber professionals seeking to identify and mitigate cyber threats faster and more effectively, and by malicious actors using increasingly complex techniques to carry out attacks. Such emerging technologies, including quantum computing, could rapidly change the cybersecurity landscape, and the EU must be ready for such advances (Apriorit 2025).

***

The aforementioned challenges highlight the need to adopt and implement comprehensive cybersecurity strategies, policies, legal frameworks, education, cooperation, and investments in both technology and human resources to address the growing cyber challenges. Given these challenges, cyber security is no longer an option but a fundamental necessity to ensure the protection and resilience of EU societies and economies.

Essential components of a cybersecurity project proposal for successful EU grants

Developing and submitting a proposal for a cyber security grant project is a complex exercise that requires the strategic integration of European, national, and organizational priorities. Such alignment not only demonstrates the relevance of the project, but also ensures that it responds to the real needs identified at all levels.

How can European, national, and organizational strategies be aligned?
One of the most important challenges is to demonstrate the alignment of the project proposal with the priorities set at European, national, and organizational levels. This requires a well-defined process based on thorough analysis, integration, and justification. Understanding the strategic context, making direct links between the project objectives and the proposed solutions, and justifying the intended impact are essential steps. These are only the first steps.

EU legal framework on cyber issues to consider...
The European Union has put in place several strategies, regulations, policies, and a legal framework to strengthen its cybersecurity. Thus, according to key documents such as the *EU Cybersecurity Strategy for the Digital Decade*, the EU considers cybersecurity as a major strategic priority. This document demonstrates the EU's proactive approach to cybersecurity and sets clear objectives for protecting critical information infrastructures, creating a secure digital space, and strengthening cooperation between Member States. These objectives are essential for any project that aims to contribute to strengthening the EU cyber security framework.

Another key document is the *NIS2 Directive (Network and Information Systems Directive*) (EUR-Lex 2022a), which sets stringent standards for cybersecurity management in key sectors such as health, transport and energy. Compliance with the requirements of the Directive is essential to demonstrate that the project aligns with European priorities. The NIS2 Directive is linked to the *Critical Entity Resilience Directive* (EUR-Lex 2022b).

Regulation 881/2019, known as *the EU Cybersecurity Act* (EUR-Lex 2019), strengthens the role of the European Union Agency for Cyber Security (ENISA 2025) and establishes a Cybersecurity Certification Framework for ICT products, services and processes. The Regulation also aims to ensure the smooth functioning of the internal market and to achieve a high level of cybersecurity, resilience, and trust within the EU. On the other hand, ENISA produces a large number of reports on EU projects and comprehensive analyses of the EU cybersecurity landscape.

The Regulation on Cyber Resilience - Regulation (EU) 2024/2847[1] (EUR-Lex 2024) provides EU-wide minimum cybersecurity standards for digital products and software connected to the internet, setting a high level of technological excellence. This regulation will improve the overall security of society, with increasingly secure electronic devices available on the market as designs with ICT components must clearly demonstrate how they meet or exceed the set standards.

[1] The Regulation is also known as the *Cyber Resilience Act*.

There are, of course, other sectoral directives and regulations that form part of the legal framework on cyber issues. All these, together with the new European Cyber Security Competence Center (ECCC 2025), the EU's innovation hub for advancing cybersecurity technologies, reflect the commitment of the EU and its Member States to build a united and secure digital ecosystem.

Alignment with national strategies...

At the national level, each EU Member State has its own cybersecurity strategy, adapting European priorities into measures specific to the national context. These strategies often emphasize CERT[2] capacity building and securing critical information infrastructures. At the same time, national recovery and resilience plans include strategic investments in digital transformation, creating opportunities for projects focused on building digital resilience.

A well-founded project should clearly demonstrate how it addresses the priorities outlined in these national strategies. For example, a project focused on securing the digital infrastructure of hospitals should align with national digital health strategies and specific measures specified in the implementing legislation of the NIS2 Directive and also with additional sector-specific measures.

[2] Computer Emergency Response Team.

Integrating organizational strategy...

In addition to being aligned with European and national priorities, the project proposal should also reflect the mission, vision and strategy of the organization developing it. This integration demonstrates that the project is not just a response to a funding application, but is part of a broader, well-articulated plan that reflects the values and strategic direction of the organization.

For example, if an organization's mission is *to increase the digital resilience of the public sector*, the proposal should outline how the proposed solutions contribute to this mission. Similarly, the organization's long-term vision, such as *becoming a regional leader in cybersecurity solutions*, should be supported by the project's ambitious goals.

A project aligned with the organization's strategy is more likely to benefit from its resources and expertise. For example, if the organization's strategy includes securing critical information infrastructures, the proposal should highlight its continuity with previous initiatives and demonstrate how it adds value. Such alignment can be argued through concrete examples of the organization's experience, such as the successful implementation of similar projects. This demonstrates a deep understanding of the domain and the ability to deliver tangible results.

... And the objectives of open calls – "call-fiche"

Another key aspect of developing a proposal is to explicitly align it with the objectives of the open calls for proposals. These calls set out specific priorities,

expected results and eligibility criteria that the proposal must address.
For example, if a funding request focuses on *increasing the digital resilience of critical information infrastructures*, the proposal must articulate how the proposed solution directly addresses this objective. This may include presenting a detailed technical solution that addresses the problems outlined in the request, demonstrating its alignment with strategic priorities such as interoperability, innovation, or sustainability, and defining clear performance indicators such as, for example, reducing response time to cyber incidents or improving data protection.
Open calls may also specify additional requirements, such as *cross-border collaboration or private-sector involvement*. The proposal should address these requirements explicitly, detailing how the project contributes to the objectives pursued.

Justifying the impact and establishing a solid implementation plan...
A well-structured proposal includes a clear section justifying the impact of the project, supported by measurable objectives and performance indicators. For example, a monitoring system that reduces the response time to cyber-attacks from 24 hours to 2 hours should be explicitly presented in the proposal. Such results can be backed up with relevant statistics and reports, such as those from ENISA.
The proposal should also contain a detailed implementation plan, including the resources available, the team involved and the project milestones. These elements create an overall picture that gives confidence to the evaluators.

Who said it was easy?
Developing a proposal for a cybersecurity project is an achievable process when it is approached systematically, following steps of thorough documentation, strategic alignment, and detailed justification. By integrating EU, national and organizational strategies, as well as the objectives of open calls for funding, the proposal proves its relevance, feasibility, and value. In this way, the proposed project becomes more than just an idea; it emerges as a solid solution that contributes to increasing cybersecurity resilience at all levels.

Challenges, lessons learned, good practices, and success factors for successful application to EU-funded cybersecurity programs

Applying for EU-funded cybersecurity programs can be a complex but rewarding process. Such activity presents several challenges, which can be both complex and time-consuming. Based on experiences from previous applications, some key challenges, lessons learned, and good practices related to funded programs dealing with cybersecurity have been revealed, such as:

Understanding program objectives, priorities, and requirements. Not all EU programs are similar. Each program has its own specific goals, objectives, and

priorities. Many applicants fail to align their project proposals with the main objectives of the program, leading to rejection. Please carefully read the call for proposals, work programs and any related documentation. The project must align perfectly with the objectives presented. Priority needs to be given to addressing EU-wide challenges such as critical infrastructure protection, cross-border cyber threats, or resilience to cyber attacks. It is particularly important that the technical, legal, and financial aspects required in proposals for EU-funded projects should be well understood and respected.

Focus on innovation and impact. EU funding tends to favour innovative, scalable, and impactful cybersecurity projects. Proposals with vague objectives or low impact often fail to stand out, with limited chances of winning. The project must provide a clear innovative solution to urgent cyber security challenges. Measurable results such as strengthening cyber security capabilities, improving threat detection, or developing cross-border collaboration need to be demonstrated.

Strict compliance with EU policies and the legal framework to be followed (regulations, financial management directives, eligibility criteria, funding limits, evaluation criteria, reporting, data protection, state aid law, sustainability objectives and any other sector specific legal requirements). Applicants must ensure compliance with these rules and failure to do so may lead to disqualification of the project or rejection of funding. This can be particularly difficult for organizations that are unfamiliar with specific EU rules or that operate in multiple jurisdictions.
Applicants should invest time and effort to understand the policies and legal framework relevant to the projects. In parallel, it is essential to involve legal or financial experts who are familiar with EU compliance and funding requirements.

Highly competitive environment. Many EU funding programs, particularly in the area of cybersecurity, are highly competitive because of the fairly large number of applicants and the low proportion of proposals that could receive funding. A strong record in cybersecurity or EU-funded projects, development of a highly innovative and impactful project that directly addresses EU cybersecurity priorities, strong partnerships and clear alignment with EU objectives can significantly increase the chances of success.

Complex application processes and procedures. The application process for EU-funded programs is often complex and requires extensive documentation. It involves several steps (proposal writing, budgeting, partner agreements, compliance checks, etc.). The complexity of the application may be a barrier for smaller organizations or those with limited experience in EU funding. Incomplete or inaccurate proposals may result in disqualification. This is why applicants should devote sufficient time and resources to understand the requirements of the application and to ensure that all conditions are correctly fulfilled. Career guidance or consultants can also be helpful.

Difficulty in creating the right consortium. Collaboration is often key to the success of proposals. Many EU-funded cybersecurity programs require the involvement of multiple partners, including government bodies, research entities, academia, private companies, and NGOs. Weak or insufficient partnerships can lead to the failure of a funding application. Identifying suitable, reliable partners to commit to the project can be a challenge and an incomplete or weak consortium can undermine the quality and chances of the proposal, making it difficult to meet the program requirements. In addition, inter-partner dynamics, different organizational cultures and unclear roles can affect project implementation. Experts with complementary skills should be recruited and all partners must be fully engaged and contribute equally to the project. Establishing a strong consortium requires careful planning, and clear and transparent communication from the outset about roles and responsibilities is essential. On the other hand, applicants should partner with trusted organizations that bring complementary skills and resources. It is clear that the EU's international initiatives in the field of cybersecurity should be further explored, including cooperation with NATO, the UN, and non-EU states in addressing global cyber threats.

Budgeting and financial planning. Poorly prepared financial plans, unrealistic budgets or administrative errors are often found in submitted proposals. Insufficient clarity or transparency can also lead to doubts about project feasibility. Projects have to adhere to specific rules on eligible costs, co-financing and reporting requirements, and there is often a detailed breakdown of how the funds will be allocated. A lack of clarity or inaccurate financial planning may lead to the rejection of the proposal. In addition, financial complexity may discourage small businesses or research institutions without in-house financial expertise. Applicants should carefully follow the program's financial guidelines. A detailed and realistic budget and transparency in the allocation of funds are essential. Consultation with financial experts can ensure compliance with EU rules. Applicants must be clear about how the funds will be allocated and ensure compliance with EU financial rules. It is also necessary that the programme guidelines are followed and that the administrative documents are complete and accurate.

Risk of blocking activities and limited reporting. After receiving funding, beneficiaries must report regularly on progress, results, and financial management. This can be time-consuming and failure to comply with reporting requirements can lead to sanctions or loss of funds. Applicants may underestimate the effort required for post-grant activities (e.g. progress monitoring and reporting), which may result in delays, mismanagement or even project failure.
In order to avoid such problems and to ensure good project management, applicants should prepare a robust monitoring and evaluation framework to track project milestones, outputs and expenditure incurred, as well as allocate the necessary resources for regular reporting and internal audits.

Risk management. Cybersecurity projects face numerous risks, including delays, technical challenges, and potential collaborative failures. Underestimating risks or providing weak mitigation strategies can lead to poor evaluation scores. A comprehensive risk management plan outlining potential risks (technical, financial, operational) and mitigation strategies should be developed. Being proactive in addressing risks increases confidence in project execution.

Holding discussions with EU officials and other entities involved. Many applicants fail to make timely contact with EU officials or other involved entities with an important role in cybersecurity. This may limit the understanding of the program priorities, leading to poorly aligned proposals. Active participation in information days, networking events and webinars organized by the EU or funding bodies could be a huge asset. In the meantime, engagement with relevant stakeholders and officials early in the process to clarify any questions and refine the project, as well as getting feedback from EU bodies, is important.

Sustainability. To be successful, projects need to consider long-term sustainability, as EU funds are interested in supporting projects that have a lasting impact beyond the funding period. Applicants need to clearly articulate how the project will be sustained beyond the end of funding, conditions which would require establishing self-financing models, partnerships with industry actors or ensuring that the results will be adopted by end-users, including government bodies, businesses, and the public sector.

Communication and reporting. To avoid creating confusion and undermining confidence in the project, a transparent, clear, and concise communication plan should be developed, including measurable results, timelines, and regular reporting. All stakeholders should be kept regularly informed of project developments.

Long and uncertain deadlines. Applications for EU funding usually involve long preparation times and a delayed funding approval process. The assessment, selection and funding agreement phases can take months or even longer. Prolonged timelines can create uncertainty for organizations, especially if they need immediate funding to start cybersecurity projects. Delays in receiving funding can also affect the project implementation timetable. Applicants should plan ahead and be prepared for possible delays. It is useful to have alternative funding sources or backup measures in place to fill gaps during waiting periods.

Managing cross-border collaboration. Many EU cybersecurity programs involve international collaboration, which means different partners in different EU Member States need to work together. Cultural differences, different regulatory environments and different legal systems can complicate the coordination process. Managing a multinational project requires effective communication, understanding of different laws and a harmonized approach to project objectives. These challenges can lead to misunderstandings, delays, or inefficiencies.

Clear governance structures, well-defined roles and regular communication are essential for successful international collaborations. It is important that all partners understand the project objectives and are committed to the common vision.

Limited knowledge of cybersecurity needs. Applicants may have difficulties in fully understanding or addressing the specific cybersecurity challenges highlighted by the EU. As the cybersecurity landscape is constantly evolving, it is essential to be well versed in new types of threats, trends and emerging technologies through briefings and consultation of EU publications, research papers, as well as participation in relevant EU events addressing cybersecurity issues. The project proposal should also be aligned with the latest EU cyber security strategies.
Proposals that do not adequately address current or future threats to cybersecurity are unlikely to be accepted. In addition, misalignment of the project with EU priorities or failure to demonstrate the relevance of the project to the European cybersecurity agenda may affect the application.

Lack of post-project sustainability. EU funding often requires projects to demonstrate how the results will be sustained and scaled up after the end of the funding period. Many applicants strive to provide a clear roadmap for the long-term sustainability of their projects, as those who fail to demonstrate clear sustainability after the EU funding period risk being rejected. Funders want to ensure that projects create a lasting impact and do not rely solely on continued EU funding. A sustainability plan should be developed outlining how the project will continue to operate, whether through commercialization, government support, industry partnerships or other means.

Intellectual property and data sharing. In EU-funded collaborative projects, intellectual property and data-sharing issues can be controversial. Some rights disputes may also arise, especially when partners have different national or institutional policies. To avoid friction between partners, delayed projects, legal problems or funding sanctions, attention should be paid to the mismanagement of intellectual property and non-compliance with data protection legislation. Intellectual property, data-sharing agreements and confidentiality clauses should be defined in advance. All partners need to be aligned on these issues and comply with EU data protection and intellectual property legislation.
Preparing applications in advance. As the proposal development process often requires significant time and effort, work should start early, allowing time for drafting, review, refinement, and revisions.

***

By applying these best practices and learning from previous experiences, organizations can increase their chances of success when applying for EU-funded cybersecurity programmes.

Conclusion

Looking ahead, it can be concluded that the continued evolution of cyber threats and the increasing dependence on digital technologies require sustained investment, innovation, research, and development of digital infrastructure while increasing the level of security of networks and information systems, capacity building in the cyber security sector, exchange of information and experience, and better collaboration in the field of cyber security. Strengthening international cooperation, fostering public-private partnerships and improving cyber security education will also be essential to ensure a secure digital future in the EU and the world, to ensure the protection of privacy, the resilience of EU societies and economies, stability, national and international security, the security of critical information infrastructure assets, as well as democracy and the functioning of democratic institutions.
This paper has analysed the importance of cyber security project proposals for ensuring the protection and resilience of EU societies and economies.

The scientific research, based on an analytical and exploratory methodology, validates the research hypotheses and confirms that the success of cybersecurity project proposals is conditioned by their alignment with EU strategies, compliance with the legal framework and effective integration of European funding requirements. The literature review of relevant directives and regulations, such as the NIS2 Directive, the Cyber Resilience Act and the Horizon Europe, Digital Europe and CEF Digital funding programs, highlights the importance of projects' compliance with the objectives set by the European Union for cybersecurity and digital resilience.

Comparing EU strategies and policies with the needs and challenges of applicants reveals that differences between European requirements and the ability of organizations to meet them can influence the chances of success of proposals. Thus, strategic and documented alignment of projects not only demonstrates their relevance but also ensures better integration into the European digital security ecosystem. The research also confirms that a systematic approach to project development, including a clear justification of their impact and long-term sustainability, is essential for the success of applicants.

Analysis of good practice from previous successful proposals shows that a key determinant is the formation of strong, interdisciplinary, and international consortia, where partnerships between government institutions, private companies and academic entities contribute to increasing innovation capacity and demonstrating project impact. In this context, impact assessment and the definition of measurable objectives are critical to validate the relevance of proposals.

Research also underlines the importance of effective risk management and compliance with EU requirements. The implementation of a detailed risk management plan, including clear mitigation strategies and robust monitoring

mechanisms, contributes to optimizing the implementation process and avoiding administrative obstacles. Therefore, projects that demonstrate rigorous planning, clear integration into EU strategies and a sustainable approach are the most likely to get funding and contribute to strengthening the EU's digital resilience.
By recognizing and proactively addressing the challenges identified, while applying the good practices presented and learning from past experiences, applicants/ stakeholders can increase their chances of success in securing EU funding when applying for cyber security programmes.

Identifying the strategies and key components of successful proposals, examining best practices, relevant case studies and lessons learned from previous EU cybersecurity proposals could be vital factors for writing effective applications.

The current scientific research contributes to a better understanding of the specific complexities of obtaining EU grants and developing sustainable cybersecurity solutions in the EU and EU Member States and could have a direct impact on EU policies on cybersecurity project proposals or the effectiveness of specific funding programs.
The study is of importance for national governments, the cyber security industry, academia, civil society, legislators, and the EU institutions as it identifies the specific challenges, lessons learned, best practices, success factors and difficulties in preparing successful cyber security project proposals within the European Union.

At the same time, this work may be of relevance to cybersecurity professionals, organizations, and policymakers in the EU. The material also provides concrete recommendations for organizations wishing to submit successful cybersecurity project proposals in the EU context.

References

Apriorit. 2025. "CyberSecurity Trends in Information Technology and Emerging Future Threats." doi:10.6084/m9.figshare.16937014.

CISCO. 2025. "What Is Cyber Resilience?" https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html.

DNSC. 2022. „Lege nr. 366 din 19 decembrie 2022." https://legislatie.just.ro/Public/DetaliiDocumentAfis/262941.

ECCC. 2025. "European Cybersecurity Competence Network and Centre." https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre.

EEAS. 2024. "Tackling Disinformation, Foreign Information Manipulation & Interference." https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

ENISA. 2025. "ENISA." https://www.enisa.europa.eu/.

EUR-Lex. 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data." https://eur-lex.europa.eu/eli/reg/2016/679/oj.

—. 2019. "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA." https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

—. 2022a. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

—. 2022b. "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC." https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

—. 2024. "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements." https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

European Commission. 2020a. "COM(2020) 605 final." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605.

—. 2020b. "The Cybersecurity Strategy." https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

—. 2021a. "Connecting Europe Facility." https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en.

—. 2021b. "EU Funding & Tenders Portal." Editor European Commission. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

—. 2021c. "Horizon Europe." https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.

—. 2021d. "The Digital Europe Programme." https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

—. 2023. "Cyber Skills Academy." https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy.

European Union, General Secretariat of the Council. 2023. "Revised Implementing Guidelines of the Cyber Diplomacy Toolbox no. 10289/23." https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

Giles, Keir. 2016. "Handbook of Russian Information Warfare." https://www.ndc.nato.int/news/news.php?icode=995.

Gleeson, Brent. 2013. "The Silo Mentality: How To Break Down The Barriers." https://www.forbes.com/sites/brentgleeson/2013/10/02/the-silo-mentality-how-to-break-down-the-barriers/.

Maftei, Dănuț. 2024. "The Cyber Competences Act – a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union." *Informatica Economică* 45-60. doi:10.24818/issn14531305/28.2.2024.04.

—. 2025. "LinkedIn post." https://www.linkedin.com/posts/danut-maftei-phd-39418a68_cyberincidents-criticalinformationinfrastructure-activity-7291046307190759424-LL9w?utm_source=share&utm_medium=member_desktop.

Maftei, Dănuț și Lorin Nicolae Bogdan-Duica. 2024. "Risks, threats, and vulnerabilities related to social media platforms and search engines. Regulations and national legal frameworks." *Bulletin of "Carol I" National Defence University* ("Carol I" National Defence University Publishing House) 13 (4): 249–265. doi:https://doi.org/10.53477/2284-9378-24-62.

Romanian Government. 2021. „Ordonanță de urgență nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică." https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652.

—. 2022. „Strategia de Securitate Cibernetică a României, pentru perioada 2022-2027." https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf.

Snegovaya, Maria. 2015. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare, Institute for the Study of War." https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Spencer, Patrick. 2024. "2024 Cybersecurity and Compliance Landscape: 50 Critical Statistics Shaping Our Digital Future." https://www.kiteworks.com/cybersecurity-risk-management/2024-cybersecurity-landscape-50-critical-statistics/.