Cyber Security for Europe

Policy Recommendation

Promote new sovereign solutions in cybersecurity: support blue-sky research and nurture their results

Context and Findings

- **Europe's digital sovereignty may be at risk** from imported cybersecurity technologies developed in non-EU countries.
- **Most EU-funded research projects in cybersecurity have a duration that is too short** to allow the development of fundamentally new innovative solutions.
- **Most calls for proposals in the area of cybersecurity ask for projects with a technology readiness level (TRL)** that is far too high for basic research minimising the opportunity to deliver fundamentally new breakthroughs.
- European researchers in cybersecurity have demonstrated that their new ideas can have an impact worldwide.
- EU funding instruments should **support European cybersecurity researchers at the very earliest stages** of idea development.

The Problem

Although Europe invests significant amounts of funding in cybersecurity research, most of the funds are for **short-term medium to high TRL projects** which have practically no time to explore fundamentally new and promising technologies. Unfortunately, without the proper environment to create new developments and to nurture them to fruition, **Europe is forced to import its cybersecurity technologies from overseas**. Such a practice not only increases Europe's reliance on imported technology but may also significantly undermine its long term digital sovereignty.

The Scene

Ground-breaking ideas that could significantly change the world for the better usually need a lot of time to develop and reach maturity. In addition, such ideas also need space: a nurturing environment in which to grow, flourish and find their place in the sun. We should be willing to take high risks to create such environments and to give them a chance to ultimately reap high rewards. Highly innovative ideas and technologies need a lot of time between their gestation and the time they achieve a noticeable market share. For example, the mobile phone took 29 years to reach 20% market penetration; LED lights took 24 years; the Internet took more than 25 years, ATM cards took 25 years, etc[1].

These are inventions that most people in the developed world use every day and almost no-one can properly function without. And, still, it took those amazing and desperately useful inventions almost three decades to get out of their nurturing environment and achieve a decent percentage of market share.

TRL	Definition
1	Basic principles observed
2	Technology concept formulated
3	Experimental proof of concept
5	Technology validated in relevant environment (industrially relevant environment in case of key enabling technologies)
9	Actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies or in space)

The Implications

As the old proverb goes: **"great things just take time"**. Time, indeed, is what most new cybersecurity ideas are deprived of in the current European Commission funding scheme. Indeed, over the past few years research funding in the area of cybersecurity follows a completely different approach with respect to time: it favours short-term projects with immediate market application, high TRLs and rapid market exploitation. This approach effectively deprives cybersecurity ideas from the nurturing environments they need to grow and thrive in: these environments are dwindling, market-ready solutions do not leave enough space for new ideas to grow and new inventions just cannot reach maturity quickly enough.

We are afraid that such a short-term approach to cybersecurity is just not the proper environment for fundamental ideas which need an opportunity to grow and eventually a chance to change the world. We are afraid that, without such a nurturing network for new ideas, Europe will be forced to just import its cybersecurity technology from abroad – a practice which will have dire implications for Europe's long term digital sovereignty.

Policy Recommendations

If EU-supported cybersecurity funding initiatives do not change, we will probably end up with an environment that is hostile to the development and fruition of new inventions. This will probably have an adverse impact on the European cybersecurity ecosystem, the development and fruition of novel inventions and eventually on European digital sovereignty. To reverse this trend, we have three policy recommendations:

1) **Develop new funding instruments to support blue-sky research in the area of cybersecurity**
Currently very few, if any, instruments exist to support blue-sky research in cybersecurity. We need a new FET-like or EIC Pathfinder-like programme completely dedicated to cybersecurity. Such programmes would support the entire range of cybersecurity projects ranging from hardware security all the way to application security. One might think that such instruments already exist (such as the European Research Council or Marie Skłodowska-Curie Actions) and that they are enough to cover cybersecurity along with the rest of the disciplines that they cover. However, the existing instruments provide only a small fraction to funding cybersecurity research. We need to step up on this, as cybersecurity is one of the very few areas of research that touches almost all aspects of life: from the mundane, such as the coffee maker not working, to the important, such as cars crashing because of faulty software, all the way to national security, such as an electricity grid going down during a time of crisis because of an advanced persistent threat that was maliciously planted by a third-party supplier.

2) **Support cybersecurity research projects with very low TRLs**
Existing funding instruments should support cybersecurity projects with a very low TRL. Indeed, current funding instruments request a medium to high TRL of 4 or 5 which is equivalent to technology implemented and validated in a relevant environment. This deprives all low TRL inventions from the opportunity to receive funding. Without support for very low TRLs, it's unlikely that new algorithms will be created or new systems developed from scratch. And without new algorithms and new systems, we would not be able to pave the way to real ground-breaking innovation. One might think that funding for new algorithms and new systems as well as their testing and validation falls outside the scope of EU support, which is a valid point. But it does not solve the problem. It just takes us back to square one. Fundamental low TRL new ideas will not be funded by the EU and without funding they are less likely to be created, at least on European soil. They will more likely be invented (and possibly patented) in non-EU countries and imported back to Europe perpetuating the endless loop. Europe keeps importing its cybersecurity because Europe does not fund low TRL research that will develop the required technology.

3) **Provide funding for cybersecurity research projects that last more than five years**
Most existing calls for proposals provide funding for projects that are relatively short: two to three years long. This is shorter than the time it takes for a PhD to complete. Indeed, a PhD often takes five to six years at leading universities, although it can be even seven to eight years in most US universities[2]. A typical EU-funded project lasts for half or even a third of the duration of a PhD. Such short-lived projects just do not have the time necessary to catalyse the creation of fundamentally new inventions that start from a very low TRL. Some European countries, such as the Netherlands, have already realised this problem and have started funding projects that last five or even six years.

References

1 Hanna, R., Gross, R., Speirs, J., Heptonstall, P., & Gambhir, A. (2015). Innovation timelines from invention to maturity: A rapid review of the evidence on the time taken for new technologies to reach widespread commercialisation. UKERC Technology and Policy Assessment, December.

2 Betsy Bizot. Time to degree in computing, https://cra.org/crn/2014/04/time_to_degree_in_computing/

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Evangelos Markatos markatos@ics.forth.gr

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.