A GRANTS OFFICE PUBLICATION

FUNDED EUROPE

DEC 2022 | VOLUME 2 | ISSUE 4

Zero-Knowledge Proof: The next big thing they are not funding yet.

In This Issue

Dear Readers

Russia's invasion of Ukraine in February illuminated the place of security at the top of the European political and economic agenda. It is not only the vexed question of military defence in the union, but also ongoing debates across the broader region concerning energy, data and economic security, that have been reoriented by the conflict.

Our winter issue of Funded Europe takes the multivalence and complexity of security as its primary theme, exploring different forms of security with a particular emphasis on cybersecurity in our new digital era. At the centre of the EU's much vaunted (and ongoing) digital transition is a serious concern about data security and personal privacy in the age of the internet. In fact, cybersecurity is an increasingly complex topic of interest for grant funders and innovators across the continent at the national and regional levels as well.

As Marie-Christine Noujaim shows in her article on the state of cybersecurity in the French public sector, "From reactiveness to proactiveness: What are the lessons learned from the recent cyber-attacks in France?", concerns about cybersecurity are not themselves new. However, increasing numbers of sophisticated cyber-attacks, as well recent global events—especially the COVID-19 pandemic—have seriously aggravated the problem. By contrast, in our cover issue, Gregory Clare focuses on a possible solution to certain kind of cyber problem—zero-knowledge proofs—that we may well start seeing integrated regularly into the kinds of innovation projects targeted by programmes like Digital Europe. Meanwhile, Adele Lebano tackles some of the political-philosophical questions, at the core of the Italian cybersecurity strategy, concerning the relationship between freedom and security raised by recent efforts to address cyber threats. Adding to these articles focusing on digital security, Charlotte von der Brelie examines the recent change in rhetoric concerning the European Defence Fund stimulated by the war in Ukraine and explores how the Fund is working in practice.

As always, our objective is to provide a broad context to the various grant funding programmes open across Europe, and in this case the security-relevant programmes discussed include Horizon Europe, Digital Europe, the Recovery and Resilience Facility as it pertains to Ireland and many more!

Kind regards,

William Bond & Adele Lebano
Editors

GRANTS OFFICE EUROPE IS NOW ON TWITTER AND LINKEDIN!

Grants Office has built a leading reputation in grants intelligence in the United States. Over the past year, we have taken that expertise internationally. With the help of our team of locals and native speakers, we recognise that the European cultural, legal, and economic context shapes policies related to funding and creates a particularly European grant landscape. To that end, we offer our clients and partners tailor-made grant education and intelligence, such as you find here, in our quarterly magazine Funded, and ongoingly on our social media platforms.

Give us a follow on Twitter & LinkedIn to find the latest in European funding as well as information on webinars, and more.

Security as freedom: The Italian Strategy for National Security in the digital era

Adele Lebano

SECURITY AND FREEDOM: FRIENDS OR FOES?

At first glance, security and freedom share an antagonistic relationship. The more security, or securitization, the less freedom. It suffices to think about what happened to the average individual's experience after 9/11: we were no longer free to walk to plane gates with friends; we became used to the ubiquity of security cameras in city streets. Even more simply, it suffices to think about what it means for a child to be told that jumping is not safe, or for a teenager that they should be watched and accompanied when walking down the road. They will move less freely in the world and trust their senses and judgment less, while their confidence and trust will be diminished in exchange for safety. Security and freedom have also come to dominate public health debates. Since the dramatic onset of the Covid-19 pandemic in 2020, the tension between security and freedom has been weaponized against scientific evidence and public health policies by an array of public intellectuals, social media influencers, politicians, and citizens all over the world.

Giving up some freedom in exchange for security is at the root of most social interactions, and of our basic survival strategy. As political thinkers of the social contract tradition put it, it is at the origin of any social and political edifice. To be together as citizens is to be less free. Or, rather, it is to be free in a different way. It is in fact to possess a superior kind of freedom, as Rousseau argued while he himself remained conflicted about whether the initial loss was worthwhile. The Hobbesian version of the freedom-security tale relies on the role of a single powerful political actor who, by social contract, demands the submission of everyone in exchange for the protection of all. In this bargain, the citizens' power to defend themselves from the Leviathan—the despot himself—is curtailed. The promise of welfare and stability trumps freedom and agency.

Yet there is another, more nuanced, side to the relationship between security and freedom. Security also means protecting the privacy of individuals from external, unwanted interference (including those of the Leviathan). Some of these external interventions in our life we may be aware of and reject, and some we may unwillingly resign ourselves to. But, sometimes, we are subjects of interference and violation of privacy without our knowing. This happens more often now today in our digitally connected lives, in which every act of data-sharing exposes each of us to the possibility that information will be intercepted, and our privacy will be infringed. This, in my view, is the most relevant side of the security and freedom story in the digital era.

THE ITALIAN STRATEGY FOR NATIONAL SECURITY: 2007, 2017, AND 2022-2026

"Security is Freedom", Sicurezza è Libertà, was the title of a publication and the essence of the address of the Italian Prime Minister Paolo Gentiloni on the occasion of the 10th anniversary of the new National Security Strategy in 2017. In his speech Gentiloni invited Italy to keep striving simultaneously to protect security and freedom, security and privacy, secrecy and transparency, without being tempted by what he called 'shortcuts that are deceptive and dangerous'. The reasons he gave for this commitment are as follows (the text here is translated almost verbatim): 'It is not by compressing citizens' freedom that we can effectively fight against terrorism; it is not by sacrificing personal data protection that one can achieve cybersecurity; it is not with secrecy for its own sake that Information Services can protect national interests'. The country should strive for its citizens to be 'aware and digital', which is to move freely and without being conditioned; free to choose their life and future, as J.S. Mill, another famous political theorist, said.

THE CURRENT 2022-2026 ITALIAN STRATEGY FOR NATIONAL CYBERSECURITY

(https://www.acn.gov.it/strategia-nazionale-cybersicurezza) is consistent with this general approach to security and freedom. Its priorities are incorporated among the goals of the Recovery and Resilience Plan. In summary, cybersecurity in the Italian framework must meet the following challenges:

- enabling the access of citizens to digitalized public administration services
- fighting misinformation and building awareness to protect citizens' fundamental freedoms
- anticipating dangers
- coping with crises by recovering quickly through the coordinated efforts of public and private actors
- achieving national and European autonomy in the digital sphere to maintain control over the data stored, produced, and shared through digital technologies.

Each of these challenges, some more than others, results from the tension between freedom and security and from the attempt to meet their demands simultaneously.

In order to meet these challenges, the Italian Recovery and Resilience Plan is investing EUR 623 million to 'strengthen the national digital ecosystem by means of auditing services and managing of cyber threats.' These investments are linked to those in digital infrastructure (EUR 900 million), migration to cloud for the Italian public services (EUR 1 billion), and data and interoperability (including a single digital gateway for public services) (EUR 646 million).

The new Agency for National Cybersecurity (ANC) has published 5 calls in 2022 that focus on developing skills and infrastructure in the Italian PA to increase security and protect freedom and privacy of citizens. The first 4 calls, the latest of which closed in mid-October, aimed to increase cyber-resilience of local public administration by providing financial support to Italian Regions, autonomous Provinces, and local metropolitan cities. A 5th call closed on 30th November 2022. This is a formula grant that provides financial support to public administrations, public entities, and private subjects that want to open testing labs for software and network evaluation and certification.

SECURITY AND FREEDOM: LESSONS FROM POLITICAL THEORY AND POLICY MAKING AND FUNDING SCHEMES

Gentiloni quotes mid- 19th-century liberal thinker J.S. Mill, and I would like to recall the idea of another liberal master, and one closer in time, Isaiah Berlin, political thinker of the 20th-century liberal tradition. Berlin thought that freedom can be conceptualized in two main ways: as the state of not being interfered with (the 'freedom from,' the so-called negative freedom) and as freedom to be and to do (the 'freedom to', the so-called positive freedom). The first is a more minimal notion that protects the space around people, it is the freedom of civil liberty and of privacy, that expects state power to step back, unless that power is used to defend the negative freedom of others. The second is freedom as autonomy and self-mastery, the freedom of social rights and welfare, which relies on a central power as enabler for each and everybody, of what can or cannot be achieved. Each of these versions of freedom and of security—the first one in my view more relevant to the discussion on cybersecurity—asks difficult questions for the making of policies and the funding of innovation.

CONCLUSIONS

How can one enhance security while building confidence and trust and protecting freedom?

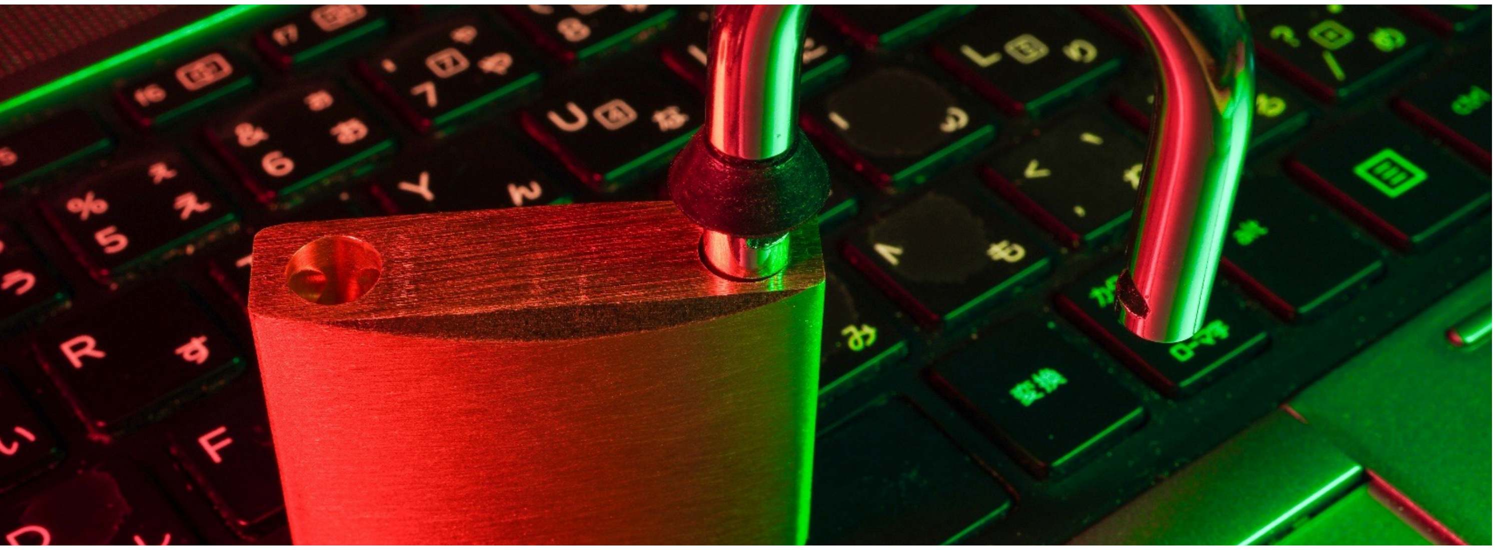
Trust is the confidence that what is put in front of us is safe and in our interest. But trust is also what exposes people to risks. Trust is reassuring, makes us feel safe. We feel we do not always need to pay attention—we do not need to protect ourselves from enemies or threats. Trust means we are not in a constant state of vigilance, as in the Hobbesian state of nature. And yet the buzz-word we hear most often when discussing cybersecurity is 'zero-trust'. This may be a reminder that also for IT developers, policy makers and funding agencies—in the continuum between freedom and security—we are to hold the first, freedom, dearest in order to achieve the second.

ABOUT THE AUTHOR

Adele Lebano is Grants Development Consultant for Italy at Grants Office Europe. She has gained a rich experience through her former positions in academia, business, and the public sector across a variety of European countries and the United States. Evident throughout her writing and consulting are her passion for rigorous research, effective communication, as well as her commitment to freedom, equality, and inclusion.

From reactiveness to proactiveness: What are the lessons learned from the recent cyber-attacks in France?

Marie-Christine Noujaim



Twenty years ago, we thought that, in 2022, we were going to live in an ultramodern, futuristic and revolutionary era. Instead, we are still here fighting with each other over scarce resources, worrying about whether or not we will find fuel for our cars or to heat our homes in the winter, and simply worrying about the chaotic world we are leaving to our children in which health, economic, and social crises, not to mention wars, seem never-ending. Perhaps, the only "virtual" reality which was loyal to our futuristic dreams is that of cyber space. As Mary Aiken puts it, "'Cyber' refers to anything involving computers or computer networks, such as the Internet." Unfortunately, this world too is not free of dangers. In fact, the Covid-19 crisis has brought the challenges and risks related to our increasing dependence on digital technologies into even starker relief as businesses, services, and education suddenly had to shift to connectivity and cloud solutions in order to enable remote working, distance learning, and even access to critical healthcare services. With this shift, unsurprisingly, came increased vulnerability and an intensification of incidents of fraud, data theft, ransomware attacks, hacking, and phishing.

Europe was hit particularly hard by cyberattacks. A 2022 Statista Research Department survey among professionals responsible for their company's cyber security strategy in the United States and Europe found that the Netherlands saw the highest share of cyber-attacks among the examined countries (57 percent). French companies ranked second by the share of reported cyber-attacks (52 percent). A 2022 report by CyberEdge Group, which includes responses from information security professionals in various regions across the globe, found that 89.3 percent of French organizations experienced a successful cyber-attack within a 12-month period. In Q1 2022, French public administrations were the second-highest sector in the country affected by cyberattacks. While the United States took the top position with the largest number of attacks on public administrations with 13 major attacks, France was just behind with 9 cyberattacks. The report mentions that public administration was the hardest hit industry in 2021, with 137 major cyberattacks. The healthcare industry was concerned with 131 attacks, with France taking its share with 14 attacks on local hospitals (O'Driscoll, 2022). In fact, in 2021, the French National Agency for the Security of Information Systems (ANSSI) reported that, on average, one cyber-attack was happening per week in a hospital in France! Moreover, half of French companies have experienced at least one cyber-attack in 2021, according to the French Club of Experts in Information and Digital Security (CESIN), in the last edition of its annual barometer of cybersecurity in companies. And just as in 2020, half of the French companies surveyed said they were worried about their ability to cope with cyber risks.

Amidst this series of seemingly unstoppable and severe cyberattacks, the French national cyber strategy, which is now part of the France 2030 investment plan, was launched on 18 February 2021. The main ambition of this national acceleration strategy for cybersecurity is to triple the turnover of the cyber sector and create 37,000 cybersecurity jobs by 2025, with a plan worth more than one billion euros. The strategy is based on 4 axes: (1) developing sovereign and innovative cybersecurity solutions, (2) strengthening the links and synergies between the players in the sector, (3) supporting demand (individuals, companies, local authorities and the State), in particular, by raising awareness of cybersecurity among the French, while (4) promoting national offers to train more young people and professionals in the cybersecurity professions. Important and concrete actions have been launched thanks to this strategy, among which are:

THE FOSTERING OF THE COLLABORATION BETWEEN CYBERSECURITY ACTORS AND ECOSYSTEM VIA THE CYBER CAMPUS

On 15 February 2022, the Cyber Campus was inaugurated in France. It is currently the leader of France's cyber policy and the embodiment of French policy in the field of cybersecurity. The Campus brings together more than 160 national and international players in digital security, i.e., 1,800 experts. Headed by Michel Van Den Berghe, the Campus is promoting research and development projects as well as the emergence of tomorrow's cyber unicorns, i.e., start-ups valued at more than one billion dollars. This campus is hosting and promoting collaboration between companies and State service operators. The aim of this joint collaboration is to reverse the balance of power with cyber-criminals. A place for experimentation and sharing, the Campus is strongly supported by the cyber acceleration strategy, with nearly 100 million euros of direct and indirect funding.

SUPPORT FOR CYBER INNOVATION VIA:

The creation of calls for projects to develop the French cybersecurity sector

Funded to the amount of 150 million euros by France's 2030 plan, the 3 following calls for projects have already been launched:

Call for Projects	Objective
Supporting the development of innovative and critical cybersecurity technologies	This call aims to support the development of innovative and critical cybersecurity technologies, such as detection of cyberattacks or encryption solutions. It is part of the 1st axis of the national cybersecurity acceleration strategy. This call was opened until 15 October 2021. The target audience included both single companies and industrial or collaborative consortia (i.e., involving research laboratories).
Pooling cybersecurity data	This call aims to support the pooling of cybersecurity data between the various players in the sector in order to develop knowledge of threats. It is part of the 2nd axis of the national cybersecurity acceleration strategy. It was opened until 16 November 2021. Industrial or collaborative consortia providing both diverse data and advanced processing capacity were able to benefit from this call.
Supporting innovative projects on the Cyber Campus	This call aims to support innovative projects on the Cyber Campus. It is in line with the 1st and 2nd axes of the national cybersecurity acceleration strategy. Applications were able to be sent by 29 October 2021. The target audience included both single companies and industrial or collaborative consortia that are members of the Cyber Campus.

Source: Press release - Cybersecurity: The Government launches three calls for projects to support the development of innovative cybersecurity solutions

The creation of the cyber booster start-up studio:

Numerous actions to support entrepreneurship have also been set up, such as the cyber booster start-up studio, funded by the Future Investments Program PIA4. The cyber booster start-up studio scheme, which is unique in Europe, supports the creation and start-up of companies in the field of cybersecurity. 3 start-ups have already been incubated and nearly 50 applications are currently being examined.

The actions that leverage the full potential of research:

The national cybersecurity acceleration strategy also aims to support research. To this end, a €65 million priority research equipment programme (PEPR) is underway. This programme should make it possible to leverage the strong research and growth potential of the French cybersecurity industry. To support and promote the transfer of skills and technologies from public research, a transfer programme on the Cyber Campus, operated by the French National Institute for Research in Digital Science and Technology (INRIA), will specifically focus on identifying and implementing high value-added research and development projects.

THE STRENGTHENING OF THE CYBERSECURITY OF ADMINISTRATIONS AND LOCAL AUTHORITIES

The cybersecurity component of the France Relance plan, mobilising €136 million under the guidance of the National Agency for Information Systems Security (ANSSI), is intended to significantly raise the level of the digital security of the state and public services. This scheme is aimed primarily at local authorities and entities involved in the daily life of French citizens. Nearly 600 beneficiaries have already been selected. Within this framework, the Computer Security Incident Response Teams (CSIRT), which are alert and reaction centres for computer attacks intended for companies or administrations in several regions, namely Bourgogne Franche-Comté, Centre-Val-de-Loire, Corsica, Grand-Est, Normandy, Nouvelle Aquitaine and Provence-Alpes-Côte-d'Azur regions, took part in the 4-month incubation programme that was set up by ANSSI in February 2022. This incubation programme should enable regional CSIRTs to be rapidly operational in order to respond in a relevant and efficient manner to identified needs, while fully integrating into the territorial and national cybersecurity ecosystem.

THE TRAINING OF THE CYBER TALENTS OF TOMORROW

The objective of this measure is to create 37,000 jobs in the cybersecurity sector, and it will only be achieved if significant training resources are deployed. Around 9,250 students will be trained to become specialists in the field at all levels from baccalaureate +2 to baccalaureate +8. Research is also to be supported through the funding of 100 doctoral theses.

Since the Covid-19 pandemic, our increasing dependence on digital services and new technological developments, such as the proliferation of interconnected devices (IoT) or of the Cloud, has brought the importance of cybersecurity to the fore. Over the past few years, France has turned its attention to this increasingly strategic issue. In response to the numerous cyberattacks, the French Government is supporting its cybersecurity objectives through substantial funding across various national and regional funding programs in order to support the development of innovative cybersecurity solutions and their upscaling, the improvement of digital skills via cybersecurity capacity-building activities, and the implementation of cyber solutions. "Digital technology brings hope and a future, but it also brings threats. In the face of these threats, the state is raising its shields to protect its citizens, its businesses and its public services," according to the Economy Minister, Bruno Le Maire, speaking at the opening of the Cyber Campus. Indeed, as cybersecurity capacity is built, the time required for response and recovery from attacks should be getting shorter; additionally, with improvements in the direction of proactiveness, as well as prevention and prediction, resilience towards cybercrime could be seriously enhanced in France.

Once again, it remains challenging to determine whether the French historical cybersecurity ambitions would succeed amidst the manifold crises that punctuate our post-Covid world, including the ongoing Russian-Ukrainian conflict. Due to the multiplicity and seriousness of the cybersecurity problems that France is facing today, re-evaluating and adapting its national cybersecurity acceleration strategy, could be necessary in order to try to fight, fundamentally and structurally, against cybercrimes, and perhaps succeed in eradicating them one day. The Covid-19 health crisis highlighted the importance of prevention rather than cure. This paradigm could be also applied to cybersecurity: proactive prevention is key!

ABOUT THE AUTHOR

Marie-Christine Noujaim is the Lead Grants Development Consultant for France at Grants Office Europe. She graduated with a Bachelor's degree in Management in 2013. In 2016, she received her Master of Research in Management. From 2017 to 2021, she was enrolled in a PhD program at Université Bourgogne-Franche-Comté; her thesis was entitled "The practice of diversity in companies: a quest for efficiency or legitimacy?" She has participated in several EU-funded projects and has spoken at various international webinars, including the TandEM webinar "Empowering Youth as agents of integration and social cohesion" and the Grants Office Europe webinar on the key measures of the French recovery plan.

LinkedIn Profile

EU Programme Snapshot - Private Sector

Satellite Connectivity for Autonomous Land Vehicles Safety

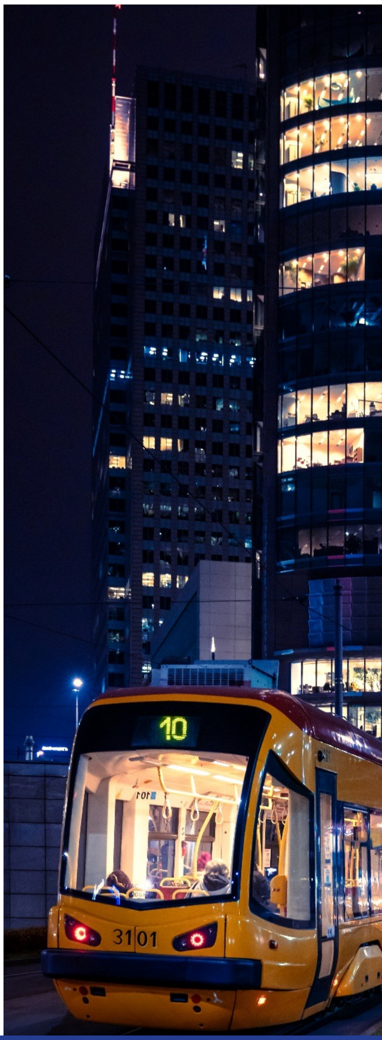
SUMMARY

The goal of this programme from the European Space Agency (ESA) is to fund innovation demonstration projects that make use of satellite connectivity technology within the Connected Autonomous Vehicles (CAVs) sector. The programme is designed to be open to a range of applications including, but not limited to, projects focusing on the following:

- Connected car performance parameters collection and processing
- Seamless transition between 4G/5G and satellite communication
- Commercial Fleet management and logistics
- IoT for connected devices on field monitoring and connected vehicles
- Real-time hazard warning.
- Hazard information collection and sharing
- High Definition map updates

As with all ESA programmes, projects must involve the innovative use of space assets, such as Satellite Communications (SatCom), Satellite Earth Observation (SatEO), or Satellite Navigation (SatNav).

Projects will receive, at maximum, 80% of the project costs—up to €200,000.



The ESA is looking for innovation in public transportation as well as private vehicles.

ELIGIBILITY

Businesses of any size within ESA member states, associated to the ESA's Business Applications and Space Solutions (BASS) umbrella programme are eligible to apply. These are: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland and the United Kingdom.

DEADLINE

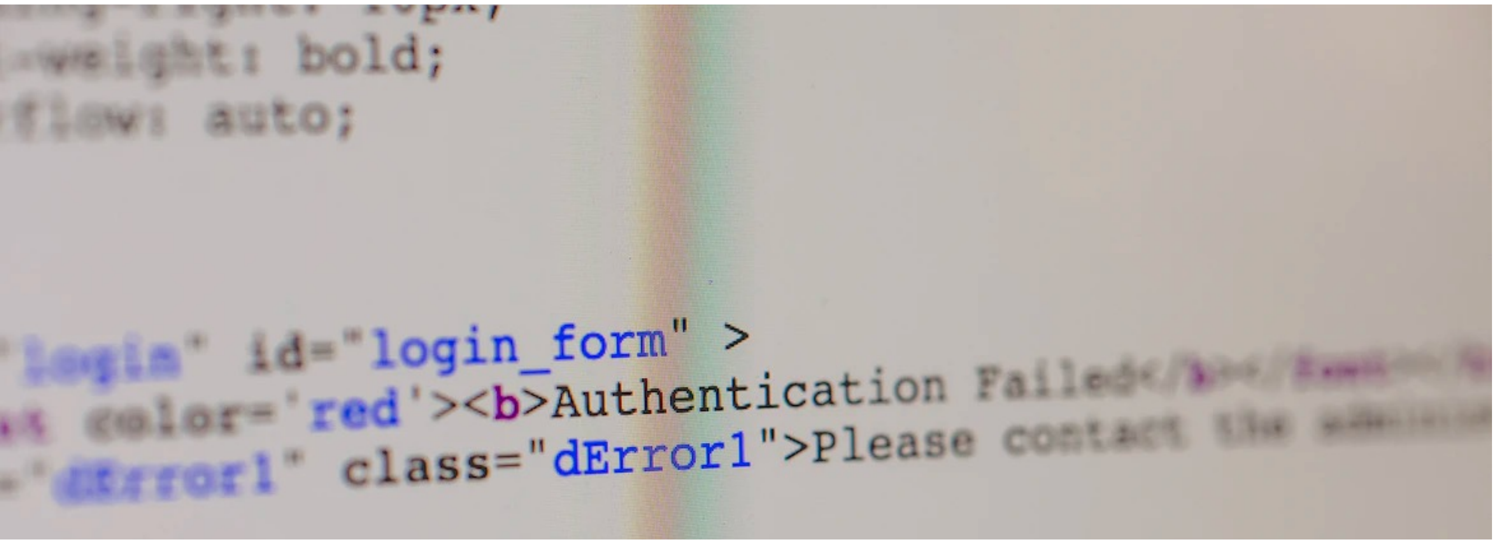
The deadline for the submission of outline proposals is 28 February 2023, and the tentative deadline for full proposal submission is 30 May 2023.

FOR MORE INFORMATION

Satellite Connectivity for Autonomous Land Vehicles Safety

Zero-Knowledge Proof: The next big thing they are not funding yet

Gregory Clare



```
-weight: bold;
flow: auto;
login" id="login_form" >
color='red'><b>Authentication Failed
"dError1" class="dError1">Please contact the
```

What is the best way to determine if something is true? By providing proof that supports a claim. In modern day society, we repeatedly engage in the act of proving claims. Our citizenship in a nation must be proven; our ownership of property must be proven; we are required to present proof of our income and bank statements to landlords, etcetera. As a paranoid individual myself, I am sceptical of the fact that our societies require so much invasive proof to take part in them—particularly when the items carrying these proofs also provide information that is irrelevant to the recipient.

Beyond the discussion about having—or not having—something to hide, your person can be adversely affected by scattered information about you. It is for this reason, therefore, that you are subject to rules to protect your personal information. Passwords are examples of such enforcement. They are required for safeguarding your accounts, which serve as proofs of ownership. And unless you use unique unbreakable twelve plus character passwords for each and every account you use, you create the real possibility that someone else can prove the ownership of your account after guessing your Welcome2022 work password.

However, the dawn of a new era might be around the corner. In this new world, you won't have to memorize 39D%E1297&$C&#hhi_2h2%, and you won't have to disclose your birthdate and birthplace to verify your citizenship. By utilising a cryptographic concept that originated in the 1980s, called Zero-Knowledge proof, cybersecurity experts are eliminating these dreadful threats to our privacy. The term Zero-Knowledge proof refers to a method by which a 'prover' convinces a 'verifier' of a truth without revealing any additional information beyond this truth.

The purpose of this article is to explore this highly intricate concept and why funders will want to encourage its use more widely. Spoiler alert: the reason is GDPR stupid!

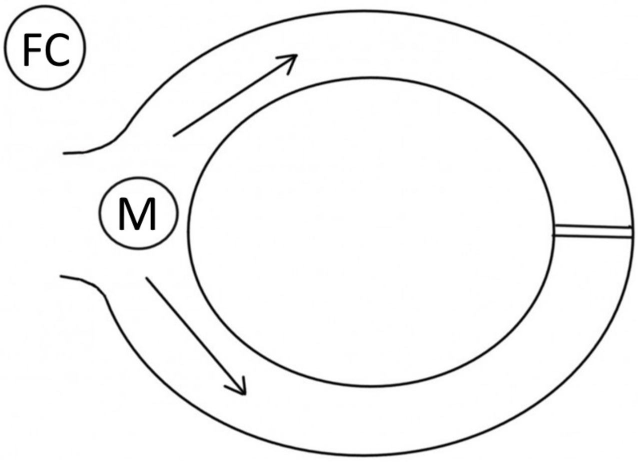
WHAT IS ZERO-KNOWLEDGE PROOF?

It is clear from my introduction that I am concerned with the prevalence of oversharing in our current proof systems. The extra information learned during the course of proving something is known as information leakage, a concept coined by MIT researchers Shafi Goldwasser, Silvio Micali, and Charles Rackoff. Zero-Knowledge proof was proposed by them as a theoretical system in which a first party (the Prover) communicates with a second party (the Verifier) to convince the latter of the truth of a statement.

Something is considered Zero-Knowledge proof when it meets three conditions:

1. Completeness: being convinced with a negligible chance of error with two honest parties involved.
2. Soundness: improbability of an untruthful prover convincing an honest verifier.
3. Zero-Knowledge: verifier will never learn more than the truth.

To help you better understand Zero-Knowledge proof, I will use a short excerpt from Jean-Jacques Quisquater's "How to Explain Zero-Knowledge Protocols to Your Children". Quisquater imagined finding the cave of the Ali Baba folktale in real life. It consisted of one entrance and two paths that curved around a toroidal geometry, as well as a magical door at the opposite end.



Following the excavation of the cave by archaeologists, a descendant of Ali Baba, Mick Ali, wanted to prove that he knew the secret code to open the rotating wall through which the 40 thieves escaped. Inviting a television crew for a demonstration, he did not intend to reveal the secret. Instead, he would demonstrate to the crew that he knew the secret without a doubt.

Mick went into the cave and went down one of the passages. Shortly after the film crew proceeded to follow him only as far as the fork. A reporter would flip a coin to choose between right and left. If the coin came up heads, he would shout to Mick to come out on the right. If the coin came up tails, he would shout to Mick to come out on the left. Remember, the wall is revolving, allowing anyone who knows the secret phrase to come out from any side they wish.

Proving that he knows the secret phrase, Mick came out on the right when the coin came down heads. In memory of the forty thieves, and to prove without a doubt that he knows the secret, this demonstration went on for another thirty-nine times. Each time Mick came out on the side the coin flip decided on. The probability of Mick failing if he didn't actually know the secret was considerably high, it was, therefore, certain that Mick knew the secret.

USE CASE FOR ZERO-KNOWLEDGE PROOF

The use cases for Zero-Knowledge proof are plentiful. Taking my previous example of passwords, Zero-Knowledge proof can include a series of questions that convince the verifier, a website or another online platform, that you own the account.

I can already hear your complaint that answering a load of questions instead of writing your password isn't very efficient. It could even become cumbersome, as it's eerily similar to the dreadful secret questions that some platforms already incorporate for password recovery. In comes an augmented password-authenticated key exchange protocol, named the Secure Remote Password (SRP) protocol, that allows users to authenticate to a server without providing it with a password.

With the help of a session encryption key, SRP encrypts a hash of the master password and sends it to the server, which decrypts the message and verifies the authentication. It is impossible for the server to know the master password, as it never existed on the server. However, the hashed message is used successfully to authenticate, because, like Mick Ali, the encrypted message proved that it knew the master password.

It is beyond the scope of this contribution to cover all the technical details of how SRP works. It should suffice to say that it serves as an example and a basis for other identification processes. I can envision the system being incorporated into passports, with barcodes triggering encryption that shares truths needed by verifiers, such as age or nationality verification.

WHY WOULD IT BE FUNDED?

In many ways, the methods for deploying Zero-knowledge proofs are closely aligned with the two measures of Article 25 of the General Data Protection Regulation (GDPR). These involve minimisation and limitation of data accessibility.

The use of protocols such as SRP can also alleviate companies, especially those with smaller budgets, from paying for expensive security measures and processes. Information you are not storing does not require protection. The use of Zero-Knowledge proof can allow businesses to communicate effectively with their customers without having to store all the customer's data. Sovereignty over your own data is an absolute must, with more and more data being weaponized by private and state entities.

It is highly persuasive to convince EU (European Union) funders that self-sovereign identity reduces GDPR exposure and all the related risks.

The key programmes to this end would be the following:

1. **Digital Europe:** the €7.6 billion programme that is designed to bridge the gap between research and technology deployment. One of the areas it seeks to strenghten European digital technology deployment is in cybersecurity.
2. **Connecting Europe Facility:** predominately aimed at funding trans-European networks and infrastructures. the CEF has a digital component that is worth up to €2 billion in funding in telecommunication projects.
3. **Horizon Europe:** the EU's most famous, and perhaps most notorious, funding programme that will be spending €95.5 billion to develop research and high-end innovation in enabing technologies. Approximately 35% of the budget is intended to support projects aiding the digital transition of Europe.
4. **InvestEU:** one to watch out for if you are also open to investment funding, as 10% of the €372 billion in public and private investments wil be covering the EU's digital goals.
5. **EU4Health:** another programme that has put 10% aside for digitalisation efforts to complement the core component of the programme, health. The programme has a budget of €5.3 billion.

ABOUT THE AUTHOR

Gregory Clare is a senior Grants Development Consultant and Business Development Manager at Grants Office. His areas of expertise include the funding landscape in the Netherlands and the EU, with a particular focus on digitalisation processes in education and the developing labour market. As a former grant writer and fundraiser in the Lebanese, Syrian and Turkish context, he is also adept to developing compelling projects for non-profit organisations seeking European funding. His spare time is filled with as much sports as possible and he claims to be an expert on European film.

LinkedIn Profile

Recovery Plans around the EU: Spotlight on Ireland's Green Transition

The design for a new platform at Kent Station in Cork is underway after the contract was awarded via Recovery and Resilience funding. Construction is expected to take place through 2023 and 2024.

Ireland's Recovery and Resilience Plan was approved by the European Commission back in July 2021. Compared to other member states' recovery plans, it is relatively small and consists altogether of €915 million in funding. Ireland's Recovery and Resilience Facility (RRF) plan is divided into priority areas:

- Priority 1: Advancing the Green Transition
- Priority 2: Accelerating and Expanding Digital Reforms and Transformation
- Priority 3: Social and Economic Recovery and Job Creation

COMPLETED PROJECTS

Several elements of the RRF plan have already been completed. Within the Green transition strand, for example, we have already seen a design contract awarded and planning permission requested for a redesign and expansion of Kent station in Cork as part of a broader RRF commitment to improve, electrify and expand the capacity of the commuter rail system in Cork. Construction is expected to start in 2023. We have also already seen significant developments in Ireland's efforts to enable the enhanced rehabilitation of the country's peatlands.

Meanwhile, within the Digital Transition priority strand, completed elements include the publication of a Ten-Year Strategy on Adult Skills and Literacy, the distribution of funding to schools to pay for digital infrastructure investments and ICT equipment for disadvantaged students, as well as project awards made to successful applicants to the Technological Universities Transformation Fund.

ONGOING PROGRAMMES

This year, we have seen the opening of two sets of grant programmes with rolling deadlines, funded through the Recovery and Resilience Facility, aimed at the private sector. These are schemes primarily intended to support established businesses in adapting to and taking advantage of the "Digital Transition", while also becoming more energy and resource efficient and developing low carbon processes and products as part of the "Green Transition":

Grants on offer under the banner of the Green Transition Fund include:

Climate Action Vouchers and Green Start

These are both small-scale grant funds aimed SMEs, large companies and high performing start-ups, designed to fund short external consultancy projects. Climate vouchers consist of EUR 1,800 towards the costs of up to 2 days independent technical or advisory services. These services should be ultimately focused on helping the company develop a Sustainability/Decarbonisation or Circular Economy Action Plan. Green Start offers a slightly larger grant (up EUR 5,000) towards the cost of hiring an Environmental consultant who will lead on what Enterprise Ireland is calling an "in-company assignment" to introduce environmental best practices achieve cost reductions targets and enable future environmental improvement projects.

Strategic Consultancy and GreenPlus

The Green Transition Fund also includes larger grant opportunities for consultancy projects. Via the Strategic Consultancy offer, for example, companies can get up to EUR 35,000 (covering up to 50% of costs) to enable the hiring of an external consultant to develop organisational carbon reduction roadmaps. Meanwhile, the Green Plus scheme offers up to EUR 50,000 (again covering 50% of costs) in support for training projects that develop the company's high level environmental management capabilities and drive environmental efficiencies. Unusually for a consultancy grant, this scheme does allow grant funding to be put towards certain internal salary costs—for up to 10 company "green project team members" who will be responsible for learning about green processes and tools and then training others within the company.

Enterprise Emissions Reduction Investment Fund

In addition to consultancy projects, the Green Transition will also support research and innovation projects in the areas of sustainability and decarbonisation (whether focused on developing new processes or products), as well as capital projects via two schemes—1) Capital investment for Energy Monitoring & Tracking (EM & T) Systems; and 2) Capital investment for decarbonisation processes. Through the former, companies can get up to EUR 50,000 towards the hardware, installation and commissioning costs of new energy monitoring and tracking systems, which will then allow them to account for the carbon footprint of their activities. Through the latter scheme, businesses can receive up to EUR 1 million (50% of costs for small businesses, 40% for medium businesses, and 30% for large businesses) to support significant capital investments in carbon abating technologies, such as Industrial Heat Pumps (including air, water, and ground source), Electric steam boilers, Heat recovery technologies, Mechanical Vapour Recompression (MVR) evaporators, and Biomass boilers.

For further details about the Digital Transition Fund, see "Upskilling, Infrastructure, and 'Process Innovation': Diving into Ireland's Digital Transition" in this issue of Funded.

Examining the Cybersecurity Initiatives available under the Digital Europe Programme

Vanessa Del Pozo Sánchez

Our current environmental problems, alongside the demands of advanced science, twenty-first-century communication, and the modern workplace, require the development of digital technologies and infrastructure in order to make Europe greener and more digitally integrated.

The Digital Europe programme, with its 7.5-billion euro budget—implemented by means of several multiannual Work Programmes—will accelerate the economic recovery in Europe and reshape society and the economy through a digital transformation. The programme focuses on five crucial areas to bridge the gap between digital technology research and market development. One of those areas is cybersecurity, and in particular, strengthening European cybersecurity infrastructures—the 'cyber shield'—and promoting the widespread adoption of state-of-the-art cybersecurity practices and equipment. It will benefit everyone, but small and medium companies especially.

Over this autumn, several funding programmes have been mobilised as part of the Cybersecurity and Trust call. This call aims to develop a secure network across the Member States of the European Union, which relies heavily on resilient data infrastructure.

In brief, these are the programmes involved in the call, which will remain open until 24th of January 2023:

1.CAPACITY BUILDING OF SECURITY OPERATION CENTRES

As part of this programme, funding is provided for the creation of Security Operation Centres, which can serve as central hubs for security tools, practices, and responses to security incidents, thereby strengthening cyber threat surveillance and early detection capabilities. A faster, more effective, and more cost-effective response to security threats across Europe will result in improved preventive measures and better security policies.

Budget: €80,000,000

2. UPTAKE OF INNOVATIVE CYBERSECURITY SOLUTIONS

A key objective of this programme is to enable organisations, especially SMEs, to adopt innovative cybersecurity tools, services, and solutions developed by entities participating in EU-funded innovation projects.

Budget: €32,000,000

3. DEPLOYING THE NETWORK OF NATIONAL COORDINATION CENTRES WITH MEMBER STATES

This program aims to establish a European Centre of Industrial, Technological and Research Competence in Cybersecurity. The member states will cooperate transnationally and will take joint actions through their national coordination centres. Through joint contributions, industry, civil society, business, research entities, and government will be able to share expertise on cybersecurity issues that emerge as solutions to national and regional challenges.

Budget: €22,000,000

4. EU CYBERSECURITY RESILIENCE, COORDINATION AND CYBERSECURITY RANGES

Applicants can choose between two objectives, when designing projects for this program: a) To strengthen cybersecurity actors in the Union so they can respond to major incidents in value chains, enable feedback on cases, and also foster the role of the CSIRTs, the CyCLONe network, and the Joint Cybersecurity Unit, all while taking into account the Blueprint. b) To Develop, interconnect, and strengthen cyber security ranks at the European, national, and regional levels, as well as within and across critical infrastructures, and to foster networking between them in order to develop cyber-security capabilities and expertise in technologies—such as 5G and artificial intelligence—that can be applied to a wide range of industries. Additionally, this objective aims to support cybersecurity trainings and workshops for public and private entities.

Budget: €15,000,000

5. SUPPORTING THE NIS DIRECTIVE IMPLEMENTATION AND NATIONAL CYBERSECURITY STRATEGIES

This programme extends the work currently supported by the CEF Telecom programme. As part of the programme, Member States and the European Commission will build their technical, operational and strategic capabilities in cyber security and improve cross-border cooperation in cyber security.

Budget: €20,000,000

6. TESTING AND CERTIFICATION CAPABILITIES

This scheme is aimed at improving capabilities and facilitating cooperation by enhancing security and interoperability testing capabilities and certification for connected ICT systems. This programme may also fund national cybersecurity certification authorities and small to medium-sized companies in capacity building as well as in testing and certifying their ICT products, services, or processes.

Budget: €5 000 000

7. SECURING 5G STRATEGIC DIGITAL INFRASTRUCTURES AND TECHNOLOGIES

This scheme aims to develop the knowledge and capacity of national authorities, via, for example, the exchange of best practices, training of staff, deployment of innovative assessment methods, support for standardisation activities, and the procurement of specialised services (such as audits and technical assessments).

Budget: €10 000 000

8. LARGE-SCALE PILOTS FOR CLOUD-TO-EDGE BASED SERVICE SOLUTIONS

Through this programme, organisations with sustainable, innovative, secure, and cross-border cloud-to-edge services will receive funding to deploy pilot projects on a large scale to test the versatility and robustness of their cloud-to-edge solutions. Projects that can be taken up by a variety of public sector entities, in different geographies, and that can deliver a variety of services will receive preference.

Budget: €40 000 000

9. SPECIALISED EDUCATION PROGRAMMES OR MODULES IN KEY CAPACITY AREAS

By enabling collaboration between higher education institutions and the private sector, as well as with digital technology research centres, this programme aims to enhance educational programs in key capacity areas, enabling professionals and students to acquire advanced and relevant digital skills, as well as facilitating businesses in attracting and retaining digital talent to close gender disparities.

Budget: €56 000 000

A key aspect of all these programmes is that their objectives, especially in cybersecurity or data protection, can only be achieved through a thorough understanding of the Union's security interests. As a result, the programme aims to bridge the gap between digital technology research and market deployment all over the European Union.

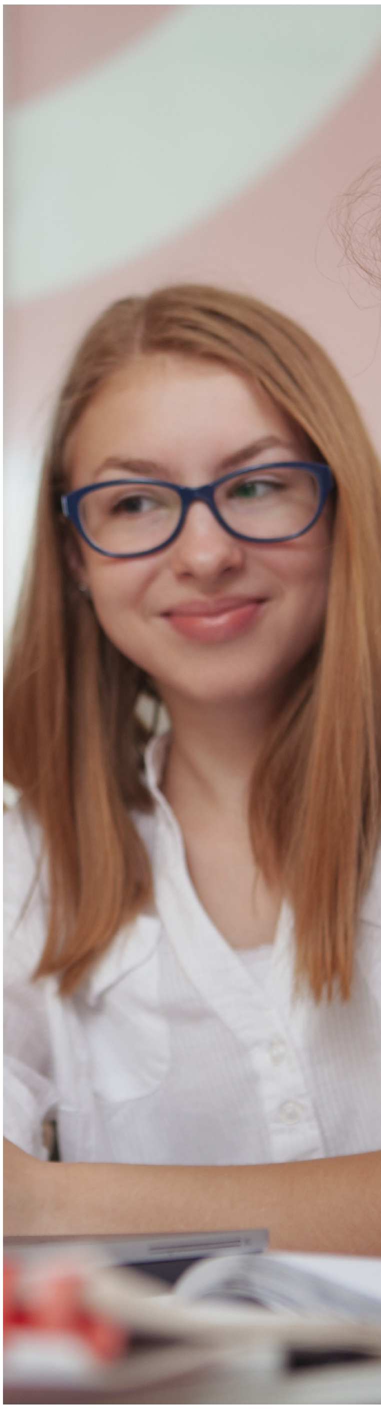
ABOUT THE AUTHOR

Vanessa Del Pozo Sánchez is a senior grants consultant for Grants Office Europe. Driven by reason, analysis, and the disposition to help others, she takes pride in coming up with plausible solutions for a broad range of problems, all as part of a system of human cooperation. As part of the team of Grants Office, her goals include support to public and private entities in their search for grants for high-tech projects in Spain.

LinkedIn Profile

UK Programme Snapshot - Public and Third Sector

Youth Investment Fund: Phase 2



SUMMARY

Phase 2 of the Youth Investment Fund (YIF) is being delivered by Social Investment Business, the National Youth Agency (NYA), Key Fund, and Resonance. The funding itself has been allocated to the YIF by the Department for Digital, Culture, Media and Sport (DCMS). The basic idea behind the fund is to support the renovation and construction of facilities for non-school youth activities in the public and voluntary sectors in England. The ultimate goal in funding these capital projects is to empower young people to be active members of their communities, to equip them with skills that will be useful within and outside of work, and to improve their health and wellbeing.

Alongside capital costs (covering construction of new facilities, refurbishment of existing facilities, and installation of fixtures & fittings), the YIF will also in certain circumstances cover the associated revenue costs such as project management, professional costs, legal fees, and the hiring & training of more youth workers and staff.

Buildings used not only for youth sector services but for other purposes as well are eligible under the programme; however, the proportion of youth work conducted in the building will be taken into account during the proposal review process.

The grant-makers have said they expect the majority of grant requests to fall between £300,000 and £8.7 million. For this round, covering 2022-2025, £288 million has been allocated to the YIF for capital grant requests and £80 million for revenue grant requests.

ELIGIBILITY

The following organisation types can apply, whether alone or as part of a consortium:

- local authorities, including parish and town councils
- registered or exempt charities
- uniformed organisations
- community interest companies (both companies limited by guarantee & companies limited by shares)

Funded projects can only take place within wards in England identified by the YIF as areas of greatest need. The location eligibility applies to the site only, not to organisations' base locations, or the location of young people who may use or benefit from the site. A map and list of the eligible wards can be found here.

DEADLINE

Applications can be submitted at any time, and the grant-makers have said they will likely hold grant committees to decide on applications through until March 2024.

All grant funding must be spent and accounted for by 31st March 2025.

FOR MORE INFORMATION

Youth Investment Fund (YIF)

Upskilling, Infrastructure, and "Process Innovation": Diving into Ireland's Digital Transition

William Bond

Back in February, the Department of the Taoiseach published the whitepaper Harnessing Digital, which laid out the Irish government's strategic approach to digital transition over the next ten years—or what the EU is calling the "new digital decade." Following the four pillars of EU's Digital Compass, Ireland's plan consists of commitments to the digital transformation of business, essential infrastructure and public services, as well as digital upskilling across the workforce. All of these pillars entail increased levels of investment from National government and the EU, as well as—in the case of the Digital transformation of business—significant long-term grant funding opportunities for the private sector.

INFRASTRUCTURE AND PUBLIC SERVICES

The plan for developing Ireland's digital infrastructure focuses on digital connectivity and cybersecurity. Key goals include the provision of Gigabit network coverage for all homes and business by 2028, with 100% 5G coverage arriving in 2030. In addition, the plan sets out an ambition to have all government departments increase their cyber resilience, an objective first articulated in the National Cyber Security Centre (NCSC)'s 2019-2024 strategy.

Equally fundamental to the long-term strategy is the digitization of the public sector. We have, for example, already seen €64 million in funding from Ireland's Recovery and Resilience Facility (RRF) allocated to primary schools to support Broadband connectivity (as part of the Schools Broadband Programme) as well as to support the purchase of devices and other measures to ensure no students are left behind during the digital transition. Meanwhile €75 million has been committed as part of the RRF to fund the development of a range new e-pharmacy systems across Ireland's hospitals, as well as a single national "integrated financial management system" to improve procurement efficiency within the health system, which—despite planning delays this year—is expected to be completed by December 2023.

DIGITAL SKILLS

The government's strategy also involves new investment in high-level, specialist digital skills; we can see a model for how this will play out in practice over the next few years in the Human Capital Initiative, a 2022 competitive scheme which has been supporting Irish universities in developing and offering new courses to target innovation, digital skills and "priority skills needs for the economy." Additionally, Harnessing Digital saw the government commit to funding transferable (less specialized) digital skills for the labour market via the National Training Fund (which is funded by a 1% payroll levy on Irish employers). The NTF surplus in September 2022 was €855 million with projections suggesting it would rise to €1.5 billion by 2025, leading to greater scrutiny on the NTF from the Irish business community and consternation from deputies in the Oireachtas over a lack of clarity about how the funds are going to be used at a time when digital upskilling is such a key priority.

Significantly, the view of the Irish Business and Employers Confederation (Ibec) is not merely that such funding for skills should make its way back to employers via, for example, grant programme for businesses; in fact, among Ibec's September recommendations was that additional NTF funding be used to "mainstream" successful innovative skills projects piloted through from the Human Capital Initiative, so as to better align the whole Higher Education sector to the skills needs of the wider economy.

TRANSFORMING IRISH BUSINESS: DIGITAL TRANSITION FUND

Despite the salience of the government's commitments to digital upskilling, the most important pillar of Harnessing Digital from the perspective of the private sector is the first—the Digital Transformation of Business. The major goals of this pillar are to encourage investment in "Cloud Computing, Big Data, and AI," to raise 90% of small and medium-sized enterprises to "Basic Digital Intensity level by 2030," to target national funding for start-ups and early-stage businesses towards new digital innovators, and finally to use the RRF-supported Digital Transition Fund to accelerate the digitalization of established Irish business.

The Digital Transition Fund opened this summer, and is being administered by Enterprise Ireland. Its purpose is to distribute €85 million to Irish businesses to enable a range of digitalization measures from now until 2026. The funds are allocated via competitive grant programmes, targeting businesses of different sizes as well as a variety of different project types. Depending on the individual scheme, applicants must be clients of Enterprise Ireland (EI), Údarás na Gaeltachta, or one of Ireland's 31 Local Enterprise Offices (LEOs).

The competitive programmes include several schemes specifically targeting external consultancy and training projects. The Digital Discovery grant, for example, is designed to enable businesses to put together a "strategic roadmap for their digital transition," by helping to cover the costs of the necessary external consultancy. EI will cover 80% of the project's costs, and the maximum total award is €5,000. Projects should consist of analysing the company's existing digital systems, processes, skills, and culture, exploring opportunities for improvement (including the potential utility of certain digital services or products), and finally creating the roadmap itself. The Digital Marketing Capability grant, meanwhile, offers larger awards to cover the consultancy costs for developing a digital marketing strategy and training senior management. The typical grant rate is 50% and the maximum award is €35,000.

In addition to funds for consultancy and training projects, the Digital Transition Fund includes support for Digital innovation and R&D. The Exploring Innovation grant offers up to €35,000 (covering 50% of costs) for projects that enable planning for future R&D. This could involve viability analysis, prototype development, or analysis of current scientific or technical knowledge in a particular area. R&D grants (up to 45% of costs) are also available for experimental development projects and will cover costs such as existing and new staff, overheads, materials, patenting, and capital depreciation. The Operational Excellence grant is a particularly interesting new element of EI's funding portfolio, as it offers funding not just for innovation and training to enable business growth, but also for capital assets (covering 15%-35% of costs), including new or second-hand equipment and installation costs.

Crucially, several of the Fund's innovation programmes (including the Operational Excellence scheme) will accept applications for funding to support Digital Process Innovation (DPI). DPI refers to projects which involve innovation in digital production methods, service delivery or organisational structure. The idea is that the business will be able to integrate new technologies into their existing work-flow, develop new digitized modes of experiences for their customers (whether through new digital products or services), or use digital methods to make their business practices more sustainable. DPI can include the use of cutting edge robotics, automation or visualisation technologies in a manufacturing context, but it can also include new digital customer service systems, or new business models. The ultimate goal is to improve the competitiveness and productivity of Irish business. Across all schemes, if an applicant is looking to fund a DPI project, the maximum grant is €150,000 (covering no more than 50% of costs) regardless of the applicant's organisation size.

ABOUT THE AUTHOR

William Bond is a grants development consultant for Grants Office Europe, where he supports grant-seekers in the UK and Ireland in identifying government funding for various projects including and low-carbon and green transition initiatives. He received his PhD in English, which focussed on early American environmental aesthetics and thought, in 2021 from Northeastern University, Boston, Massachusetts.

LinkedIn Profile

The European Defence Fund

Charlotte von der Brelie

Following Russia's invasion of Ukraine, the defence budgets of European nations have increased significantly—by nearly 200 billion euros. In addition, we have seen announcements concerning the block's new military strategies. These strategies have so far predominantly focused on the procurement of military equipment, and the European Commission (EC)—the policy-making arm of the European Union (EU)—has since reiterated a commitment to defence and innovation.

The European Defence Fund (EDF) is the first foray into funding military research collaboratively across the block. It has been in the planning stages for many years; however, the first calls for grant proposals are remarkably timely. This being said, there remains some uncertainty about the delivery of the EC's promise to increase funding in defence innovation and R&D, since most of the R&D funding announced, including the EDF, has been years in the making with the Russian invasion adding urgency to these pre-existing plans to increase collaboration and funding for defence research across Europe. Uncertainty remains as to whether the EC intends to implement their renewed support for defence on the European level and if and how further funding will be allocated to military outcomes.

THE EU IS A PEACE PROJECT

The change in policy is striking, since the EU is nominally a peace project, born out of an economic collaboration designed to manage the coal and steel industries, and EU policy has always been centred around economic targets and interests. The main raison d'être of the EU is the promotion of trade, prosperity, and peace. Defence has therefore remained a national aspect of governance and has been handled by the individual member states.

The EU's biggest funding mechanism for R&D, its flagship if you will, is the Horizon Europe programme. With a budget of €95 billion, Horizon Europe explicitly excludes defence-related research. Military spending has continuously declined in Europe following the fall of the Berlin wall, while the three largest European spenders since 1989 have been France, Germany, and the UK. Following the Crimean annexation, the EC President at that time, Jean-Claud Juncker, pushed for a stronger defence role for the EU. Calls of this kind have only intensified in subsequent years, in part as a reaction to the Trump presidency and the subsequent fragilization of the US-EU Partnership.

The EDF started in full in 2021 with a seven-year budget of €7.9 billion, €2.8 billion of which is designated for research, while the remainder is devoted to development. The grants only support internationally collaborative work, and most of these grants go to institutions such as semi-governmental research and technology organisations (RTOs) rather than to universities.

THE EU'S LIMITATIONS

Throughout the current crisis, the EC has made several announcements of strategies designed to counter the underinvestment in both European defence capabilities and research and development in the area. However, the EDF remains the block's only defence R&D fund. In May, the European Defence Innovation Scheme (EUDIS) was announced. This EUR €2 billion package of support measures was pitched as means of helping firms provide technology to the military over the next 5 years but at least three-quarters of the fund, it turns out, are simply repackaged yet already-budgeted EDF funds. The bottom line on additional EU defence funds is that the EU can do little, since the budget for 2021 to 2027 has already been set. These multiannual financial frames are the core of European funding organisation, and they allow for very little wiggle room or later additions. This hindrance will keep EU action limited.

ABOUT THE AUTHOR

Charlotte von der Brelie is specialised in German funding opportunities, as well as European structural funding and IPCEI projects.

NATIONAL LEVEL

However, member states have individually significantly increased their budgets since the invasion. Germany is the most notable case, with a special defence budget of €100 billion that will be spent over an undefined time frame. Most of these funds will support the defence industries and RTOs and focus on procurement but there is also a €400 million pocket for R&D defence spending. France added €3 billion to its defence budget in 2023, which is the highest increase in 50 years, with the largest investment being made in ammunition.

THE EDF

Awards for the first batch of calls from the EDF have been made, amounting to a cumulative €1.2 billion for 61 defence R&D projects. Applicants were required to build a consortium consisting of at least three firms from at least three member states or Norway, and the EC announced that it received 140 proposals. The selected projects represent nearly 700 companies from 26 member states as well as Norway. Most projects are related to air, ground and naval combat capabilities with €190 million, €158 million and €104 million allocated, respectively. Air and missile defence efforts will receive €100 million, whilst space, cyber, sensors and information superiority alongside other emerging and disruptive technologies should receive around €227 million in cumulative funding.

France, Germany, Spain, and Italy are all represented in large numbers with each accounting for more than 100 participating industry partners. Importantly, a number of these awarded projects are building upon ongoing efforts funded by the EDF's predecessor, the European Defence Industrial Development Program (EDIDP). One example is the MBDA-led consortium "Modular Architecture Solutions for EU States (MARSEUS)," which is developing a beyond-line-of-site missile capability, and which for these efforts, will receive €25 million over 36 months.

The new round of funding for 2023 will be worth a cumulative €924 million and is separated into several parts. The first part of 2023 with a total of €255.5 million will support capability development (€213 million) and defence research (€42.5 million). Further topics that are expected to be addressed next year are semi-autonomous naval vessels, multiple space-related assets, and a variety of ground, air combat and disruptive technologies. Below you can see an excerpt from the call program that shows the indicative budget for the multi-financial framework 2021-2027.

Category of Actions	Indicative EDF budget contribution during 21-27
1. Defence medical support, CBRN, biotech and human factors	
2. Information Superiority	> 10%
3. Advanced Passive and active sensors	
4. Cyber	
5. Space	> 10%
6. Digital Transformation	
7. Energy Resilience and environmental transition	> 5%
8. Materials and components	
9. Air Combat	> 10%
10. Air and missile defence	> 5%
11. Ground combat	> 10%
12. Force Protection and mobility	
13. Naval combat	> 10%
14. Underwater warfare	
15. Simulation and training	
16. Disruptive technologies	4% - 8%

EU Programme Snapshot - Public and Private Sector

Connecting Europe Facility (CEF)—Backbone connectivity for Digital Global Gateways (CEF-DIG-2022-GATEWAYS)

SUMMARY

The goal of this call from the Connecting Europe Facility (CEF) is to support the deployment of strategic networks as part of the EU's Digital Global Gateway Strategy to improve the quality and availability of connectivity within the Union as well as with third countries. The call also tackles the lack of or unbalance in connectivity across Members States and Outermost Regions and Overseas Countries and Territories.

The call funds 'works' rather than 'studies', even though it is possible to include studies within work proposals. Construction and interconnection are funded by the call, but costs for operating the infrastructure are not. The grant will cover:

- networking solutions for the foreseeable system lifetime, from end to end, including cable landing stations and their connectivity infrastructure
- satellite backbone solutions, but only the costs linked to the construction of satellite ground stations and their interconnection with local networks
- cost related to significant improvement of local access network, but only in areas where the infrastructure is unlikely to develop, and only within limits defined in the Call
- costs related to integrating sensors into a submarine cable system (e.g., smart cables)

It will not cover:

- costs for operating the infrastructure during its lifetime and extra components at the landing sites not required for the basic end-to-end connectivity such as data centres, hosting facilities and other services

Project budgets (maximum grant amount) are expected to be up to EUR 30 000 000 per project. The amount is indicative and may be exceeded if duly justified by the applicants.

ELIGIBILITY

Eligible partners and beneficiaries are public and private bodies established in one of the EU Member States, including EU Member States, including overseas countries and territories (OCTs). Other entities may participate in other consortium roles, such as associated partners, subcontractors, third parties giving in-kind contributions, etc.

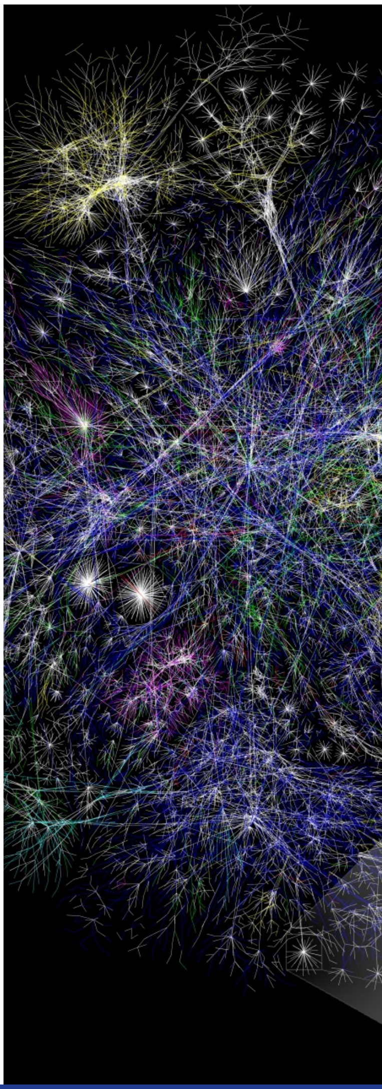
Please note that this call is subject to restrictions due to security reasons. This means that entities must not be directly or indirectly controlled from a country that is not an eligible country.

DEADLINE

The deadline for the submission of full proposals (this is a one-stage application) is 23 February 2023.

FOR MORE INFORMATION

Backbone connectivity for Digital Global Gateways (CEF-DIG-2022-GATEWAYS)



The CEF Digital Backbone connectivity for Digital Global Gateways scheme aims to contribute to bridging the digital divide and ensuring equal access to Gigabit networks for EU citizens and businesses.

Grants Office Europe needs writers!

Do you have experience working with national, regional or local institutions or SMEs in the following EU Member States?

- France
- Germany
- Italy
- Spain
- The United Kingdom
- Ireland

Are you a native speaker of French, German, Italian, Spanish or English?

Do you have experience with European Union programmes?

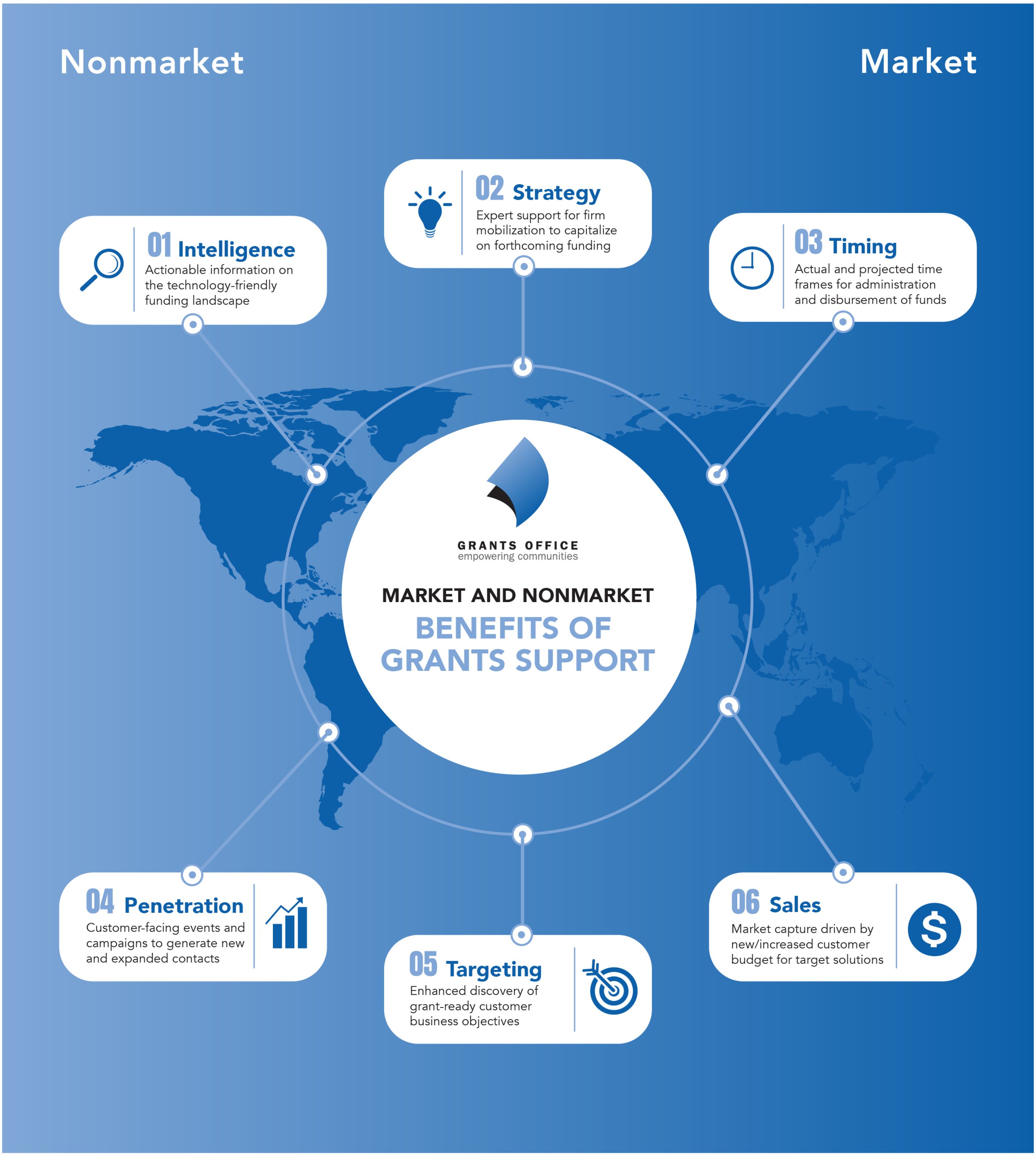
Grants Office Europe, LLC is a full-service provider of strategic grants development services for municipalities, education institutions, non-profit organisations, healthcare providers, and technology industry partners. Our approach to proposal development is based on collaboration and open communication among team members and clients. We aim to lower risk and shrink the investment of time and resources required for our clients to pursue grant funding.

Our grant writers work directly with clients to help develop all elements of the project and coordinate the submission of a high-quality competitive proposal.

WE'RE ALWAYS LOOKING FOR NEW WRITERS, JOIN THE TEAM TODAY!

Reach out to us at info@grantsoffice.com with:

- Your CV
- A listing of the European, national or regional agencies for which you have submitted grants
- A list of the grant programs for which you have been a proposal reviewer, if any
- 2 writing samples (preferably narratives from successfully funded projects)



Nonmarket

Market

GRANTS OFFICE
empowering communities

MARKET AND NONMARKET BENEFITS OF GRANTS SUPPORT

01 Intelligence

Actionable information on the technology-friendly funding landscape

02 Strategy

Expert support for firm mobilization to capitalize on forthcoming funding

03 Timing

Actual and projected time frames for administration and disbursement of funds

04 Penetration

Customer-facing events and campaigns to generate new and expanded contacts

05 Targeting

Enhanced discovery of grant-ready customer business objectives

06 Sales

Market capture driven by new/increased customer budget for target solutions

USA:
grantsoffice.com
info@grantsoffice.com

CANADA:
grantsofficecan.com
CanadaHelpdesk@grantsoffice.com

AUSTRALIA:
grantsoffice.com.au
AustraliaHelpdesk@grantsoffice.com

EUROPE:
grantsoffice.eu
EuropeHelpdesk@grantsoffice.com

A GRANTS OFFICE PUBLICATION