



International Cyber Security Forum 2019, Moscow

A

PSYCHOLOGICAL SECURITY

Prof. Evgeny Pashentsev

Leading Researcher

Diplomatic Academy of the Ministry of Foreign Affairs
of the Russian Federation

Director

International Centre for Social and Political Studies and Consulting

icspsc@mail.ru

Artificial Intelligence (AI): Economic Dimension



- The possibilities of artificial intelligence and machine learning are growing at an unprecedented speed: from machine translation to medical diagnostics.
- The volume of investment in the field of artificial intelligence in the next two decades could be trillions of dollars. According to the report of the international company PricewaterhouseCoopers Middle East (PwC), published in Dubai during the World Government Summit, economic growth in The world will be provided by 14% through the use of artificial intelligence, which is equivalent to 15.7 trillion dollars.
- To the greatest extent the possibilities of AI to accelerate its growth according to the PwC will be able to benefit from China (up 26% of the country's economic growth at the expense of AI).

AI: Discussion



- Tektology, Systems Theory, Action Theory, Punctuated Equilibrium Theory (PET) etc. are contributing today to the research of social dynamic systems.
- At the same time, insufficient attention is being paid to the comprehensive analysis of the issues of the unstable dynamic equilibrium of modern society, especially, in the context of random and targeted negative impacts in the field of strategic psychological warfare.
- It is aimed at long-term disorientation of the real or potential enemy on the most important issues, and this is impossible without measures to reduce its ability to strategic thinking, and to make appropriate decision-making. Thus ISIS, al-Qaeda and other at least leading terrorist organizations try and will try more to use Big Data, prognostic weapons and AI as efficient instruments in their asymmetric warfare efforts through Internet.

See more: Pashentsev E. Unstable dynamic balances and psychological warfare. Moscow: ICSPSC, 2017

Challenges for unstable dynamic systems



A flock of birds surround a Boeing 777 at London's Heathrow airport is dangerous

Challenges for unstable dynamic systems



A flock of problems for unstable dynamic system like the first power of the world is much more dangerous.
Is it dangerous to change horses while crossing a stream?

Challenges for unstable dynamic systems: One of not worst-case global scenarios



AI and UDSE

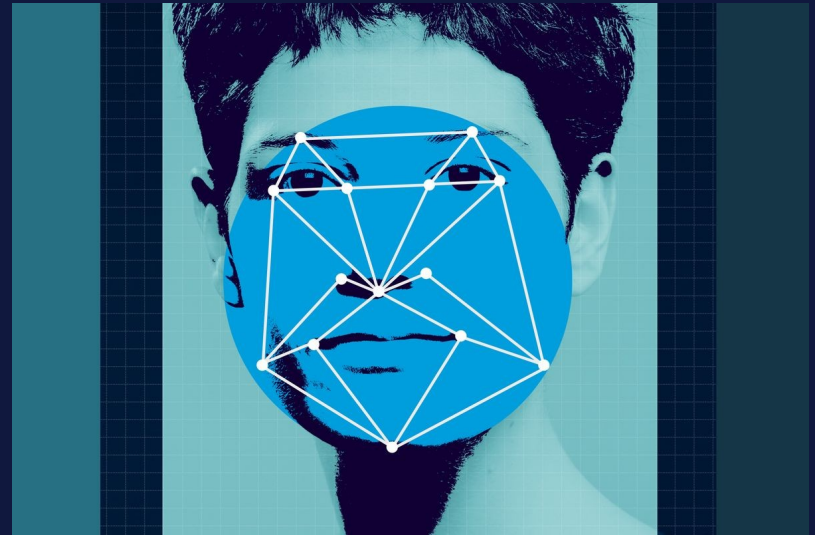


- As SPW is conducted with different degree of professionalism, by various state and non-state actors, there is an overlay (interference) of various control schemes resulting in decrease of the efficiency of SPW tools in controlling of UDSE.
- The role of AI in overcoming this problem is great, because it radically increases the ability of the human mind to calculate not only the options for social development, but increasingly makes it possible to foresee the specific parameters of individual events, allows you to identify the effectiveness of influence operations much faster and more effectively.
- Thus, AI is one of the leaders among other means and methods of conducting offensive HTSP, as, however, creates new and adequate capabilities of protective HTSP, which is typical for all dynamic unstable balance of offensive and defensive weapons .

Artificial intelligence to expose liars at EU borders



- The European Union has recently revealed plans to harness AI at the border to weed out suspicious travelers based on their gestures.
- The project, which will be trialed for a period of six months (in 2019), has been made possible through an EU contribution of roughly €4.5 million.



Across border control in Hungary, Latvia, and Greece, the AI, known as an "intelligent control system," will "deliver more efficient and secure land border crossings to facilitate the work of border guards in spotting illegal immigrants, and so contribute to the prevention of crime and terrorism," according to the EU.

Travellers who have been flagged as low-risk during the pre-screening stage will go through a short re-evaluation of their information for entry, while higher-risk passengers will undergo a more detailed check. But possible 99.9% confirmation of lies by AI and rather easy inevitable availability of such programmes inevitably bring not only big political and social advantages but risks as well and be manipulated by terrorist as well.



The development of information weapons

- Psychological warfare is waged between competing systems with the purpose of taking control over mass target audiences.
- Putting it differently, the object of information warfare can be divided into a hostile controlling system(s) and the controlled mass target audiences.



AI: Discussion

- In July, 2,400 leading artificial-intelligence (AI) researchers, including Tesla TSLA, -13.90% CEO Elon Musk, signed a pledge against killer robots, promising not to participate in the development or manufacture of machines that can identify and attack people without human oversight. It may sound encouraging, but countries can easily source the necessary know-how and tools to build their lethal “tin men” even without these researchers joining the team.
- However, the U.S. government remains oblivious. DARPA (Defense Advanced Research Projects Agency) has already announced a \$2 billion development campaign for the next wave of technologically advanced AI (dubbed “AI Next”). One of the goals is to have the machines “acquire human-like communication and reasoning capabilities, with the ability to recognize new situations and environments and adapt to them.”

Narrow AI (1)



- **The growth of complex comprehensive systems** with active or leading AI participation increases the risk of malicious interception over its control. According to Marc Ph. Stoecklin, principal research staff member and manager at Cognitive Cybersecurity Intelligence (CCSI), a class of malware “like *DeepLocker* has not been seen in the wild to date”.
- **Terrorist repurposing of commercial AI systems.** Commercial systems are used in harmful and unintended ways, such as the using of drones or autonomous vehicles to deliver explosives and cause crashes.
- **Deepfakes**, which are artificial intelligence algorithms that create convincing fake images, audio and video. For example deepfake of Prime Minister Benjamin Netanyahu or other government officials talking about impending plans to take over Jerusalem’s Temple Mount and Al-Aqsa Mosque could spread like wildfire in the Middle East.
- **Fake people.** After selling the first work of art created by AI in early 2018, deep learning algorithms are now working with portraits of non-existent people. NVIDIA recently shared the results of generative competition network (generative adversarial network – GAN).

Narrow AI (2)



- **Amplification and agenda setting.** Studies indicate that bots made up over 50 percent of all online traffic in 2016.
- **Damage reputation through bot activities** during political campaigns, for example, could be used by terrorist groups to attract new supporters or organize killings of politicians.
- **Sentiment analysis** provides an accurate analysis of the overall emotion of the text content incorporated from sources like blogs, articles, forums, surveys, etc. It may be a very useful tool for terrorists too.
- **Predictive analytics** as a prognostic weapon. EMBERS (“embers”) which was launched by IARPA back in 2012. Its full name – “event detection based on earlier models with the use of surrogates” (Early Model Based Event Recognition using Surrogates).
- One can imagine that, based on a system combination of techniques of psychological impact, complex AI systems and Big Data – **synthetic reality.**

See more: Pashentsev E. Sophisticated Technologies in Counteraction to Terrorism in Datafied Society: From Big Data to Artificial Intelligence // Understanding the War on Terror: Perspectives, Challenges and Issues. Ed. by R. Flanagan. Nova Science Publishers, 2019.

Predictive Analytics and Psychological Warfare

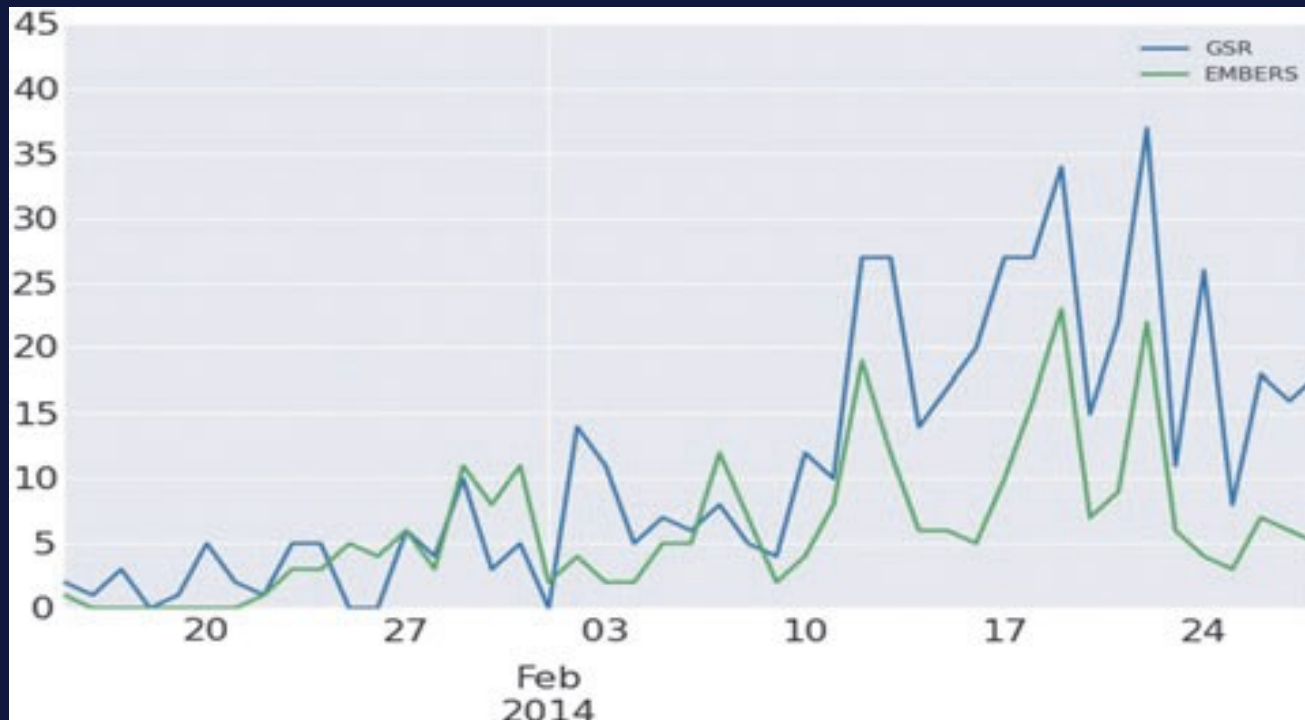


- **Predictive analytics** is a variety of statistical techniques including predicting modeling, machine learning and data mining that analyze current and historical facts to make predictions about future or otherwise unknown events.
- Predictive Analytics is developed in the USA by Recorded Future, *Palantir Technologies* and supported among other sources by CIA venture company *In-Q-It*, which aims to support innovations in the spheres related to national security and intelligence.



Big Data, Predictive (Prognostic) Weapons: To the New Horizons in Management of Political Conflicts

- Early Model Based Event Recognition using Surrogates (EMBERS).The case study of Venezuela
- Ground truth data (called the gold standard report {GSR})



Source: Big Data N. December, 2014. P. 193.

EMBERS: Correction of "Now" from the Future



Source: Big Data N. December, 2014. P. 194.



Changes in the Estimation of Terms of Creation of General AI

- In a White House document *Preparing for the Future. National Science and Technology Council of Artificial Intelligence* regarding the outgoing administration of Barack Obama in 2016, an expert assessment was given about the fact that General AI will not be achieved for at least decades.
- The GAO 2018 Report on *Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies* focuses on long-range emerging threats that may occur in approximately five or more years, as identified by nearly 30 responsible structures in the system of national security of the USA.
- Among the Dual-Use Technologies, the first in the list in the GAO report is AI. Moreover, the only two examples of AI threats given are deeply interrelated: 1) *Nation State and Nonstate Development of AI*; 2) *Intelligent Systems with General AI*.

O

When



Will AI Exceed Human Performance

- The survey prepared in 2018 by researchers of Oxford, Yale Universities and AI Impacts on the question *When Will AI Exceed Human Performance?* is based on Evidence from AI Experts. Their survey population were the researchers who published at the 2015 NIPS and ICML conferences (two of the premier venues for peer-reviewed research in machine learning).
- A total of 352 researchers responded to the survey invitation (21% of the 1634 authors were contacted). The survey used the following definition: “High-level machine intelligence” (HLMI) is achieved when unaided machines can accomplish every task better and more cheaply than human workers.
- Each individual respondent estimated the probability of HLMI arriving in future years. Taking the mean over each individual, the aggregate forecast gave a 50% chance of HLMI occurring within 45 years and a 10% chance of it occurring within 9 years. The survey displays a similar gap between the two countries with the most respondents in the survey: China (median 28 years) and USA (median 76 years).

Global Research in AGI



- Artificial Narrow Intelligence (ANI)
- Artificial General Intelligence (AGI)
- Artificial Superintelligence (ASI)

Research centres and companies in the field of AGI (globally no less than 60 in 2018)

- Cambridge Center for the Study of Existential Risk,
- Future of Humanity Institute
- Future of Life Institute
- Dalle Molle Institute for Artificial Intelligence Research
- Helen Wills Neuroscience Institute
- Machine Intelligence Research Institute
- Vicarious AI Company ...

AI is Not the End of Humanity,



b

Further Progress (1)

- Unlike hypothetical aliens, in the case of General AI, we will deal with intelligence coming from the historical, scientific, philosophical, cultural sense of modern human civilization. Intelligence that will go forward faster and better than any of the past human generations. *But this intelligence will inherit the heritage of the human race.*
- Much depends on us, when we ask the question 'what will this intelligence look like'. Will it have our legacy or not? We can destroy ourselves just before this new intelligence appears on Earth, it is a sad reality.
- It is also important that General AI will not become a product of humanity in general, but of specific people. Different options are on the table, until the appearance of General AI in the laboratory controlled by anti-social, reactionary, militaristic and other circles. If the environment often deforms people (of different intelligence), then why is this not applicable to General AI?

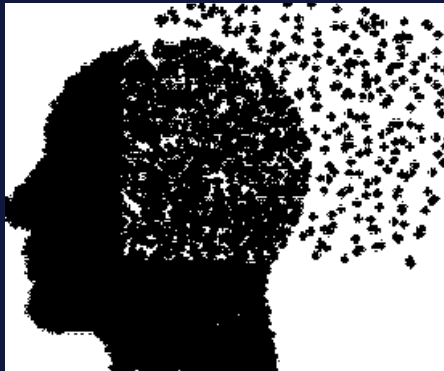
AI is Not the End of Humanity,



b

Further Progress (2)

- Although it can be assumed that the creation of General AI through an organization with criminal goals will be an additional risk factor, controlling the extremely rapid progress of General AI into ASI is unlikely to be allowed not only for egoistic groups of influence but for the whole humanity (see more: *Strategic Communication in EU–Russia Relations: Tensions, Challenges and Opportunities*. Moscow: ICSPSC, 2018, 23–96.
- We can integrate ourselves into the process of entering the singularity through cyborgization and genetic restructuring that increases our intellectual capabilities
- Jinn or Demiurge Options? General AI as the possibility of the emergence of an integrated intelligence with its own will and feelings (albeit quite different from human ones). Another integrated powerful intellectual potential capable of solving problems only on human target designation. Then, we will be dealing simply with a more powerful machine, and the advantages of its use will depend on the people who will direct it.



ICCWS 2019

**14th International Conference
on Cyber Warfare and Security**

Stellenbosch, South Africa, 28 February - 1 March
2019

**Mini Track on Psychological Warfare, New
Technologies and Political Instability in
Contemporary World**

<https://www.academic-conferences.org/>



ECIAIR 2019

European Conference on the Impact of AI and Robotics

31 October - 1 November 2019, EM-Normandie Business School, Oxford, UK

Mini Track on the Malicious Use of Artificial Intelligence: New Challenges for Democratic Institutions and Political Stability

<https://www.academic-conferences.org/>



**THANK YOU FOR YOUR
KIND ATTENTION!**