NGI THINK NEXUS

Policy Brief 5

Cybersecurity: a common challenge that requires transnational collaboration

December 2020

Policy Brief writen by:
Think NEXUS Innovation & Entrepreneurship Expert Group

Main contributors:
Vasilis Papanikolaou (ATC SA), Florence D. Hudson (Founder and CEO, FDHint)

THINK NEXUS

Think NEXUS, an EC-funded project, aims at reinforcing EU-US collaboration on NGI-related topics in three focus areas: Science and Technology, Innovation and Entrepreneurship and Policy. The aim is to boost strategic research, industrial partnerships and policy compliances in order to gain socio-economic benefits in both the EU and US regions.

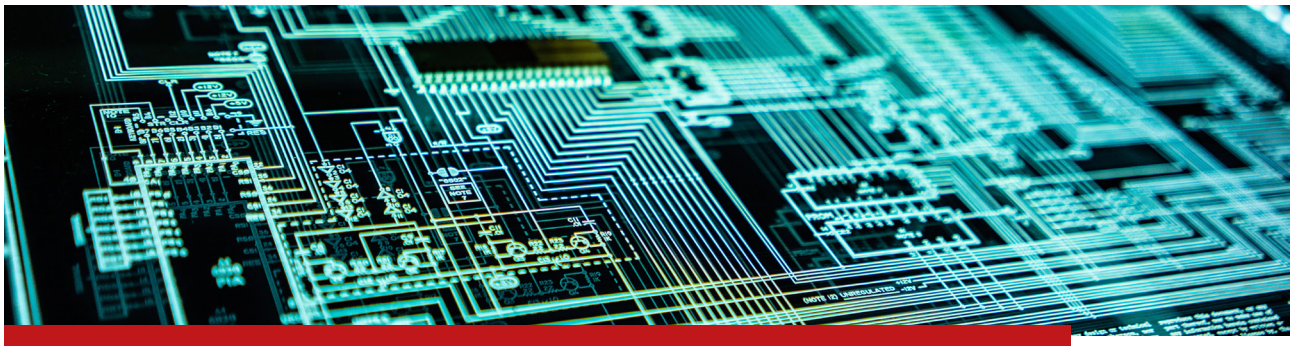
In the framework of this project, we are regularly publishing several short articles aiming at comparing the US and the EU approaches in different topics of NGI. The present document is focusing on Artificial Intelligence.

THI

NK

NEX

US



Cybersecurity: a common challenge that requires transnational collaboration

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Personal data that could result in identity theft is now posted to the public on our social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

The fact of the matter is whether you are an individual, small business, large multinational or even a government, you rely on computer systems every day. Pair this with the rise in cloud services, poor cloud service security, smartphones and the Internet of Things (IoT) and we have a myriad of cybersecurity threats that didn't exist a few decades ago[1]. Governments around the world are bringing more attention to cybercrimes. GDPR in Europe is a great example while all 50 US states have their own data breach legislation.

In September 2018, the U.S. White House released the National Cyber Strategy[2], which reinforces ongoing work and provides strategic direction for the Federal Government to take action on short and long-term improvements to cybersecurity for the government, private sector, and individuals. The National Cyber Strategy recognizes that private and public entities have struggled to secure their systems as adversaries have increased the frequency and sophistication of their malicious cyber activities, and directs the Federal Government to do its part to ensure a secure cyber environment for the country.

Following the Strategy, the R&D budget for Cybersecurity has been increased both for 2019 and for 2020[3], for the Networking and Information Technology Research and Development Program (NITRD), the Department of Energy (DoE), the Cybersecurity Infrastructure Security Agency (CISA), etc. The FY 2020 President's Budget includes $17.4 billion of budget authority for cybersecurity-related activities, a $790 million (5 percent) increase above the FY 2019 estimate. Due to the sensitive nature of some activities, this amount does not represent the entire cyber budget.

1 https://www.upguard.com/blog/cybersecurity-important

2 National Cyber Strategy, September 2018

3 Federal Research and Development (R&D) Funding: FY2020, Updated November 26, 2019

The DOD was the largest contributor to the budget authority for cybersecurity-related activities submitted in the President's Budget with $9.6 billion in cybersecurity funding in FY 2020[4] .
The European Commission has also placed cybersecurity high on the agenda in its proposals for the next long-term EU budget for years 2021-2027, to guarantee adequate funding for this key priority. Under the new Digital Europe programme the European Commission proposes to invest EUR 2 billion into safeguarding the EU's digital economy, society and democracies through polling expertise, boosting EU's cybersecurity industry, financing state-of-the-art cybersecurity equipment and infrastructure. Cybersecurity research and innovation will additionally be supported under the Horizon Europe programme[5].

The cybersecurity challenge has been profoundly acknowledged from both sides of the Atlantic, while Science & Technology efforts are taking place from a number of research intensive organisations, institutes and stakeholders. However, joint efforts should be made in order to reach to innovative technologies in a more rapid way, always for the benefit of the people. Emphasis should be given in the following topics[6] :

- Promote robust, safe, secure, inclusive and ethical Artificial intelligence where humans can understand the rationale and trust the results.
- Support the development of Quantum Key Distribution geographical high-speed networks (by using satellite and terrestrial links) for high security communications.
- Promote the standardization of secure and interoperable interfaces among critical infrastructures to prevent cascading effects.
- Help the development and sharing of independent evidence-based cyber threat intelligence and understand the trends through historical data.
- Promote and diffuse Privacy Enhancing Technologies (PETs) across different components (e.g. big data, cloud, IoT) and through application domains (e.g. healthcare, transportation, energy)

4 Analytical Perspectives, Budget of the United States Government, Fiscal Year 2020

5 https://ec.europa.eu/digital-single-market/en/cyber-security

6 ENISA, Analysis of the European R&D priorities in cybersecurity Strategic priorities in cybersecurity for a safer Europe, 12/2018

NGI THINK NEXUS

thinknexus.ngi.eu @ThinkNEXUS_NGI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825189. This publication reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains