D3.3 – Policy Briefs
Repertoire – Science + Technology

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement nº 825189. This document reflects only the author’s view and the Commission is not responsible for any use that may be made of the information it contains.
### D3.3 Policy briefs repertoire – Science + Technology

<table>
<thead>
<tr>
<th><strong>Project Title</strong></th>
<th>Think tank for the collaboration on NEXt generation internet between EU-US</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Acronym</strong></td>
<td>Think NEXUS</td>
</tr>
<tr>
<td><strong>Grant Agreement No</strong></td>
<td>825189</td>
</tr>
<tr>
<td><strong>Instrument</strong></td>
<td>Coordination &amp; Support Action</td>
</tr>
<tr>
<td><strong>Topic</strong></td>
<td>Industrial Leadership / Next Generation Internet</td>
</tr>
<tr>
<td><strong>Start Date of Project</strong></td>
<td>1st November 2018</td>
</tr>
<tr>
<td><strong>Duration of Project</strong></td>
<td>30 Months</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Name of the deliverable</strong></th>
<th>Policy briefs repertoire – Science + Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of the deliverable</strong></td>
<td>D3.3</td>
</tr>
<tr>
<td><strong>Related WP number and name</strong></td>
<td>WP3 - Think NEXUS Community Building and Expansion</td>
</tr>
<tr>
<td><strong>Related task number and name</strong></td>
<td>Task 3.1 Think NEXUS Stakeholder Management</td>
</tr>
<tr>
<td><strong>Deliverable dissemination level</strong></td>
<td>Public</td>
</tr>
<tr>
<td><strong>Deliverable due date</strong></td>
<td>30/11/2020</td>
</tr>
<tr>
<td><strong>Deliverable submission date</strong></td>
<td>30/11/2020</td>
</tr>
<tr>
<td><strong>Task leader/Main author</strong></td>
<td>Maritini Kalogerini, Antonis Ramfos (ATC)</td>
</tr>
<tr>
<td><strong>Contributing partners</strong></td>
<td>AUSTRALO</td>
</tr>
<tr>
<td><strong>Reviewer(s)</strong></td>
<td>Fabrice Clari (GAC)</td>
</tr>
</tbody>
</table>

**Abstract**

This deliverable gathers the collection of policy briefs by Think NEXUS Science & Technology Expert Group, that have been published.

**Keywords**

Next Generation Internet; EU-US collaboration; Technology, Blockchain, Big Data, NGI, Cybersecurity, Ethics
Revisions

<table>
<thead>
<tr>
<th>Version</th>
<th>Submission date</th>
<th>Comments</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>v0.1</td>
<td>15/11/2020</td>
<td>Table of content</td>
<td>Maritini Kalogerini (ATC)</td>
</tr>
<tr>
<td>v0.2</td>
<td>26/11/2020</td>
<td>Contribution</td>
<td>Antonis Ramflos (ATC)</td>
</tr>
<tr>
<td>v0.3</td>
<td>29/11/2020</td>
<td>Contribution</td>
<td>Jose Gonzalez (AUS)</td>
</tr>
<tr>
<td>v0.4</td>
<td>30/11/2020</td>
<td>Quality review</td>
<td>Fabrice Clari (GAC)</td>
</tr>
<tr>
<td>v1.0</td>
<td>4/12/2020</td>
<td>Final Version</td>
<td>Maritini Kalogerini (ATC)</td>
</tr>
</tbody>
</table>

Disclaimer

This document is provided with no warranties whatsoever, including any warranty of merchantability, non-infringement, fitness for any particular purpose, or any other warranty with respect to any information, result, proposal, specification or sample contained or referred to herein. Any liability, including liability for infringement of any proprietary rights, regarding the use of this document or any information contained herein is disclaimed. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by or in connection with this document. This document is subject to change without notice. Think NEXUS has been financed with support from the European Commission. This document reflects only the view of the author(s) and the European Commission cannot be held responsible for any use which may be made of the information contained.
## Acronyms and definitions

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>ITA</td>
<td>International Trade Administration</td>
</tr>
<tr>
<td>NGI</td>
<td>Next Generation Internet</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>SME</td>
<td>Small and medium-sized enterprise</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>US/ U.S./ USA</td>
<td>United States of America</td>
</tr>
</tbody>
</table>
The Internet of the future should be more open, provide better services, more intelligence, greater involvement and participation. It needs to reflect the European values”. EU’s Next Generation Internet initiative is a key opportunity to rethink the way the Internet works today and develop a vision involving voices from across Europe, the US, and beyond, an Internet that embodies the values Europe holds dear, such as openness, inclusivity, transparency, privacy and cooperation.

Thinking globally, the NGI will be successful only if a worldwide consensus is found, enabling the internet a Human-centric process. To that end, collaboration between the EU and the US is essential, both areas being strongly committed to develop the future of Internet, to shape a sustainable landscape for NGI developments. Indeed, the NGI initiative should design specific actions for policy collaboration, shared technology development and interaction between user-communities, with other initiatives in the world where parts of the NGI infrastructure are designed and deployed; and the US are one of the main places where such activities are held.

Think NEXUS aims to reinforce EU-US collaboration, through its dedicated think tank, involving major stakeholders (researchers, entrepreneurs, policy makers) from both sides of the Atlantic on NGI-related thematic in three Focus Areas: Science and Technology, Innovation and Entrepreneurship and Policy. Its mission is to become an important and lasting entity, involving stakeholders and disseminating NGI visions in a collaborative approach for tackling NGI challenges, and benefit society at large. More specifically, Think NEXUS is expected to boost the strategic research, industrial partnerships and policy compliances among the respective communities of the NGI areas and thus, result in substantial socio-economic benefits in both the EU and US regions.
Table of Contents

Executive Summary ................................................................................................................. 8
1. Objectives .......................................................................................................................... 9
   1.1. Policy Briefs - Introduction ......................................................................................... 9
2. List of Publications/Policy Briefs ...................................................................................... 10
3. Policy Briefs ....................................................................................................................... 14
   3.2. Policy Brief 2: Blockchain and Big Data analytics for eHealth: A topic for collaboration between EU and US 15
   3.3. Policy Brief 3: NGI technologies for Natural Hazard Prediction and Emergency Management: a fertile field for collaboration between EU and US in Science and Technology ................................. 16
   3.4. Policy Brief 4: Cybersecurity: a common challenge that requires transnational collaboration 17
   3.5. Policy Brief 5: AI Ethics: A challenge or an opportunity? ........................................ 18
4. Next Steps ........................................................................................................................ 19
List of Figures

Figure 1 - Design & final format of policy briefs-documents.................................................................9

List of tables

Table 1 – Publication #1 ................................................................................................................................10
Table 2 – Publication #2 ................................................................................................................................10
Table 3 – Publication #3 ................................................................................................................................11
Table 4 – Publication #4 ................................................................................................................................12
Table 5 – Publication #5 ................................................................................................................................12
Executive Summary

The main aim of Think NEXUS project is to bring EU-US policy makers and the public closer to the core of the programme and facilitate a better understanding of key issues, as well as to share insights and recommendations, set out by the members of the Expert Groups. A plan has been established in order to edit and release a collection of publications addressing relevant topics to the scope of each expert group. This delivery report gathers 5 different policy briefs – as short publications that present outcomes from research topics - which are focused on different technological dimensions, under the umbrella of Science and Technology Expert Group. The topics of the policy briefs of each group, align with the main concerns defined for the think tank in the series of deliverables that are mentioned bellow, outlining the strategy throughout the project lifetime.

The first policy brief analyzes the need for EU-US collaboration to deal with emerging national security threats to and counterterrorism in Social Media, Surface & Deep Web. The second policy brief, notes the necessity for creation of integrated applications, that could allow an interoperable exchange of vast amount of health data among health oriented entities across Europe and the US. The third policy brief underlines the need of transatlantic collaboration of Science and Technology communities to exploit the key NGI technologies for disaster and crisis management. Moreover, the fourth policy brief refers to the need of transatlantic Cybersecurity innovative technologies. The final policy brief that is described in this document, underlines the need for policy makers to seek convergence on the ethical principles of AI, and on the actual implementation of these principles, as well.
1. Objectives

One of the most important objectives aimed by Think NEXUS is to share and spread out insights and recommendations set out by the members of the Expert Groups, comparing the European perspective against the context of the United States, but also conveying into principles and keystones shared by both regions. To that end, the project established a plan to edit and release a collection of publications addressing topics relevant to the scope of each group, aligning with the priorities defined for the think tank in the series of deliverables outlining the strategy throughout the project lifetime - i.e. D1.2 (v1, January 2019), D1.3 (v2, October 2019) and D1.4 (v3, July 2020). The series of deliverables D3.3, D3.4 and D3.5 assemble the repertoires/compendium of these publications, covering the research lines of Science & Technology, Innovation & Entrepreneurship, and Policy Expert Groups respectively. The types of publications considered in this scope are ‘Policy Briefs’, whose specifics are detailed below.

1.1. Policy Briefs - Introduction

Policy briefs present a concise summary of information that can help readers understand, and likely make decisions about, government policies. These are short publications that present findings and recommendations of a single research topic to government policymakers and other stakeholders interested in formulating or influencing policy. Policy briefs may give objective summaries of relevant research, suggest possible policy options, or go even further and argue for particular courses of action.

Think NEXUS targets advocacy briefs directed to the Next Generation Internet Unit. The ambition is to identify common points between EU and the USA, in critical features affecting the NGI vision and approach and strategy.

Think NEXUS partners have decided on Policy Briefs' format, following the guidelines bellow:

- Format: A4 sheets, containing between 2 and 4 pages of content (without template overheads)
- Edition: Coordination by Expert Group chairs, with potential contribution from experts
- Design: Common format, defining an attractive and professional style, including graphical material

1 The writing center, University of North Carolina, https://writingcenter.unc.edu
2. List of Publications/Policy Briefs

**Table 1: Publication #1**

<table>
<thead>
<tr>
<th>Title</th>
<th>Surveillance and Analytics in the Deep Web: A Priority for Collaboration in AI and Cybersecurity between EU and the US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Policy Brief</td>
</tr>
<tr>
<td>Date</td>
<td>May 2020</td>
</tr>
<tr>
<td>Experts</td>
<td>Vasilis Papanikolaou (ATC SA), Florence D. Hudson (Founder and CEO, FDHint)</td>
</tr>
<tr>
<td>Bookmark</td>
<td>Chapter 3.1</td>
</tr>
</tbody>
</table>

**Rationale**

Although digital technology can offer numerous benefits to citizens, it can be turned against society when malicious potential of the internet is created, especially by terrorist and extremist digital media.

This ‘policy brief’ analyzes the necessity for collaboration, between scientific and technological stakeholders from both the EU and the US, in order to face emerging national security threats. Law Enforcement Agencies (LEAs) are proposed as means, able to deal with counterterrorism in Social Media, Surface & Deep Web. Terrorism on the Internet is a multifaceted and dynamic phenomenon.

There is a need for creation and constant evolution of standard methodologies and protocols for understanding detecting, retrieving, collecting and analysing malicious content. Several global groups, such as the International Institute for Electrical and Electronic Engineers (IEEE), can be set as a base to build collaboration, in order to face critical cybersecurity and AI challenges.

**Table 2: Publication #2**

<table>
<thead>
<tr>
<th>Title</th>
<th>Blockchain and Big Data analytics for eHealth: A topic for collaboration between EU and US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Policy Brief</td>
</tr>
<tr>
<td>Date</td>
<td>June 2020</td>
</tr>
<tr>
<td>Experts</td>
<td>Think NEXUS Science &amp; Technology Expert Group</td>
</tr>
<tr>
<td>Bookmark</td>
<td>Chapter 3.2</td>
</tr>
</tbody>
</table>
Rationale

More and more health oriented entities across Europe and the US generate data in a non-cohesive and standardized way. The policy brief ‘Blockchain and Big Data analytics for eHealth: A topic for collaboration between EU and US’, notes the necessity for creation of integrated applications, that could allow an interoperable exchange of vast amount of health data, across all regions. Interoperability, harmonization as well as data privacy and security are the main pillars in order to unlock the full potential of eHealth innovation, via blockchain-based research activities.

Table 3: Publication #3

<table>
<thead>
<tr>
<th>Title</th>
<th>NGI technologies for Natural Hazard Prediction and Emergency Management: a fertile field for collaboration between EU and US in Science and Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Policy Brief</td>
</tr>
<tr>
<td>Experts</td>
<td>Vasilis Papanikolaou (ATC SA), Jonathan Fink (Director of Digital City Testbed Center, Portland State University)</td>
</tr>
<tr>
<td>Bookmark</td>
<td>Chapter 3.3</td>
</tr>
</tbody>
</table>

Rationale

Knowing that disasters - as serious disruption of society’s functioning - have become common occurrences globally, there is a need for efficient disaster and crisis management. Over the last few years, social media - generated data, analytics and millions of bytes of geotagged information can bring up unseen geographical patterns of crowd reactions, when this data is analyzed from domain specialists, attributing to significant crisis management.

This Policy Brief underlines the need of collaboration of EU and US Science and Technology communities, that could exploit the key NGI technologies (analytics, AI, 5G etc.) towards the creation of tools for disaster and crisis management.
### Table 4: Publication #4

<table>
<thead>
<tr>
<th>Title</th>
<th>Cybersecurity a common challenge that requires transnational collaboration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td><strong>Policy Brief</strong></td>
</tr>
<tr>
<td>Date</td>
<td>November 2020</td>
</tr>
<tr>
<td>Experts</td>
<td>Vasilis Papanikolaou (ATC SA), Florence D. Hudson (Founder and CEO, FDHint)</td>
</tr>
<tr>
<td>Open Access</td>
<td>Not available yet</td>
</tr>
<tr>
<td>Bookmark</td>
<td>Chapter 3.4</td>
</tr>
</tbody>
</table>

#### Rationale

This Policy Brief refers to the challenge of transnational Cybersecurity. The fact that vast amounts of sensitive data are now stored in controversial cloud services, appears myriad of cybersecurity threats. Many initiatives provide strategic direction for making improvements to cybersecurity, while budget for relevant R&D fields has been increased. Moreover, the European Commission promotes cybersecurity in its proposals for the upcoming years, even for EU and the US collaboration. Joint efforts should be made in order to reach Cybersecurity innovative technologies more quickly and in the following policy brief specific topics are proposed for efficient collaboration.

### Table 5: Publication #5

<table>
<thead>
<tr>
<th>Title</th>
<th>AI Ethics: A challenge or an opportunity?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td><strong>Policy Brief</strong></td>
</tr>
<tr>
<td>Date</td>
<td>November 2020</td>
</tr>
<tr>
<td>Experts</td>
<td>Danai Tsampouraki (ATC)</td>
</tr>
<tr>
<td>Open Access</td>
<td>Not available yet</td>
</tr>
<tr>
<td>Bookmark</td>
<td>Chapter 3.5</td>
</tr>
</tbody>
</table>

#### Rationale

Increasing AI applications may pose great societal risks in addition to technological change and its impact on individual lives. It already applies in many sectors either as standalone applications or embedded in more complex systems. As a result, the wide spectrum of human activity covered by AI ranges from drones, videos of real people saying things they never said, to law enforcement and behaviour or emotion detection systems. Bias in AI, most often unintentional, may be inserted in all stages of an algorithm and lead to critical decision errors (e.g. in law enforcement systems). Emotional AI machines raise serious concerns over data
protection and privacy and often operate in the background, without users even knowing that AI is used. This may in turn lead to other situations where AI systems are used to manipulate democratic processes and influence voting decisions (e.g. in the case of Cambridge Analytica). There is also the danger of the “black box society”, where even the people behind the creation and operation of AI systems won’t be able to understand every step of the process and explain the algorithm’s specific decisions, let alone end users of these systems or policy makers, resulting in serious concerns raised about the transparency, explainability, responsibility and liability of AI systems. Generally and despite all EU initiatives, ethics components in AI policy still falls under a soft regulation approach. Policy makers need to seek convergence not only on the ethical principles of AI but also on the actual implementation of these principles through processes, broad stakeholder engagement, open public debates and forums, as well as early societal involvement and intervention in research and innovation processes. Furthermore, multicultural and transdisciplinary research and innovation environment must be encouraged, along with education and public discussion for broader ethical and philosophical questions concerning AI.
3. Policy Briefs

Policy Brief 1

Surveillance and Analytics in the Deep Web:
A Priority for Collaboration in AI and Cybersecurity between EU and the US
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.
Digital technology has transformed the lives of ordinary citizens as this new digital world can offer amazing life altering benefits.

Yet the real strengths of the internet for the citizen are also the very features that can be turned against the citizen by those wishing to instil terror in hearts and minds. A particular concern is that extremists and terrorists are using digital media to communicate, collaborate, recruit, plan campaigns, spread their messages, and persuade. As a result, the malicious potential of the internet has become a primary concern for governments, which constantly try to enhance their ability to respond to new and emerging national security threats in the constantly changing digital era.

The role of technology is becoming crucial in policing activities, as it provides Law Enforcement Agencies (LEAs) with a set of tools able to strengthen their analytical and investigative skills and expand their capacity to handle huge amounts of data, derived from monitoring and surveillance operations. This is particularly true when dealing with counterterrorism (CT), as intelligence agencies are required to put greater attention on tracking terrorist financing, monitoring propaganda activities and the dissemination of training materials, both on the Surface and Deep/Dark Web/Net – among other priorities.

However, LEAs use different tools and commercial products, while having different capabilities, expertise, skills and resources and dealing with varying forms of terrorism. Thus they need a generic platform that promotes standard methodologies for understanding content and estimating risk, yet that is sufficiently flexible that it can be customised to the specific needs of each end-user.

The need for constant evolution of methodologies and protocols is not only driven by advances in technology, but also from the fact that terrorism on the Internet is a very complex and dynamic phenomenon: The rhetoric promoting terrorism and radicalisation constantly evolves, along with the ways this rhetoric is presented to like-minded people.

1 https://www.h2020-dante.eu/
Those responsible for terrorist and extremist websites are increasingly aware that they are being monitored, and are turning to means that are more difficult to be monitored, such as the **Dark Web** and **social media**. The implications of this evolution are significant. Today on-line terrorist content is vast, and accessed by millions of people. Accurate **detection of terrorist and extremist rhetoric** among this sea of content, through efficient and effective automated techniques, is a necessity.

A global effort we can leverage is led by the International Institute for Electrical and Electronic Engineers (IEEE), which has been developing a TIPPSS framework since 2016 promoting increased vigilance in Trust, Identity, Privacy, Protection, Safety, and Security. Numerous books and articles have been written on this subject, including “Enabling Trust and Security: TIPPSS for IoT”\(^2\), “Wearables and Medical Interoperability: The Evolving Frontier”\(^3\), and a book by women in the US and EU “Women Securing the Future with TIPPSS for IoT”\(^4\).

There are global working groups on this topic, and conferences including a TIPPSS for IoT workshop in the Security and Privacy Track of the IEEE World Forum for IoT in New Orleans, Louisiana April 6-8, 2020. These global groups tackling critical cybersecurity and AI challenges are a great base to build ongoing collaboration and progress.

A collaboration between scientific and technological stakeholders from both the European Union and the United States of America is necessary. The need of joint development of an effective framework supported by **AI**\(^5\), **data mining and big data analytics functionalities**, capable of detecting, retrieving, collecting and analysing data of suspicious terrorist raising funds, propaganda and training activities within the surface, the dark and the deep web, could be of high priority.

---

5. ENISA, Analysis of the European R&D priorities in cybersecurity Strategic priorities in cybersecurity for a safer Europe, December 2018
3.2. Policy Brief 2: Blockchain and Big Data analytics for eHealth: A topic for collaboration between EU and US
Policy Brief 2

Blockchain and Big Data analytics for eHealth:
A topic for collaboration between EU and US
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.
Blockchain and Big Data analytics for eHealth: A topic for collaboration between EU and US

Vast amounts of health data are now produced, gathered and stored in electronic health records (EHRs) in multiple formats, during citizens’ medical examinations both across Europe and the US. This is largely a result of the explosion of available technological devices and medical services, which are nowadays used by citizens. Citizens and health-oriented entities generate data but the data do not flow among these entities in a seamless, cohesive and standardized way. Rather, healthcare involves a diverse set of public and private data collection isolated systems (“silos”), including health surveys, administrative enrolment, billing records, and medical records, used by various entities such as hospitals, medical doctors, health authorities, pharmacies or even citizens in different countries and regions.

Currently there is no easy and standard way or capability to gather data about citizens from these silos. The fragmented landscape is a serious set-back against deploying integrated applications that could provide better and more accurate diagnosis, aid faster research outcomes and more. The prospects of integrated health data raise the need for better integration and sharing of data within and across healthcare systems, organisations and countries.

However, most of the healthcare services and entities operate independently and use heterogeneous systems for managing health data, which makes it difficult to obtain and integrate information from different sources in the healthcare domain. Thus, opportunities to reuse this data for research and better healthcare are often missed due to the lack of data interoperability and complexity of dealing with different systems or data silos, as well as lack of standardized processes for data anonymization which would allow data sharing with respect to users’ privacy.

In addition to the technical challenges of integrating health data, the sensitive nature of the data raises many security and privacy concerns about its processing, storage and utilisation. Recent security (e.g. NHS ransomware attack in 2017\(^1\) and privacy (e.g. exploitation of personal information by Cambridge Analytica in 2018\(^2\) ) scares have raised the general awareness about the protection and privacy of data. Moreover, a broad range of new healthcare technologies

---

1 NHS cyber-attack: Everything you need to know about ‘biggest ransomware’ offensive in history, Available at: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

2 Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, Available at: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
(e.g. mobile applications and wearables) threaten to break apart the protections of existing regulations and expose the long-existing gaps in individual rights.

Therefore, any approach for data integration and management would need to be open and transparent in terms of the security and privacy mechanisms that are being put in place in order for citizens to willingly entrust the approach. Likewise, it should be compliant to the emerging GDPR (established in the EU, but already having global impact), which remedies several security, privacy and data protection concerns. However, healthcare companies are notorious for their limited investments in security, as highlighted in the 2016 HIMSS Analytics Healthcare IT Security and Risk Management Study.

For example, the US federal government spends 16% of its IT budget on security, while ABI Research estimates that investments in the industry against cyber-attacks will only reach $10 billion worldwide by 2020. Another issue currently faced by healthcare organizations is that they have sensitive data spread across a number of devices, not just servers and desktops but also laptops, mobile devices, and specialized devices for inputting medical record data. According to Healthcare Breach Report, 68% of all healthcare data breaches since 2010 were due to device theft or loss, which basically addresses the citizen-generated data.

To unlock the full potential of eHealth innovation and recent extremely fast developments, while curtailing potential negative consequences and practices, effort must be invested in standardisation and harmonization, data privacy and security. These efforts should enable citizen empowerment, since healthcare reliance has changed from an isolated system to a critical infrastructure. Interoperability and security measures must support the secure data exchange and utilisation across the interconnected health system, while facilitating citizens contributions (through ethical sourcing of the user generated social and quantified-self data) and ensuring transparency.

Collaboration between EU and US stakeholders is critical. Focus should be given in co-developing technologies and applications that will allow an interoperable exchange of health information across regions based on a citizen-centric approach that provides citizens (and other data providers) with full control over their personal data. In this direction, research activities should be focusing on blockchain as a key underlying infrastructure ensuring that data contribution, sharing, exchange, use and processing will follow citizens consent and needs to be fully secure and optimized for different stakeholders in the healthcare ecosystem that will be authorized to access them: citizens, hospitals, medical doctors, health professionals and pharmacies.

3 Federal Spending: Where Does the Money Go, Available at: https://www.nationalpriorities.org/budget-basics/federal-budget-101/spending/


Policy Brief 3

NGI technologies for Natural Hazard Prediction and Emergency Management: a fertile field for collaboration between EU and US in Science and Technology

May 2020
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.
NGI technologies for Natural Hazard Prediction and Emergency Management: a fertile field for collaboration between EU and US in Science and Technology

As stated by the United Nations Office for Disaster Risk Reduction (UNDRR), a disaster can be defined as “a serious disruption of the functioning of a community or society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope with using its own resources.” In the last few decades, societies have become increasingly aware of the fact that disasters can be analysed as the result of long-term processes; whereby the risk is created years or decades before the disaster manifests itself.

There are indications that in recent years’ disasters such as super typhoons, floods, droughts, wildfires, etc. have become common occurrences globally. In 2017 alone, 335 natural disasters affected over 95.6 million people, killing an additional 9,697 and costing a total of $335 billion. More specific, in 2018 the United States experienced 14 disasters that cost the economy as much or more than $1 billion dollars each. But the total cost of these hurricanes, wildfires, floods and other disasters that struck the U.S. last year is about $91 billion, according to the U.S. National Oceanic and Atmospheric Administration, which tracks U.S. weather and climate events that have great economic and societal impacts.

In Europe only in 2018, The European Forest Fire Information System (EFFIS), reported that wildfires have heavily affected Sweden, UK, Ireland, Finland and Latvia; countries in which wildfires have not been a concern in past years. These effects can also reach long distances. In summer 2018, the normally clean air quality of Seattle WA in the U.S. became the worst in the world due to smoke from distant wildfires. Similarly, flooding has been occurring in places where it was not observed before such as regions around the Dead Sea in Jordan. Further complicating response to these individual occurrences, cascading disasters like 2012’s combined Tohoku earthquake, tsunami, and nuclear power plant meltdown have also become more common.

Disaster and crisis management have become more important than ever with both the public and private sectors pitching in solutions to stay ahead of the problem. To that end, social media (SM) analytics has become prominent in natural disaster management. In spite of a large variety

1 http://www.un-spider.org/risks-and-disasters
3 https://www.cnbc.com/2019/07/10/billion-dollar-natural-disasters-rising-these-states-better-prepare.html
of metadata fields in social media data, four dimensions (i.e. space, time, content and network) have been given particular attention for mining useful information to gain situational awareness and improve disaster response. In recent years, there has been a spurt of interest and much research into the role of social media in disaster management. Rather than as a means of communicating hazard, risk, and disaster perceptions and warnings, SM-generated data like Facebook posts and Twitter feeds are sought to be analysed to arrive at the scale and spread analysis of disasters. This data is voluminous, different, and when used in new ways to monitor and manage a disaster, qualifies for the definition of Big Data and its five Vs (volume, velocity, variability, veracity, and variety).

The data shadows on the internet of Facebook likes, Flipkart orders, Google searches, Research Index citations, Tumblr pictures, You Tube videos—all add up to billions of bytes of information, most of which are geotagged, and which, if tweaked properly can bring up hidden, but critical geographical patterns of crowd responses. Big Data snared in the geoweb can be of critical importance in big disaster events, if its analysis is mellowed by domain experts.

Following the outcomes of the EU-US Climate Alliance forum that took place in Washington, DC on 8 November 2019, the European and the American Science and Technology community should collaborate towards exploiting the key NGI technologies, such as Big Data (analytics), AI, and 5G, for the benefit of the people from both regions, by providing a new arsenal of tools that matches the speed with which disasters occur and thus aids in very quick decision-making.

The rise of social media usage is now at its peak as they are used in all sectors right from individual citizens to non government organizations, private sectors, government stakeholders, and volunteering organizations for aiding in information communication or knowledge transfer during disaster situations. The power of SM has spanned new fields of research, which harness the power to arrive at instantaneous decisions which are needed in disaster situations.

---


3.4. Policy Brief 4: Cybersecurity: a common challenge that requires transnational collaboration
Cybersecurity: a common challenge that requires transnational collaboration

by

Think NEXUS Science & Technology Expert Group

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

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. 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, 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, 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. 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.

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

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


\(^6\) ENISA, Analysis of the European R&D priorities in cybersecurity Strategic priorities in cybersecurity for a safer Europe, 12/2018
3.5. Policy Brief 5: AI Ethics: A challenge or an opportunity?
AI Ethics: A challenge or an opportunity?

Danai Tsampouraki (ATC)

The plethora of policy initiatives, documents, and recommendations related to AI ethics indicates that there is a widely shared belief that AI applications will raise – and are already raising – complex ethical challenges that, if not addressed correctly, may pose great societal risks. After all, AI ethics is not solely about technological change and its impact on individual lives, but also about societal, economic, and cultural transformations and the future of our societies.¹

Even if general or human AI has not been achieved yet, and for some it may never happen in practice, narrow AI is already here and is pervasive, with applications in many sectors, including manufacturing, transportation, agriculture, healthcare, science, education, finance, human resources management, security, entertainment, and marketing. These applications are sometimes visible, as in the case of autonomous cars or cancer diagnostic systems, but, more often than not, they are hidden as parts of larger, more complex systems. Increasingly, different technologies with applications that cover a wide spectrum of human activity will have some AI components embedded in their systems. This is already happening with drones that use AI, AI conversational agents, AI in the workplace used as part of HR systems, AI that writes articles or AI systems that generate synthetic images and videos of real people, often making them look like saying or doing things they never did. AI is already used in decision making processes in courts, for example the COMPAS system in the US and the HART system in the UK have been used to predict those likely to re-offend. AI is also heavily used for law enforcement purposes, such as predictive policing, facial recognition technologies, behaviour detection, and detection based on biometric data.² AI is also permeating more personal and intimate aspects of our life, such as machines that can read our faces and emotions or online dating apps that use AI for matchmaking.

These AI applications raise ethical and legal concerns and create real world risks that directly affect both individual lives and collective societal processes. Bias in AI, most often unintentional, may be inserted in all stages of design, testing, and application of an algorithm. In law enforcement applications for example, research has shown that the use of the COMPAS system has already led to false positives and false negatives,³ reinforcing existing biases and unjust discrimination already present in our societies and thus our data. So bias seems to be ubiquitous in our world and societies, suggesting that AI models will never be totally bias free; although there are still things we can do to minimise bias and take quick corrective measures.⁴

¹ Mark Coeckelbergh, AI Ethics (Cambridge, MA, USA: The MIT Press, 2020).
The use of facial recognition systems and so called emotional AI enables machines to identify us and read our emotions, collect our biometric data, predict our mental, emotional, and physical status without even being noticed, raising serious concerns over data protection and privacy. These concerns are not new, but AI applications magnify the problem, as they collect and process much more personal data, often operating in the background, without users even knowing that AI is used. This may in turn lead to other situations where AI systems are used to manipulate democratic processes and influence voting decisions (e.g. in the case of Cambridge Analytica or social media bots propagating political disinformation).

The nature of some AI algorithms also raises the problem of the “black box society”, a term coined by Brooklyn Law School professor Frank Pasquale to express the notion of a networked society based on opaque, nontransparent algorithmic systems⁵. We may know how these algorithms work, but we don’t fully understand how they come to a particular decision, and thus we cannot fully explain this decision, albeit the impact the latter may have on an individual’s life. Current machine and deep learning applications are too complex in their automated decision making processes. There is the danger that even the people behind the creation and operation of AI systems won’t be able to understand every step of the process and explain the algorithm’s specific decisions, let alone end users of these systems or policy makers. These concerns raise the issue of transparency and explainability of AI systems; how can we make AI more transparent and explainable, and is this fully possible? The issue of algorithmic transparency or opacity is also closely connected with other issues, such as responsibility (an ethical concern over who should be responsible over automated decisions), liability (a legal concern about who should be held liable for unlawful consequences), and explainability (as a philosophical concern over the very nature of explanation and the human decision making process).

How many decisions, how much of these decisions, and what kind of decisions should be delegated to AI algorithms, especially if we can’t fully explain the decisions they make? Should we design AI systems to adhere to ethical requirements and if yes, which requirements and to what extent? Do we agree every time on the interpretation and real world implementation of ethical principles and how do we reconcile contesting ethical views? To what extent will we need or want to balance explainability, privacy, fairness with other considerations like financial benefits, innovation, and competiveness? Who shapes the future of AI?

The breadth of ethical questions and problems raised in the context of AI has highlighted the need to include ethics in the AI discourse. As such, a wide range of public and private policy initiatives around the world have included ethical aspects into their AI policies; for example, the European Commission set up in 2018 the High-Level Expert Group on Artificial Intelligence, which released a set of ethical guidelines towards developing trustworthy AI⁶. Others talk about explainable AI, while other ethical principles for AI include those of justice, fairness, sustainability, non-maleficence, freedom and autonomy. Although the HLEG AI and other relevant initiatives have formulated many ethics guidelines and some attempt to apply these guidelines through technical guidelines and processes, generally ethics components in AI

---

policy still tend to remain too vague in their implementation, fall under a soft regulation approach, and are distant from the actual technology environment and practices.\textsuperscript{7}

To better cope with the ethical challenges raised by AI, more proactive and radical policy responses need to be formulated that will enable us to effectively embed ethics guidelines in development and validation processes. To foster a culture of responsible AI innovation that integrates ethics by design and privacy by design approaches, policy makers need to **seek convergence not only on the ethical principles of AI but also on the actual implementation of these principles through processes.** It is also important that this process is as much democratic and inclusive as possible. To this end, a bottom-up approach should replace the current top-down approach in formulating policy recommendations. This can be achieved through **broad stakeholder engagement** that includes AI researchers, academics, and professionals, people affected by the applications of AI, and citizens; **open public debates and forums;** as well as **early societal involvement and intervention in research and innovation processes.** Although initiatives such as the European AI Alliance move towards this direction, it needs to be ensured that these efforts will actually reach the “lowest” levels and actively seek to engage communities like developers and end users of AI systems in their processes, as well as specific population groups that are affected by the use of the AI system in question.

Moreover, we need to **encourage a multicultural and transdisciplinary research and innovation environment** and to **foster ties to exchange knowledge and practices** with the US, but also with non-Western political and cultural systems that may have to offer us new approaches and alternative “AI lessons learned”. At the moment there seems to be little collaboration in international level and between the social sciences and the natural sciences when it comes to AI research and development, even within Europe. A more holistic approach requires the involvement of both social and natural sciences in R&D projects and the education of each side’s professionals on the other side’s main concepts. In other words, philosophers, psychologists, and lawyers need to learn how machine learning works, while software developers, data analysts, and system engineers need to understand the ethical and legal concepts concerning AI.

The matter of education is crucial in general. **More policy focus should be given on designing appropriate education concerning AI,** its uses, and applications in all levels of the society. From schools and universities to professionals in different industries, end users, scientists and policy makers, education should be tailored to the specific context, target group, and objectives of each case. **Algorithmic literacy should be generally enhanced** and people should be familiarized with the technological, ethical, and legal concepts around AI in order to be able to meaningfully participate in public debates and consultations.

Last but not least, to fully materialize the dynamic and possibilities of AI ethics we shouldn’t hesitate to **put up into debate broader ethical and philosophical questions** about what is important and valuable for us as individuals and our societies moving to the future and how can we transcript these concepts into AI applications. For example, should we try to design AI systems following the principle of non-maleficence, as in “you should not cause any harm”, or

\textsuperscript{7} For example, recent criticism of the EU’s approach towards AI focuses on the fact that the ethics guidelines for trustworthy AI fail to ensure the effective protection of human rights. See Access Now and European Digital Rights (EDRi), ‘Attention EU Regulators: We Need More than AI “Ethics” to Keep Us Safe’, EDRi <https://edri.org/our-work/attention-eu-regulators-we-need-more-than-ai-ethics-to-keep-us-safe/> [accessed 30 November 2020].
the principle of benevolence, as in “you should also do good things”? In the latter case, we also need to define what good means and for whom. A more positive approach towards ethics will therefore require not only to set ethical constraints on AI systems; but also to actively engage with broader ethical questions and collectively seek answers and ways to shape a vision of the future that reflects these notions.

---

4. Next Steps

Think NEXUS will update the collection of publications and text herein, with new releases until the project End. A second version of this deliverable will be released, including Policy Brief 4 and Policy Brief 5 final design. Also the Open Access links that are not available at the moment, will be updated.