(Biotechnology I Robotics I Artificial Intelligence I Nanotechnology I Space I Strategic Services)

BRAINS² TÜRKİYE* IMPLEMENTATION PROGRAM

SYNTHETIC REALITY TECHNOLOGY

"Building DeepFake Product and Defence Ecosystem"

deepware

SMART CITIES INNOVATION LAB

TASAM BGC
Business and Government Consultancy
İş ve Devlet Danışmanlığı

[BRAINS² Türkiye* Implementation Program]

Synthetic Reality Technology

"Building DeepFake Product and Defence Ecosystem"

(June 2019 - December 2022, Turkey)

---

* **BRAINS² TÜRKİYE** is a brand/initiative with multi-programs based in Turkey which develops market, ecosystem and capacity in the '**Biotechnology**', '**Robotics**', '**Artificial Intelligence**', '**Nanotechnology**', '**Space**' and '**Strategic Services**' fields. The programs planned through identical visions and strategies for each main fields which transforms the new business models and multidimensional power distribution in the global economy, are implemented under the common title of **BRAINS² TÜRKİYE**.

BRAINS² TÜRKİYE Programs, titled **"Building International Comparative Vision, Strategy, Ecosystem and Market"**, aims to explore and understand the technologies involved in Turkey's strategic agenda, within the scope of its current scientific and industrial strength/potential, to examine which of the domains in such technologies may promise the highest potential for future growth, and the **National Sectors** and their advantages that they may have from this growth. The new ecosystems, which is the subject matter of **BRAINS² TÜRKİYE** in this context, grow by ten billion dollars each year with the markets emerging in various domains, ranging from SMEs to main contractors and technology companies or startups, creating huge markets, which have not matured yet but have the potential to create new opportunities, and continues to grow with many new technological developments and private sector initiatives. The National Sectors, the boundaries and scale of which become clear as the research efforts to explore the unutilized capacity that boosts both public and private sectors progress through the **BRAINS² TÜRKİYE**'s subject-specific programs with the objective of identifying the most feasible and promising national interest areas, has become a part of the sectors that have the potential of the highest impact on the competitiveness, economic effectiveness and growth. **Synthetic Reality Technology**, the first application program as part of **BRAINS² TÜRKİYE**, will be held under the theme **"Building DeepFake Product and Defence Ecosystem"**. The program, which is proactively shared with all the key authorities, is announced through online platforms.

The efforts of the US to create a new-age national security infrastructure that fits well the needs of the 21st century have also been explored as part of the **Program**, which was developed within the framework of the integration of early-stage high-tech solutions into the national security ecosystem at the very beginning of the commercialization process. Findings, analyses and recommendations on the ways designed by the US to withstand asymmetric threats in the new world, and how Turkey can respond to similar threats with brand-new approaches, given the current circumstances, as well as the **earlier phase technology model** developed by a distinguished team in our corporate ecosystem are introduced in this framework.

deepware SMART CITIES INNOVATION LAB TASAM BGC Business and Government Consultancy İş ve Devlet Danışmanlığı

Elimination of Asymmetrical Threats by New Generation Purchasing Models

The concept of "asymmetric threat", which was introduced by the US and the UK in the 1990s, is a nomenclature used to describe threats that the world is not familiar with, and includes elements of unconventional warfare using unprecedented methods. Although it became more widespread after the September 11 attacks, this approach, which has increasingly become familiar to today's world, basically points to the radical changes must be provided by relevant institutions in their value chains.

The decision of the US-based national security institutions to change the paradigm in their old security visions, which was built on the ground of countering the threats of the Cold War period, dates back to the September 11 attacks. In this context and as an outcome of the efforts to explore and understand the US's new national security infrastructure and possible challenges that may be encountered in the 21st century, the experts have tried to build a dynamic security ecosystem that have the ability to turn the potential asymmetric threats into opportunities at their very early phases. One of the most important problems identified was that the purchasing models of all the security institutions could not perfectly serve the needs of the government. It is concluded that there were still major supply problems in the most crucial link of the value chain, which were not in harmony with the prevailing tendency of the time.

If we inquire into the key resources of innovation standing at the core of the US governmental body, we see that there are three significant organizations that promote novel technology development in cooperation with the Ministry itself and private corporations, under the US Ministry of Defense.

Defense Advanced Research Projects Authority (DARPA), which is the most prominent among these three governmental bodies, analyzes the warfare modalities of the future and produces sort of disruptive technologies for both the US's national security and military objectives. Certain inventions, such as stealth aircrafts, armed or non-armed drones, and broadband internet routers, are just some of the outcomes that demonstrate how crucial DARPA is. However, the major deficiency in this organization that it has had to focus only on long-term, and "high return-high risk" research projects instead of concentrating on short-term national security solutions.

The second major organization, which is the Federal Government Supported Research and Development Centers (FFRDC), conducts research projects to provide solutions for a set of complex technical issues arising between universities and non-profit organizations. These organizations seek to focus on research activities for what the public interest entails, instead of producing the goods by themselves. The major problems concerning these organizations are the relatively slow progress in the processes, the presence of cumbersome bureaucracy and the inability to adapt to solutions for rapidly developing Information and Communication Technologies (ICTs).

The third key innovation resource is the Research and Development Laboratories in the service of the entire spectrum of the US armed forces operating under the Ministry of Defense. These centers conduct network driven applied research activities on niche issues through public contracts. However, these labs also have certain drawbacks such that their solutions far from being affordable and able to meet to short-term technological requirements.

The US's Central Intelligence Agency (CIA), like all other government agencies, is now facing serious problems with procurement in terms of the supply and value chains. It is such a serious problem that, given that the average shelf-life of a technology in the free-market environment is 18 months following its commercialization process, certain technologies would already be out of date during the time to choose, purchase and put them into practice. Such technologies, however, are intended to meet the needs of corporations with the current procurement or purchasing pace and policies of such critical institutions.

Moreover, the Agency has been put under serious strain posed by new challenges, which has left it increasingly helpless in the face of the asymmetric threats of the 20th century, due to the delays in accessing cutting-edge technologies, choosing reactive approaches instead of proactive ones, the increasing need for information superiority, the growing gap between corporate needs and private sector solutions, and the need for a more entrepreneurial approach that has been stripped of its cumbersome bureaucratic structure.

The reasons why this agency had experienced constant delays in catching up with information technologies until 1998 can be found in this background, which shows that contractor companies of the time could not effectively meet the information and communication technology needs of the institution.

Moreover, small-sized firms had not only had deficiency in recruiting staff involved in tender offers by federal governments but also serious concerns about sustainability of their intellectual property rights. It was certainly the case that the institution would have had to face major problems at the onset of the new century, if the situation remained unchanged.

Considering the collapse of the Soviet Union, the September 11 attacks and the war in Syria, it appears that the modern world has witnessed the struggle of the great powers by and large for over successive decade-long periods, and undergone a dramatic change.

It is now inevitable for the US's adversaries, who are aware that military power may not always be overwhelmed by conventional responses, to prioritize unconventional warfare methods and to use them as a threat not only for the economic security and citizens but also for the governmental body of the United States, which is stuck in how to respond this challenge.

The solution for the US's problem was found when Norman Augustine, former Chairman of the Executive Board of Lockheed Martin, pioneered the establishment of the venture capital firm In-Q-Tel in 1999. It was originally established, even though its legal entity is a venture capital firm, as an innovative hybrid model and previously un-attempted "non-profit" venture capital firm, so that the state does not run against free market players.

With the help of this new purchasing model, the problems of the federal purchasing system were resolved. Using this active investment company as a means of developing relations with the ICTs market and building much closer contacts with investors made it possible to identify the latest technologies at the earliest phase in their life- cycle, before they were commercialized. A bridge was built between this company, and the CIA and Silicon Valley, and this network has been investing in more than 400 startup companies since 1999.

There have also been claims that many of the well-known companies, such as Google and Facebook, have not only collaborated with the In-Q-Tel but also made co-investments or developed joint projects. One of the most important preconditions for investments by the In-Q-Tel is that not investing in any company that does not have a product that will serve for public use at the same time. And so far, it has noticeably made more than 40 investments either direct or indirect in data analysis companies alone.

One of these companies is the Dataminr, which is a real-time data mining company, and it works in areas such as finance, governance, media, city security and crisis management. This company appears to have had the capacity of analyzing high impact events, emerging risks and growing trends by detecting Twitter messages and spotting from among all other publicly available data, as well as making notifications with live feed showing the location and date of any high impact event.

Another heavily invested company in this context is TransVoyant, which also provides real-time big data services in dozens of areas such as weather, logistics delays, aircraft departure planning, terrorist threats, geopolitical trends, breakdown maintenance or repair. Over one trillion global behavior events are analyzed by this system each day, which are detected through the data pulled from sensors, public databases, satellites, radars, drones, video cameras etc. Feedbacks, furthermore, the kind of the events that are expected to be happen for instance, as well as their dates and locations are reported by this company's website with business analytics and insights.

If the investment portfolio of this company is viewed, it will be seen that it has made investments, apart from business-data analytics, for early integration purposes in hundreds of high technology companies ranging from biology to chemical detection companies, from cyber security to mobile security sectors, from sensor technologies to image processing technologies, from artificial intelligence to communication.

It is of particular importance that related authorities support high-tech companies at an early phase, as part of national security policies, by developing different alternatives to the government's procurement models, as an investment ecosystem equivalent or similar to In-Q-Tel does not exist yet in Turkey and the available opportunities and conditions are unfavorable compared to large states. It is extremely important in this context that authorities deliberately promote the use of these technologies for public purposes.

So it is evident that how important it is both for the New World and the New Turkey to evaluate the novel technologies from regional, multilateral and international perspectives, to address entire spectrum of the issues of technology, to emphasize critical thinking with interdisciplinary interaction both within the security ecosystem and other domains. The following topics, which is the outcome of a systematic analysis, contain exemplary outputs and models for this end.

An Imminent Threat: Deepfake

A powerful national, regional and global change is possible only if the right persons who think outside the box come together over these crucial issues. The disobedience of qualified minds against mediocrity and bringing them together more often with qualified heads will be the principal formula for the success driven by new dynamics and security perspectives of countries.

Another one of the emerging problems, which Turkey proactively act upon in line with the "New Turkey" vision as a play-maker against the impending threats, is the imminent cyber threat, which is called "deepfake". It is a new generation media type in which either the image or voice of a person can be changed with those of other persons -in sizes that the human eye and ear cannot distinguish this image or voice from the original one- using neural-network-based artificial intelligence. These file types are generated by a set of deep machine learning programming techniques used for creating clones of original media files.

This process, which started in 2017 after the announcement by a user on the website called Reddit claiming that he had already developed such an artificial intelligence algorithm, alarmed the US government and led to intensive discussions in the Senate, while prompting extensive coverage in the newspapers such as Washington Post, the Economist and New York Times. It is observed that deepfake content is often used for generating inappropriate fake videos of celebrities etc. Misuse of these programming techniques, however, to generate fake news as well as involvement of such videos in financial frauds caused great concerns to the US's leading companies such as Facebook, Google and Microsoft.

The US's Senate passed a resolution in 2019, which was presented by Senator R. Portman, for the discussion of the governance processes and required studies of these type of issues, allocating a preliminary budget of around 500 thousand dollars. It was decided to issue an annual "deepfake report" by the Homeland Security for the years 2019-2024.

According to the US's National Security Advisory Council Emerging Technologies report (November 14, 2019) deepfake content is expected to turn into an artificial intelligence threat that will threaten the US's security within two-to five-year time span. Deepfake images are currently made by manipulating only the facial expressions. Yet, this deepfaking is capable of dubbing through stunt-performers or substitutes as well as using voice-clones but very low quality fake voices.

The US National Security Unit's report points out that certain orders or instructions might be given even by using only the voice part of this technology. There are various possibilities on the table for such a situation that might be able to result in certain political crises, nationwide emergency announcements, mislead military units, lead to stock market manipulations, and take part in secret intelligence operations.

Synthetic Reality Technology in Security Domain

The DARPA, which was aware of the threat posed by these kind of manipulations, started two different research programs, namely MediFor (Media Forensics) and SemaFor (Semantic Forensics), and encouraged its researchers to develop not only technologies in order for the authorities to be able to **spot** these kind of deepfake content, but also cyber security apparatus. Approximately $68 million were spent by DARPA for these research projects between 2018 and 2019.

This issue was regarded as a high-level threat by another company as well, which is In-Q-Tel, and together with Microsoft's corporate venture capital firm M12 and the US-based high-tech fund Silicon Valley Bank awarded Truepic as the most successful "deepfake detection technology" developer of the year in 2019, which has been on the radar since that time.

Today, any totally effective technique that allows to spot deepfake images has not been developed yet in any country, so they are all vulnerable to this threat. The threat is so insidious that it has been observed that the users exposed to these type of moving images for a while no longer trust even the real images. For this reason alone, the need for taking a raft of new emergency measures against the deepfake threat, which is the new nightmare of the cyber-media domain, to cyber security have come to the fore-front among the subject matters of many studies.

SYNTHETIC REALITY TECHNOLOGY

"Building DeepFake Product and Defence Ecosystem"

Deepfake technology causes concerns around the world due to its implications not only for security instruments but also for societies. Creating deepfake content over a very short video, a photo or recorded voice of a person, whether he is alive or not, is a threat that many sectors may be faced with -such as entertainment, education, culture, tourism, communication, arts, textile, cinema, advertisement, health. It is possible, with the help of this technology, to bring the digital version of a dead person to life or to manipulate the digital avatars of actual persons with different identities.

Only one of the reasons of why even developed countries have concerns about the disruptive capability of this technology is that the deepfake video released in 2019 about current medical condition of Ali Bongo, the president of Gabon, prompted the country's army to attempt a coup by false alarm.

Moreover, on July 15, 2020, Twitter platform was hit by the world's largest cyber-attack involved well-known personalities such as Joe Biden, Barack Obama, Elon Musk, Jeff Bezos, Bill Gates, while compromising their accounts. We can readily expect a chaotic atmosphere across the cyber-domain caused by possible broadcasting efforts to manipulate speeches and images of individuals, particularly of those who have the influence over certain segments of world population.

At this maturation level of technology, deepfake is still in its premature phase in terms of not only security concerns but also users. However, one the most sophisticated "a whole body image" and voice-cloning technologies is very close to be developed as an outcome of a two-year challenging task accomplished by a distinguished team of cyber security experts in this domain.

One of the most important national security measures that Turkey should take against the imminent asymmetric threats, concerning all of the issues mentioned above, is to backup urgently and adapt its instruments to this technology as soon as possible. Although it appears to be a strategic disadvantage not to have an effective national investment fund like In-Q-Tel, it is now not impossible to close this gap to a certain extent through new generation approaches.

A regularly updated deepfake detection system has already been developed as a complementary tool of the security toolbox as part of the Implementation Program with ongoing studies on Synthetic Reality technology, while security concerns caused by this technology are increasing.

It is imperative to give priority to this technology in security policies, if Turkey is to effectively protect its national security interests and to integrate it to its institutions for public purposes.

IMPLIMENTATION AREAS

Security Models and Tools Against Deepfake

Given the maturation pace of the core technology in question and its potential implications, it appears that the security measures, as part of the fight against disinformation, should be dealt not only with a technology-oriented approach, but with a holistic framework, including the public and private sectors, universities and think tanks. Technical and non-technical measures offered during the Program are evaluated together.

Technical Measures or Solutions

Deepfake "Detection System" Technology

The technology proposed within the scope of this regularly updated program is an outcome of the tremendous and long-lasting efforts of thousands of people. One of the most decisive factors in the fierce competition for reaching a technological edge in artificial or synthetic reality (deepfake) technology is the ability to simultaneously produce better processed deepfake images or videos. Therefore, the newly developed detection system, based on the artificial intelligence algorithm, which is fed by deepfake images perfected by both internal and external data sources, improves its performance.

Cloning Technology

Countries that excelled in video and audio cloning technology at an early stage of its development, as well as deepfake detection, will have the ability to respond and deter their rivals by giving them advantage over the adversaries. The technology, which will be developed within the Program, will be very close to be a cutting edge technology, and within a few-month period of time, the world's first highest quality cloning technology level will be achieved.

Authentication

Blockchain technology plays a very significant role in tagging any type of media data while it is still in the source-server, during the generation process in particular, and in detecting any possible interference with the source file. Leveraging the technology used within the program, it will be possible to circulate or share any type of image, video and voice file online more securely.

Non-Technical Solutions or Measures

Education

As social media applications and multi-featured smartphones penetrates deeper into the daily life of populations, the risk of being exposed to deepfake images or videos more and more increases. A task of great importance is, by means of educational institutions in particular, to raise public awareness as much as possible against disinformation or misinformation threats posed by synthetic media and fake news spreading like wildfire on cyber-domain.

Media Policy

So, it is now all the more imperative that the authorities accelerate the efforts to develop certain standard rules or guidelines to regulate the spread of deepfake content and determine the evaluation criteria of malicious content. There is a risk that national technological development and innovation efforts may be disrupted by haphazard and hasty regulation measures, as the public use of technology has increasingly become almost inevitable in today's world. For this reason, governmental action plans should be prudently studied in close contact with the private sector, think tanks and universities.

Legal Regulation

Considering the political manipulations based on deepfake videos, which have the potential to cause public outrages, it is all the more imperative to have, in cooperation with public and private sectors, universities and think tanks, clearly and distinctly drafted measurable regulations, which prevent, the threats in question at an early stage.

Annual Reports

There is a need for regular examination of the synthetic reality ecosystem both nationally and internationally in close cooperation with public-private sectors-university-think tanks, which will be resulted in regular reports and annual evaluations. It is important to allocate a special budget for this end and to continue research efforts to fight against the synthetic disinformation.