Журнал "Мировые цивилизации" / Scientific journal "World civilizations" https://wcj.world

2020, №3–4, Том 5 / 2020, No 3–4, Vol 5 https://wcj.world/issue-3-4-2020.html

URL статьи: https://wcj.world/PDF/03aECMZ320.pdf

**Ссылка для цитирования этой статьи:**
Рольф Клауберг Киберфизические системы и искусственный интеллект: шансы и угрозы для современной экономики // Мировые цивилизации, 2020 №3–4, https://wcj.world/PDF/03aECMZ320.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

**For citation:**
Rolf Clauberg (2020). Cyber-physical systems and artificial intelligence: chances and threats to modern economies. *World civilizations*, [online] 3–4 (5). Available at: https://wcj.world/PDF/03aECMZ320.pdf (in Russian)

**Rolf Clauberg**
Peoples' friendship university of Russia, Moscow, Russia
«InterKulturForum» GmbH, Zürich, Schweiz
E-mail: r.clauberg@hispeed.ch; klauberg-r@rudn.ru
РИНЦ: https://www.elibrary.ru/author_profile.asp?id=1067538
SCOPUS: https://www.scopus.com/authid/detail.url?authorId=6603566417

# Cyber-physical systems and artificial intelligence: chances and threats to modern economies

**Abstract.** This article analyzes the potential chances and threats to modern civilizations and economies caused by cyber-physical systems and artificial intelligence. Literature describing the evolution of cyber-physical systems and artificial intelligence is analyzed for discerning the underlying forces driving these evolutions, the potential chances brought by these new technologies as well as the most serious threats stemming from these technologies. Special emphasize is given to the merge of operational technology and information technology and corresponding cyber-physical systems in critical infrastructure, industrial plants, and unmanned aerial vehicles. For cyber-physical systems in critical infrastructure and industrial plants we find the chances driving the evolution mainly in enhancements of productivity and improvements of efficiency and ease of use within their existing markets. For unmanned aerial vehicles the corresponding chances are mainly new applications, in markets accessible before only with high risk for human life and health. For the threats we try to estimate the size of threats from previous events and the potential to realize these threats from what is needed for the realization and what is easily available in terms of hardware, software, and technical knowledge. The threats for both areas are mainly in cyber-terrorism and cyber-warfare.

**Keywords:** artificial intelligence; cyber-security; cyber-terrorism; cyber-physical systems; digitalization; unmanned aerial vehicles

## Introduction

Today's digitalization mainly started after the dot.com crisis of 2000 with the evolution of e-commerce, e-procurement, digital marketplaces, digital value chains, e-services, business models and technologies for digital business [1]. It was accompanied by globalization of trade [2] and correspondingly integrated value-chains. The entire operation of many companies changed towards something which Samuel J. Palmisano – then Chairman, President, and CEO of IBM Corporation – in 2006 called a "globally integrated enterprise"[1]. An enterprise where specific corporate functions would

[1] The Globally Integrated Enterprise [Electronic source] http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/globalbiz/transform/ (date of access: 03.12.2018).

be concentrated anywhere on the globe where the conditions for these functions were optimal for the specific company. In the industrial area this evolution was accompanied by the occurrence of the so-called Industrial Internet of Things (IIoT) [3] which itself evolved from industrial control systems (ICS) and supervisory, control, and data acquisition (SCADA) systems by coupling these systems to the internet thereby allowing business people direct access to industrial process data. This coupling of operational technology (OT) which controls machines to information technology (IT) generates cyber-physical systems and allows the global integration and automatization of supply and value chains. It is also an important point in Industry 4.0 or smart factories [4], which both aim towards highly automatized factories in which it is possible to modify a product or even change to a different product by just changing the input given to the computer control system of the factory. This is possible with nearly complete automatization where all production processes are controlled by sensors which measure all kind of status information about the production processes. This information is then used to automatically steer the production processes. The generation of huge amounts of sensor data within the IIoT requires automatic data processing. This is nowadays supported by artificial intelligence (AI). Within the old ICS/SCADA systems this was mainly restricted to algorithm based AI, but neural network based AI is already occurring to recognize intrusion detection in IT and cyber-physical systems [5].

A second area where cyber-physical systems are operated with AI are autonomous or semi-autonomous Unmanned Aerial Vehicles (UAVs) [6]. UAVs are widely used in industrial inspection, as well as mapping and surveying.

Today cyber-physical systems and artificial intelligence are two of the new technologies which strongly shape the digitalization of our present world.

In the following sections we will first briefly describe the methods used to arrive at the conclusion, then discuss the chances and threats of cyber-physical systems and artificial intelligence and finally present the conclusion.

## Methods

We will analyze the cited literature resources to deduct the main driving forces behind a specific trend like the switch from separated systems of operating technology and information technology towards a united system with cyber-physical units or the exploding use of artificial intelligence. Then we will analyze the new technologies to find their most promising applications as well as serious threats and the probability to realize these threats.

## Discussion

Considering cyber-physical systems within critical infrastructure or industrial plants, the advantages of coupling operational technology with the internet are all related to productivity enhancements through easier access to operational or production data. On the one hand the data from the operational technology can be accessed by the businesspeople, and highly aggregated and processed data provide insight into operational and production processes and thereby allow optimization and adaptation to changes of these processes. On the other hand, software updates to OT systems can be easier and faster implemented [3; 4].

Considering the threats to critical infrastructure and industrial plants, they are mainly related to cyber-terrorism and cyber-warfare. We must consider the damage which can be caused by corresponding attacks and the difficulty or ease with which these attacks can be performed. Critical infrastructure includes power, water and traffic (air, road, river) networks. From World War II it is clear that attacks on these kinds of infrastructure can cause decisive damage to the economy and health in a country. A second example for the devastating damage caused by an industrial accident is the Bhopal catastrophe from 1984 in India [7]. This was an accident caused by non-functioning or non-existent safety systems which costed thousands of live[2]. The question is whether such an accident can be enforced by cyber-attacks through the internet. The answer to this question depends on two factors. Firstly, whether we can find examples of existing computer viruses or worms which are sophisticated enough to allow manipulation of the operating parameters of cyber-physical systems. Secondly, whether existing computer security solutions are good enough to guaranty protection against such attacks. Here, the most evident example for a highly sophisticated computer attack program is the Stuxnet worm [8]. This worm searched for specific programmable logic controllers (PLC) connected to the computer it had infiltrated. Only if these PLCs were detected and the operating system and other parameters of the system showed the expected values, this worm started its destructive activities. It changed operating parameters of the controlled industrial systems so that operation destroyed the systems without sending alarm signals. This example clearly demonstrates that dedicated attacks on specific cyber-physical systems are possible. The Stuxnet worm still reached its goals through software updates using infiltrated USB-sticks. Nowadays these systems are accessible directly through the internet. Mostly, OT systems are protected somewhat better than pure IT systems by using e.g. so-called de-militarized zones with double firewalls. Also, there have been assessments of security aspects for cyber-physical systems [9–11] addressing the specific aspects of such systems. However, the general degree of security of IT and OT systems is still not convincing. The Ponemon Institute, which is concerned with data conservation and new technologies, has prepared a report entitled "2017 Cost of Data Breach Study"[3]. This report is a computer security research study which was sponsored by the American computer concern IBM and covers 419 companies in 13 countries or regions. The countries covered are USA, UK, Germany, Australia, France, Brazil, Japan, Italy, India, Canada and South Africa. The regions covered are the Middle East and the ASEAN (Association of South-East Asian Nations) region. Figure 22 on page 27 of this report lists the mean time to identify a data breach caused by a malicious or criminal attack as 214 days and after identifying such a data breach it still takes a mean time of 77 days to maintain the data breach. This is plenty of time for a sophisticated computer virus or worm to analyze the system and execute the corresponding attack.

Considering autonomous UAVs, there application is mainly in control, repair and rescue activities where human activities are difficult or dangerous and requirements for fast response time make remote human control impossible or at least unpractical [6]. Hence, in contrast to cyber-physical systems in critical infrastructure or industrial plants, these applications are not just a matter of convenience or improved efficiency, but an important element of modern life. Many of the work that is now done by autonomous UAVs was previously impossible. Present applications are mainly using an optical system to navigate the UAV and to optically recognize specific objects. For both cases they use AI either based on algorisms [12; 13] or on neural networks [14; 15].

As for cyber-physical systems, the most serious threats with autonomous UAVs are again in cyber-warfare and cyber-terrorism. Autonomous UAVs are able to hunt down specific targets, recognize specific objects and then take those actions for which they are programmed. Object recognition is normally done with the use of neural networks and is still not perfect. There is the problem with specific situations where objects are wrongly identified with high confidence [16]. Also, errors must be expected if the materials to train the neural network are not carefully analyzed and cleaned from potentially bad material. National military operations may be reluctant to use such

[2] Encyclopedia Britannica. [Электронный ресурс]. URL: https://www.britannica.com/event/Bhopal-disaster (дата обращения: 19.03.2020).

[3] 2017 Cost of Data Breach Study [Электронный ресурс]. URL: https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states?s=2017+Cost+of+Data+Breach+Study (дата обращения: 19.03.2020).

systems for elimination of targets, but still may be using them coupled with remote human control to permit or prohibit the final strike after the system autonomously found the target. However, terrorist groups may not care too much about hitting the wrong target. So, we can say that these systems may be used for destroying specific targets. The question is, how easy it is for a terrorist group to build such an autonomous UAV. Looking at the publications we cited above, there are small University groups which successfully built their own autonomous UAVs. The important point is that all hardware components to build such systems can be bought on the market at quite low prices. Especially, in addition to the GPUs (Graphical Processing Units) which were the first kind of accelerators for AI neural network operations, Google developed specific TPUs (Tensor Processing Units)[4] that offer corresponding capabilities at much lower power consumption and smaller dimensions. In addition, several organizations offer corresponding software and education material for[5] free. Therefore, we can conclude, that even small groups are able to build autonomous UAVs at low cost as long as the group contains some persons with the necessary skills in building small hardware systems out of components openly available on the market and adapting freely available software packages to their specific goals.

Considering AI in general, one often discussed issue is its impact on labor, i.e. how it will change existing jobs, which jobs it will destroy and what kind of new jobs it will create. A report from the National Academy of Sciences of the USA [17] discusses various perspectives ranging from the Doomsayer's Perspective to the Optimist's Perspective and also considering Unifying Perspectives. However, in their conclusion they come to the result that researchers and policy makers are underequipped to forecast the labor trends resulting from specific technologies, such as AI. The only realistic conclusion here seems to be that it will change many jobs by requiring that people working in these areas must learn to use the new AI tools, that it will destroy certain jobs and that it will create new jobs, but with skill requirements very different from those of jobs it destroyed. In contrast to industrial automation, it may also destroy jobs of highly educated people. For example, law firms in countries using case law, as e.g. in the USA and the United Kingdom, presently use young lawyers to analyze existing previous judgments to use as argument in current cases. Also, computer tomography results are analyzed by well educated people for hints of specific illnesses. In both cases, analysis with AI tools may soon show better results than the ones made by human inspection.

## Conclusion

The driving force for integrating operational technology (OT) with information technology (IT) in infrastructure and industrial systems clearly is improving efficiency and productivity by enabling easier data exchange between the OT and IT systems. In connection with smart factories these also enables highly automated operations in global supply and value chains. For autonomous and semi-autonomous UAVs the driving force is the enablement of activities like remote inspection and surveying as well as rescue operations in dangerous areas. Before, these markets were not accessible without serious exposure of humans to these dangers. The use of AI in autonomous UAVs is a necessity. The main threats for both areas are based in cyber-terrorism and cyber-warfare against humans and the economy. For autonomous or semi-autonomous UAVs this means abuse of the systems to execute attacks on specific targets. For cyber-physical systems this means attacks by computer viruses or worms on these systems leading to potentially catastrophic damages for society and economy. For both areas the potential threats are severe and the possibility to perform these threats is

[4] Edge Tensor Processing Units – [Электронный ресурс]. URL: https://aiyprojects.withgoogle.com/edge-tpu/ and small local AI platforms – https://coral.ai/ (дата обращения: 19.03.2020).

[5] TensorFlow is an end-to-end open source platform for machine learning. The Robot Operating System (ROS) is a flexible framework for writing robot software. – [Электронный ресурс]. URL: https://www.tensorflow.org/, https://www.ros.org/ (дата обращения: 19.03.2020).

realistic. In the area of critical infrastructure and industrial plants, substantial efforts to improve system security can reduce the threats. In the area of autonomous UAVs surveillance of the airspace down to objects of the size of drones capable of carrying bombs or dangerous weapons may be the only solution to reduce these threats.

Considering the impact of AI on jobs, continuous education and possibly a broader base education to enable faster adaptation to new jobs may be the best protection against job destruction.

## REFERENCES

1. Fingar P., Aronica R. Death of “e” and the Birth of the Real New Economy: Business Models, Technologies and Strategies for the 21st Century. Tampa, Fl, USA: Meghan-Kiffer Press, 2001. 360 p.
2. Friedman T.L.T. The world is flat: A brief history of the twenty-first century // New York: Farrar, Straus and Giroux. New York, NY, USA: Farrar, Straus and Giroux, 2007. 660 p.
3. Jeschke S. et al. Industrial Internet of Things and Cyber Manufacturing Systems // Industrial Internet of Things / ed. Jeschke S., Brecher C., Song H.R.D. Cham: Springer International Publishing Switzerland, 2017. P. 3–19.
4. Almada-Lobo F. The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES) // J. Innov. Manag. 2016. Vol. 3, № 4. P. 16–21.
5. Kathareios G. et al. Catch it if you can: Real-time network anomaly detection with low false alarm rates // Proceedings – 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017. Institute of Electrical and Electronics Engineers Inc. (IEEE), 2017. P. 924–929.
6. Lu Y. et al. A survey on vision-based UAV navigation // Geo-Spatial Inf. Sci. Taylor & Francis, 2018. Vol. 21, № 1. P. 21–32.
7. Yang M., Khan F., Amyotte P. Operational risk assessment: A case of the Bhopal disaster // Process Saf. Environ. Prot. 2015. Vol. 97. P. 70–79.
8. Karnouskos S. Stuxnet worm impact on industrial cyber-physical system security // IECON Proceedings (Industrial Electronics Conference). 2011. P. 4490–4494.
9. Lu T. et al. Towards a framework for assuring cyber physical system security // Int. J. Secur. its Appl. 2015. Vol. 9, № 3. P. 25–40.
10. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA // Int. J. Cyber Warf. Terror. 2016. Vol. 6, № 3. P. 1–16.
11. Wu W., Kang R., Li Z. Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities // IEEE International Conference on Industrial Engineering and Engineering Management. 2016. P. 1618–1622.
12. Opromolla R., Fasano G., Accardo D. A vision-based approach to uav detection and tracking in cooperative applications // Sensors (Switzerland). 2018. Vol. 18, № 10.
13. Suleiman A. et al. Navion: A 2-mW Fully Integrated Real-Time Visual-Inertial Odometry Accelerator for Autonomous Navigation of Nano Drones // IEEE J. Solid-State Circuits. 2019. Vol. 54, № 4. P. 1106–1119.
14. Palossi D. et al. A 64-mW DNN-Based Visual Navigation Engine for Autonomous Nano-Drones // IEEE Internet Things J. Institute of Electrical and Electronics Engineers Inc., 2019. Vol. 6, № 5. P. 8357–8371.
15. Wyder P.M. et al. Autonomous drone hunter operating by deep learning and all-onboard computations in GPS-denied environments // PLoS One. 2019. Vol. 14, № 11. P. 1–18.
16. Hendrycks D. et al. Natural Adversarial Examples [Electronic resource]. 2019. URL: https://arxiv.org/pdf/1907.07174.pdf.
17. Frank M.R. et al. Toward understanding the impact of artificial intelligence on labor // Proceedings of the National Academy of Sciences of the United States of America. 2019. P. 9.

УДК 33

**Рольф Клауберг**
ФГАОУ ВО «Российский университет дружбы народов», Москва, Россия
Доцент кафедры «Менеджмента» «Экономического» факультета
Компания «InterKulturForum», Цюрих, Швейцария
Генеральный директор
Кандидат естественный наук: направление – физика
E-mail: r.clauberg@hispeed.ch; klauberg-r@rudn.ru
РИНЦ: https://www.elibrary.ru/author_profile.asp?id=1067538
SCOPUS: https://www.scopus.com/authid/detail.url?authorId=6603566417

# Киберфизические системы и искусственный интеллект: шансы и угрозы для современной экономики

**Аннотация.** В данной статье дается анализ потенциальных возможностей и угроз для современных цивилизаций и экономики, обусловленных киберфизическими системами и искусственным интеллектом. На основе исследовательских работ, описывающий эволюцию кибер-физических систем и искусственного интеллекта, анализируется для выявления глубинных сил, движущих этими эволюциями, и потенциальных возможностей, создаваемых этими новыми технологиями, а также наиболее серьезных угроз, исходящих от них. Особое внимание уделяется слиянию операционных и информационных технологий, а также соответствующих киберфизических систем в критической инфраструктуре, на промышленных предприятиях и в беспилотных летательных аппаратах. Для киберфизических систем в критической инфраструктуре и промышленных предприятиях мы находим шансы, определяющие эволюцию, главным образом в повышении производительности и повышении эффективности и простоты использования на существующих рынках. Для беспилотных летательных аппаратов соответствующие шансы имеют в основном новые области применения, на рынках, доступных ранее только с высоким риском для жизни и здоровья человека. Для угроз делается попытка оценить размер угроз от предыдущих событий и потенциал реализации этих угроз из того, что необходимо для реализации и что легко доступно с точки зрения аппаратного обеспечения, программного обеспечения и технических знаний. Угрозы для обеих областей заключаются, главным образом, в кибертерроризме и кибервойне.

**Ключевые слова:** искусственный интеллект; кибербезопасность; кибертерроризм; кибер-физические системы; цифровизация; беспилотные летательные аппараты

## REFERENCES

1. Fingar P., Aronica R. Death of “e” and the Birth of the Real New Economy: Business Models, Technologies and Strategies for the 21st Century. Tampa, Fl, USA: Meghan-Kiffer Press, 2001. 360 p.

2. Friedman T.L.T. The world is flat: A brief history of the twenty-first century // New York: Farrar, Straus and Giroux. New York, NY, USA: Farrar, Straus and Giroux, 2007. 660 p.

3. Jeschke S. et al. Industrial Internet of Things and Cyber Manufacturing Systems // Industrial Internet of Things / ed. Jeschke S., Brecher C., Song H.R.D. Cham: Springer International Publishing Switzerland, 2017. P. 3–19.

4. Almada-Lobo F. The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES) // J. Innov. Manag. 2016. Vol. 3, № 4. P. 16–21.

5. Kathareios G. et al. Catch it if you can: Real-time network anomaly detection with low false alarm rates // Proceedings – 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017. Institute of Electrical and Electronics Engineers Inc. (IEEE), 2017. P. 924–929.

6. Lu Y. et al. A survey on vision-based UAV navigation // Geo-Spatial Inf. Sci. Taylor & Francis, 2018. Vol. 21, № 1. P. 21–32.

7. Yang M., Khan F., Amyotte P. Operational risk assessment: A case of the Bhopal disaster // Process Saf. Environ. Prot. 2015. Vol. 97. P. 70–79.

8. Karnouskos S. Stuxnet worm impact on industrial cyber-physical system security // IECON Proceedings (Industrial Electronics Conference). 2011. P. 4490–4494.

9. Lu T. et al. Towards a framework for assuring cyber physical system security // Int. J. Secur. its Appl. 2015. Vol. 9, № 3. P. 25–40.

10. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA // Int. J. Cyber Warf. Terror. 2016. Vol. 6, № 3. P. 1–16.

11. Wu W., Kang R., Li Z. Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities // IEEE International Conference on Industrial Engineering and Engineering Management. 2016. P. 1618–1622.

12. Opromolla R., Fasano G., Accardo D. A vision-based approach to uav detection and tracking in cooperative applications // Sensors (Switzerland). 2018. Vol. 18, № 10.

13. Suleiman A. et al. Navion: A 2-mW Fully Integrated Real-Time Visual-Inertial Odometry Accelerator for Autonomous Navigation of Nano Drones // IEEE J. Solid-State Circuits. 2019. Vol. 54, № 4. P. 1106–1119.

14. Palossi D. et al. A 64-mW DNN-Based Visual Navigation Engine for Autonomous Nano-Drones // IEEE Internet Things J. Institute of Electrical and Electronics Engineers Inc., 2019. Vol. 6, № 5. P. 8357–8371.

15. Wyder P.M. et al. Autonomous drone hunter operating by deep learning and all-onboard computations in GPS-denied environments // PLoS One. 2019. Vol. 14, № 11. P. 1–18.

16. Hendrycks D. et al. Natural Adversarial Examples [Electronic resource]. 2019. URL: https://arxiv.org/pdf/1907.07174.pdf.

17. Frank M.R. et al. Toward understanding the impact of artificial intelligence on labor // Proceedings of the National Academy of Sciences of the United States of America. 2019. P. 9.