Cybersecurity virtual cluster

HORIZON 2020: CLUSTER FACILITATED PROJECTS FOR NEW VALUE CHAINS/INNOSUP-1-2015

Neulogy is a Bratislava based consultancy providing complex solutions and services rendered to institutions as well as to companies in the area of research, development and innovations. As a leader in fostering R&D projects with activities spreading across the entire Danube Region, we see an enormous unused potential of the region in creation of synergistic value chains.

Neulogy is a founding member of SAPIE – Slovak Alliance for Internet Economy, together with Eset, Google and many other multinationals as well as successful innovative companies from Slovakia. As such, we decided to focus on fostering spillover effects stemming out of the cybersecurity sector within the European Commission project HORIZON 2020 - cluster facilitated projects for new value chains (INNOSUP-1-2015).

Neulogy as a project coordinator is responsible for the setup of the concept, priorities and project management. In order to fulfill the project objectives, we are looking for strategic partners from the Danube Region to coordinate and implement activities at the local level. These institutions shall be primarily clusters and/or SME intermediaries, such as industry associations, business platforms, etc.. Furthermore, involvement of other institutions form associated sectors that could further enhance synergy effects of the proposed project is desirable.

Context

Cybersecurity has become a ubiquitous term constituting one of the most searing business and societal challenges of the present. Threats arising out of the potential cyber-attacks put this area of ICT industry into the focus of not only government institutions, but also companies and private individuals.

Countries of V4 region are already in a possession of well-developed cybersecurity ecosystem. The central European cybersecurity ecosystem comprises multinational corporations, fast growing startups and SMEs, venture capitalists and technical universities with globally top-ranked ICT programs. Moreover, software antivirus vendors with origin in the region are leaders with compounded share exceeding one third of the global market. ESET, AVG and AVAST protect approximately half a billion users worldwide and are growing at a double digit pace per annum.

Those genuine entrants are currently not harnessing synergies arising out of the physical and cultural proximity neither among themselves nor with the well-established industries automotive and shared service centers, which are both of the highest significance for the economy of the region. Manufacturers such as VW Group, Kia Motors, General Motors, Fiat and PSA Peugeot Citroen and their suppliers employ more than 500 thousand people in the V4 region with total revenues exceeding 50 billion EUR. In individual countries, the automotive industry accounts for up to 6% of GDP alone. Of a similar importance are also shared service centers, which are abundantly represented in every country of the V4 region, where they employ up to 100 thousand people per single country. These industries operate with a large scale of sensitive data that are necessary for their operations. Therefore, a vehicle establishing ties among all entrants would create widespread synergies and spillovers. By doing so, such activity would aspire to reinforce strong position of the V4 region in the fast developing cybersecurity industry, positively impact the economy of the region and its innovation potential.

The Digital Agenda of the EU has set cybersecurity as one of its priorities in the coming decade. While the Agenda lays out a common platform for all member states, an immense space for regional cooperation remains open. Moreover, by taking progressive regulatory measures, the V4 region could significantly advance its ICT environment, which is seen by the World Economic Forum's Networked Readiness Index (NRI) as a laggard among the EU countries. A vehicle actively pursuing discussion at a national and regional level would pioneer strategies and policies representing a single framework for the region. Those policy measures would also serve as an inspiration for other countries and the entire EU.

Project ambitions

The proposed project aims to bring closer all cybersecurity stakeholders and promote the growth of the industry on national, regional and international scale. As such, the project will:

- Create a collaborative environment for stakeholders in cybersecurity industry
- Facilitate common projects to overcome current industry issues
- Act as a lobby representing interests of the industry at governmental level
- Support education and knowledge sharing
- Promote growth and creation of innovative SMEs
- Match attractive SMEs with venture capital financiers

With respect to the ambitions of the project and its mission stated above, a suitable vehicle for the proposed project is a virtual cybersecurity cluster. Such entity has a potential to create a well-functioning single platform, which facilitates project initiation and collaboration among partners from various countries by leading an internal and external communication among stakeholders.

Partners of the project

The goal is to connect entire cybersecurity ecosystem/relevant cybersecurity actors of the V4 region. The coordination and facilitation shall be led by cluster organisations and other intermediary organisations, by following a systemic approach that combines different resources, tools and instruments. Innovation actors, especially SMEs with mutually reinforcing competences, shall be supported in view of creating new industrial value chains that foster the development of emerging industries in Europe. Therefore, we are looking for partners acting as associations, cluster and/or other intermediary organisations.

The central European focus of the cluster presupposes partners from Slovakia, Czech Republic, Poland and Hungary. However, within a broader context of the project, the partners from the entire Danube region are welcome, too.

Project outputs

The expected outcome of the project focuses on strengthening the V4 region by fostering one of the most attractive ICT segments of today. More specifically, the most significant deliverables of the proposed cluster are:

- Creation of new collaborative projects, products and services

The only way how SMEs can remain competitive with large multinational companies is through constant innovation and flexibility. The cluster has a significant advantage over the stand-alone companies when it comes to spotting the commercial potential of emerging technologies coming out of the companies´ research. This fact would be further strengthened by establishing a knowledge transfer center operating under the cluster´s management. The center´s core activity would be management of the research and development within the cluster, evaluation of commercial potential and protection of intellectual property rights. With this set of activities, the participating SMEs will be substantially unburdened and allowed to focus on R&D and growth of their business.

By creating an internal communication platform open to every member, the cluster will also serve as an enormous directory for participating entities to share information and contacts. Moreover, this platform would allow asking for assistance and referrals, informal know-how trading or initiation of new collaborative projects for a particular purpose. This might be especially beneficial for small or young innovative companies lacking the market credibility. The internal communication platform, built up through reciprocity over time and previous knowledge of the cluster members, with assistance from the knowledge transfer center is determined as a key feature for conduction of new cybersecurity projects.

Thanks to the inclusion of universities and research centers, the proposed model of the cluster promises higher turnover of scientists and engineers collaborating with corporate professionals within an open environment. A geographical proximity to knowledge centers allows for designing, testing and prototyping results of the collaboration among the cluster members. Therefore, the expected outcome is an abundance of market-led products and services coming from participating SMEs.

- Increased efficiency and growth of the cluster members and incubation of spin-offs/startups

Cooperation among the members is expected to be also of a formal character. In this case, the emerging products and services will be transformed in spin-offs, spin-outs and joint ventures, whose creation will be facilitated and strongly encouraged by the cluster. The process of setting up these newly established startups will be simplified by a unified process developed and led by the cluster´s management. The cluster will provide, via its knowledge transfer center, also the protection of intellectual property rights, peer review from the industry experts and access to public funds, venture capital or business angels. The cluster acting as an umbrella organization can significantly speed up the investment process while minimizing risks for the founding entities. Furthermore, the newly established small and medium companies will be facing lower entry barriers since they stem out of the real market need recognized by the industry leaders. The cluster would also serve as an initial market for these companies while attracting also outside firms as business partners.

The cluster will propose enhancement of the reciprocal relations and trust among participants. As a result, the members are encouraged to create consortia with SMEs for contract tenders, join marketing efforts of products and services or share the reputation and references with them. Such synergies will foster the business development of participating entities and increase efficiency of a substantial piece of their business activities.

- Creation of a cross-industrial partnership

Leading industries of the V4 region, such as automotive and IT are natural partners of the cybersecurity cluster. The potential of the collaboration between industries is enormous with synergies beneficial for both sides. The potential outcome from this kind of partnerships lies in reconciliation of the mutual expectations and needs, emergence of industry specific products/services or even the creation of niche SMEs. Taking into account the global presence of the proposed cross-industrial partners, another potential outcome emerges in rapid internationalization of participating small and medium companies. Therefore, the cluster aims to create affiliations with existing automotive and IT

associations. This will lead to creation of new corporate partnerships and common projects as well as to creation of an open forum for improvement of the cybersecurity products.

- Adoption of progressive regulatory and policy measures

Taking into account proposed activities and integrating role of the cluster, the natural outcome is expected to be increased policy leverage on public sector. The lobby will assist to the cluster development by promoting measures and successful stories from other countries. While the primary concern will be an improvement of the regulatory framework for the ecosystem, further actions will be aimed at unlocking barriers of international and cross-sectoral collaboration and support of the education.

- Increased industry awareness

In order to clearly display a shared identity and future vision, the cluster will execute all necessary marketing and PR activities. Among the planned activities are a web page, social media communication, press releases and networking events. An indispensable part of promotional activities will be a portal providing comprehensive newscast and cybersecurity related information, while concurrently informing about possible business opportunities between the cluster and external SMEs. Furthermore, compilations such as market reports and industry yearbooks focused on V4 region will further enhance the industry awareness. All these activities would not be possible to accomplish for individual companies within their infrastructure.

- Integrated knowledge system

Cybersecurity companies are facing a lack of qualified labor. To alleviate this challenge, the cybersecurity cluster will organize practical workshops and trainings related o cybersecurity profession. Moreover, sharing of information and knowledge spillover will be promoted among the cluster members by organizing intercompany sessions.

Since the inception of the cluster, relationships with academic institutions are to be established. The collaboration with universities promises to create common study programmes with a curriculum preparing IT students for a profession of cybersecurity specialist. The ultimate goal of such efforts is a system ensuring to provide sufficient pool of cybersecurity professionals with marketable skills.

Benefits for the partners

Each partner of the project will become a member of the largest IT and cybersecurity network in Central Europe. This includes:

- Co-create a strategic vision of the region in cybersecurity
- Design and implement supporting scheme for development of new industrial value chains
- Benefit from cross-border synergies and potential
- Establish leadership position in cross-industrial innovation
- Become a preferred partner of choice for both academia, government and business