NGI THINK NEXUS

Policy Brief 1

Surveillance and Analytics in the Deep Web:

A Priority for Collaboration in AI and Cybersecurity between EU and the US

Policy Brief writen by:
Think NEXUS Science & Technology
Expert Group

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

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

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[1].

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.

2 F. D. Hudson, "Enabling Trust and Security: TIPPSS for IoT," IT Professional, vol. 20, no. 2, pp. 15- 18, Mar./Apr. 2018, © 2018 IEEE, doi: 10.1109 MITP.2018.021921646, https://ieeexplore.ieee.org/document/8338006

3 F. Hudson and C. Clark, "Wearables and Medical Interoperability: The Evolving Frontier," in Computer, vol. 51, no. 9, pp. 86-90, September 2018, © 2018 IEEE, DOI: 10.1109/MC.2018.3620987, https://ieeexplore.ieee.org/document/8481273

4 F. D. Hudson, Editor, "Women Securing the Future with TIPPSS for IoT - Trust, Identity, Privacy, Protection, Safety, Security for the Internet of Things" © 2019, Publisher Springer International Publishing, Copyright Holder Springer Nature Switzerland AG, DOI 10.1007/978-3-030-15705-0, Hardcover ISBN 978-3-030-15704-3, https://www springer.com/us/book/97830301570

5 ENISA, Analysis of the European R&D priorities in cybersecurity Strategic priorities in cybersecurity for a safer Europe, December 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