SOME CONSIDERATIONS ON AI SECURITY TRAINING AND RESEARCH ON THE WAY TO SOCIETY 5.0

Galina Momcheva Teodora Bakardjieva Antonina Ivanova
Varna Free University "Chernorizets Hrabar"

Introduction: Nowadays we're witnessing profound changes in the areas of information technologies, security, sustainability, value creation and the volume of data produced in the world is growing rapidly to an expected 175 zettabytes in 2025 [15]. The society will flourish in the global digitalized industry 4.0 only if proper training and research are realized. The way that companies do business has changed and all sectors now rely on digital technologies to produce, market and make trade. All these activities are underpinned by data flows which enable the digital products and services, from traditional email and CRM (customer relationship management) system to IoT (Internet of Things), AI (Artificial Intelligence), Virtual Reality (VR) and Augmented Reality (AR), Cloud technologies, Blockchain, Big Data Analysis, 3 D printing and scanning and other cutting-edge technologies. Communication, cooperation and monitoring in a smart organization could be in real time and make possible effective decentralized decisions as human workers act remotely. But all the stakeholders — universities, students, industrial partners — should be prepared for the above challenges of Industry 4.0 which is still at initial stage of development [3, 4]. The main achievements could be expected not earlier than 2020-2025 and the image of a new paradigm of Industry 5.0 more often called Society 5.0 could be seen today. It involves the penetration of AI in people common life and their "cooperation" with the aim of enhancing the man capacity for the benefit and convenience of each person [18].

These kinds of emerging technologies are supporting government efficiencies generating immense benefits at regional, national and global levels. To facilitate the application of the digital technologies necessary to support capacity building and wide awareness-raising campaign on security culture and work toward an inclusion vision of Society 5.0. Each new wave brings opportunities for organizations to position itself in the data-agile economy.

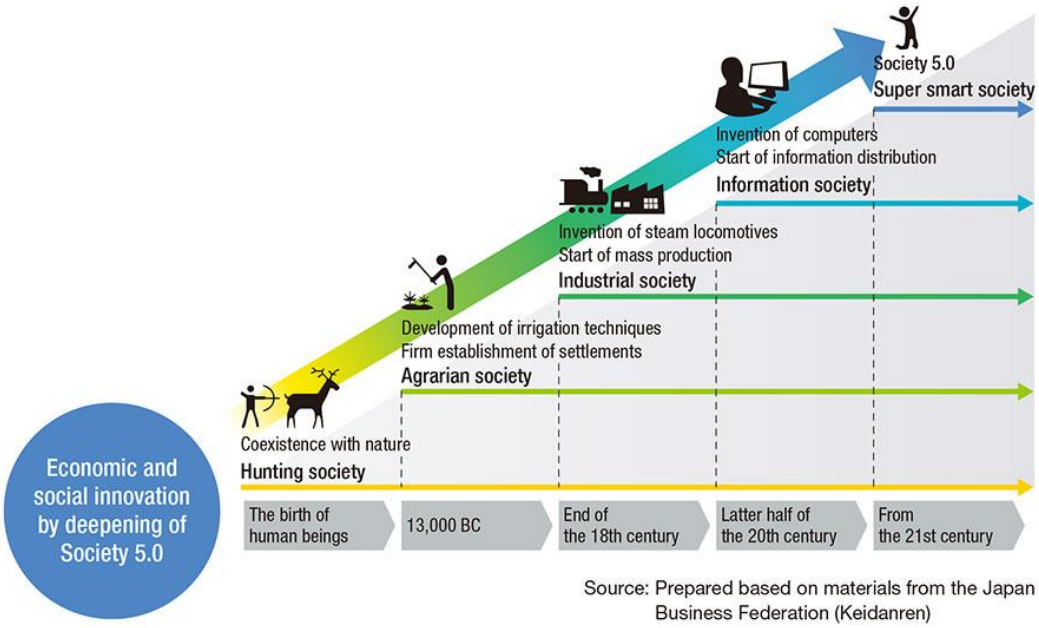


Fig. 1 The “Super Smart Society” Aimed for by Society 5.0 [16]

Society 5.0 is an information society built upon

Society 4.0, aiming for a prosperous human-centered society.”

Society 5.0 is an information society built upon

Society 4.0, aiming for a prosperous human-centered society.”

Society 5.0 is an information society built upon

Society 4.0, aiming for a prosperous human-centered society.”

Society 5.0 is a super-smart society where technologies such as AI, IoT, Big data, and robots could change every industry and all social segments with the idea to solve currently impossible problems, making people's life more comfortable, sustainable and safe. Furthermore, the way in which data are stored and processed is changing and take place in data centres and centralised computing facilities, in smart connected objects or manufacturing robots, and in computing facilities close to the user [15]

AI is a significant part of Industry 4.0 [7] that possesses a number of characteristics that may be important to consider as these technologies enter the national security arena. AI has the potential to be integrated across a variety of applications, improving IoT in which disparate devices are networked together to optimize performance. [2, 11]. AI includes various topics of learning strategies, knowledge abstraction, reasoning domain, and reasoning mechanisms – ML (Machine Learning) to adapt to new circumstances and to detect and extrapolate patterns; NLP (Natural Language Processing) to enable successful communication in a given language; Knowledge representation to store information a machine knows and receives; Automated reasoning to use the stored information to answer questions and to draw new conclusions; Computer vision to perceive objects; Robotics to manipulate objects and move about. Applying AI requires a skilled and educated workforce with domain expertise, technical training, and the appropriate tools. Organizations must cultivate a culture of data excellence. Success for users in machine learning requires iteration, experimentation, and learning through early sub-optimal performance [1].

Background

The implementation of the AI in Industry 4.0 will bring a revolutionary change. Advanced security implementation is possible by applying AI technology

[8]. Research reports suggested that AI implementation in cybersecurity would be able to find the attackers before they could result in any sort of attack. AI technology is capable of learning and adapting to the current environment and the threat landscape [9, 10].

Institutions should prioritize AI R&D on areas that can provide sustainable advantages and mitigate key risks. AI has the potential to enable many new types of low-cost, high-impact military technologies. Though, AI's implications for national security, is still in an early stage, AI has the potential to be a transformative military technology. Some of these future, AI-enabled capabilities will change the relative attractiveness of procurement and sustainment investments [12, 13, 14].

In data-driven operations and innovation it is essential that data moves in a secure manner and engenders the trust of users. Governments and HEI (Higher Education Institutions) should work to identify and share experiences related to security education and social responsibility. Each organization must build the foundational digital capability to successfully and secure implementation of AI technologies. AI makes it possible to combine semantics automatically. Languages and semantics change over time and AI mechanisms can enable them to be used more resiliently [5]. AI capabilities create potential for future business/education models and offer approaches which could intensify transfer of knowledge.

[Figure 2 Society 5.0 for SDGs]

Fig. 2 Society 5.0 for SDGs (Sustainable Development Goals) [17]

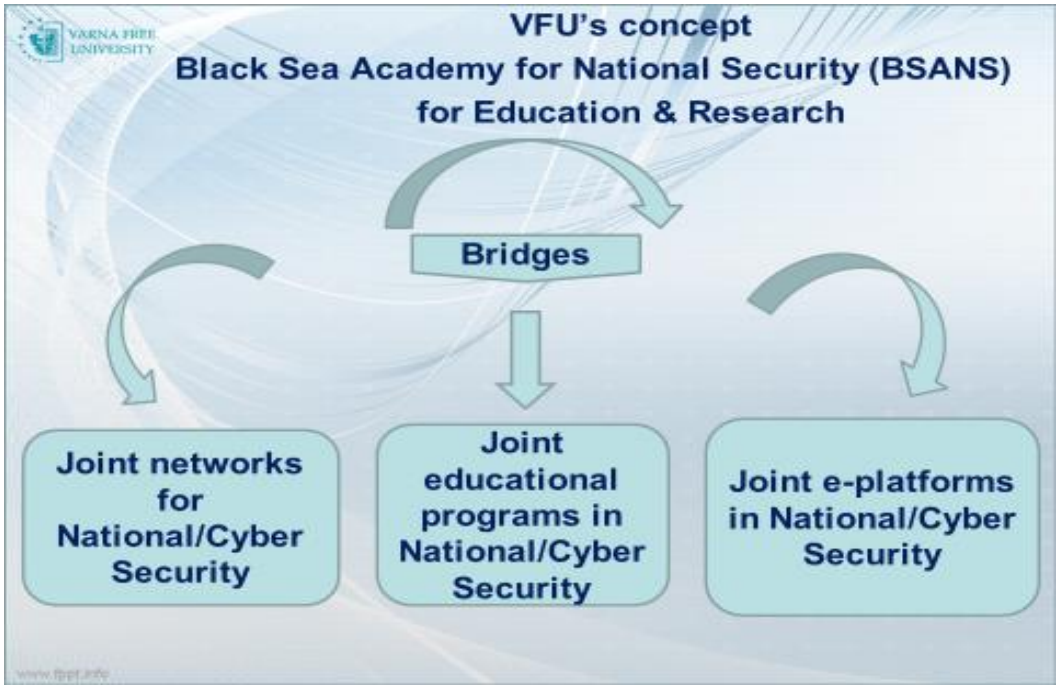
Suggestions and discussion

As already mentioned AI is adding new horizons to security solutions, research and education. In response to the challenges Varna Free University (VFU) is creating a concept establishing Black Sea Academy for National Security (BSANS). The Academy is designed to support training in M.D. programs “Cyber Security” and “Intelligent Security Systems”.

AI failures and attacks will grow in frequency and severity proportionate to AI’s capability. VFU’s project meets the needs for cooperation between universities, research institutions, business companies and NGOs to work to ensure top-level security education and development and popularization of cybersecurity culture and social responsibility. The project is inspired by the necessity all users to be aware of the many threats, the ways in which they operate, and the best options for protecting their devices, are all points on which

users should be focused in order to stay safe. An important challenge we face is the need to educate ourselves about how to be protected online, what types of information to publish, and which measures will ensure that information remains safe and private.

The aim of the BSANS is to cover most areas of security education as artificial intelligence techniques and concepts with influence on educational industry.



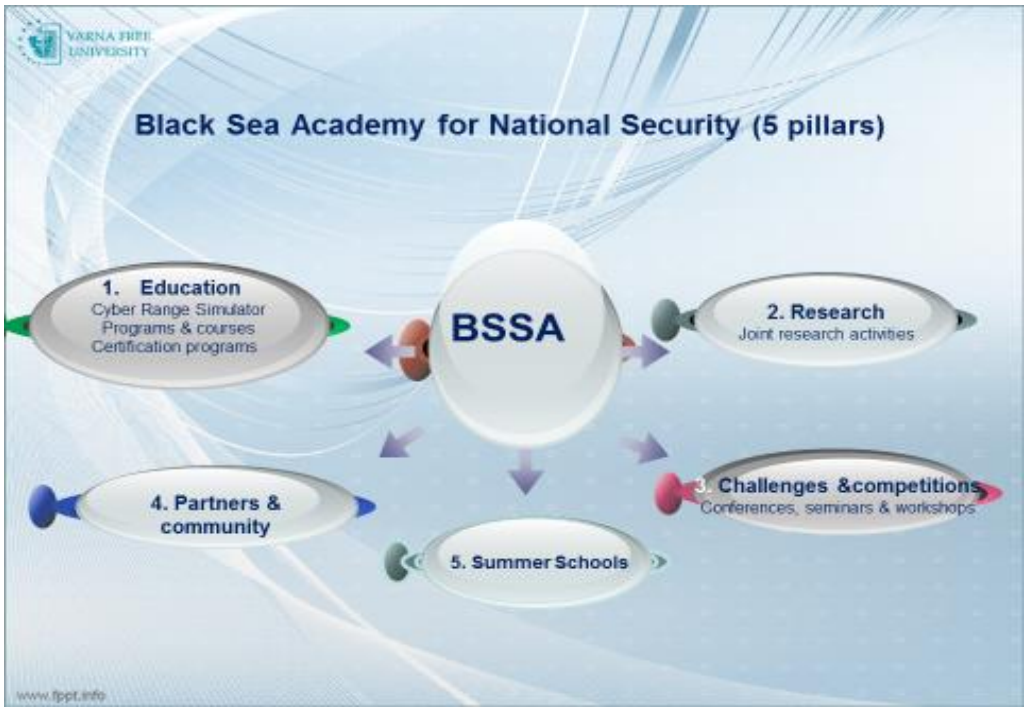
Black Sea Academy for National Security is an important step in placing Bulgaria at the center of achieving effective solutions against threats to national security, including cyber threats. Due to the dynamic changes in the Middle East, with direct effect on Bulgaria and other EU Member countries, the demand for highly qualified specialists in governmental and force structures is increasing

every year. One of the main goals of the Academy is to train and support experts in a wide range of national security disciplines as a center of excellence and to give an answer to the challenges in the Black Sea region, the Balkans and Central Europe.

The BSANS project of Varna Free University aims at developing joint platforms for education and research for elaborating effective and sustainable solutions for cyber risks and threats, sustainable strategies for digital defensibility and security of society as a whole, including organizations and citizens; stimulate knowledge development and exchange in the broad field of cyber security; develop an integrated vision on digital security.

Cyber Range Simulator environment is used to support security training courses and to prepare the trainees in encountering complex cyber incidents. The application of the simulator strengthens the communication expertise within the team, for coping with pressured situations and helps for implementation of work methodologies, including the subjects of ethics, decision-making, and escalation. The technical space includes advanced technologies related to AI, ML, Cloud Security, Privacy and Security, Big data and Analytics.

Simulation-based training has great advantages, as compared to traditional training. In a safe virtual environment processes and technologies could be tested and high-fidelity threat scenarios could be experienced. The suggested approach is an essential component of every security training, assessing, certifying, and maintaining the skill levels of security practitioners.



Conclusion

This paper presents some considerations on key steps for successful AI adoption and management into national security applications. A major finding of this effort is to outline the importance of workforce development and education.

Education and awareness should extend to the industries and sectors that previously were not so bound to information security. The importance of security issues in the critical infrastructure, the healthcare and the financial sector is raising continuously. 2020 is shaping up to be a year in which security challenges will continue to grow, even more so with the Covid 19 pandemic. Legislation and regulations, must accompany education and awareness. Legislative frameworks that promote security issues, ranging from the provision of formal education on security issues to properly protecting critical infrastructure have to be elaborated and adopted.

In this sense, it is also imperative that businesses commit to carrying out proper information security management and that developers don't prioritize usability over the security of their products.

Business companies, national and regional authorities together with universities should integrate efforts towards high-level security education with implementation of cutting-edge technologies.

References:

1. Hunter A., Sheppard L., et.al., Artificial Intelligence and National Security, A Report of the CSIS Defense-Industrial Initiatives Group, Center for Strategic and International Studies (CSIS), November 2018, pp.72

Available at:
https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181102_AI_interior.pdf?6jofgIIR0rJ2qFc3.TCg8jQ8p.Mpc81X

2. Artificial Intelligence and National Security, Congressional Research Service https://crsreports.congress.gov, R45178, November 21, 2019, pp.38

Available at:
https://fas.org/sgp/crs/natsec/R45178.pdf

3. Skrop A., Industry 4.0 - Challenges in Industrial Artificial Intelligence Conference Paper, II International Scientific Conference on Tourism and Security, Hungary, December 2018, pp.

Available at:
https://www.researchgate.net/publication/333601846_Industry_40_-_Challenges_in_Industrial_Artificial_Intelligence

4. Ervural Beyzanur Cayir and Bilal Ervural, Overview of Cyber Security in the Industry 4.0 Era, January 2019
https://www.researchgate.net/publication/319861803_Overview_of_Cyber_Security_in_the_Industry_40_Era

5. Technology Scenario 'Artificial Intelligence in Industrie 4.0', Federal Ministry for Economic Affairs and Energy (BMWi) Public Relations, Berlin, March 2019

https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/AI-in-Industrie4.0.pdf?__blob=publicationFile&v=5

6. Raffaele Cioffi , Marta Travaglioni , Giuseppina Piscitelli, Antonella Petrillo,and Fabio De Felice, Artificial Intelligence and Machine Learning Applications in Smart Production: Progress, Trends, and Directions, Sustainability 2020, 12, 492; doi:10.3390/su12020492
http://www.mdpi.com/2071-1050/12/2/492/pdf

7. Empowering Industry 4.0 with Artificial Intelligence, February 2020
https://www.dqindia.com/empowering-industry-4-0-artificial-intelligence/

8. Neel Achary, Artificial Intelligence to transform 10 Industries, March 2019
https://becominghuman.ai/artificial-intelligence-to-transform-10-industries-498338359f41

9. Claudio Cilli, Giulio Magnanini, On the security of the AI systems, February 2018
https://www.researchgate.net/publication/327868209_On_the_security_of_the_AI_systems

10. Artificial intelligence and the future of cybersecurity
https://www.researchgate.net/publication/254006500_Artificial_intelligence_and_the_future_of_cybersecurity

11. Prithvi Bhattacharya, Safeguarding Intelligent Decision-Making for Business: Towards A Model, March 2020
https://www.researchgate.net/publication/340693485_Safeguarding_Intelligent_Decision-Making_for_Business_Towards_A_Model

12. Greg Allen Taniel Chan, Artificial Intelligence and National Security, Belfer Center for Science and International Affairs, 2017, 132 pages https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

13. Alexander Babuta, Marion Oswald and Ardi Janjeva, Artificial Intelligence and UK National Security Policy Considerations, RUSI Occasional Paper, April 2020, 57 pages https://rusi.org/sites/default/files/ai_national_security_final_web_version.pdf

14. Remco Zwetsloot , Syllabus: Artificial Intelligence and International Security, July 2018, 19 pages https://www.fhi.ox.ac.uk/wp-content/uploads/Artificial-Intelligence-and-International-Security-Syllabus.pdf

15. WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020 COM(2020) 65 final, 27 pages https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

16. Society 5.0: Aiming for a New Human-centered Society

Japan's Science and Technology Policies for Addressing Global Social Challenges

https://www.hitachi.com/rev/archive/2017/r2017_06/trends/index.html

17. Özgür Önday, Japan’s Society 5.0: Going Beyond Industry 4.0, May 2019 https://www.researchgate.net/publication/333139463_Japan's_Society_50_Going_Beyond_Industry_40

18. P.O. Skobelev, S.Yu. Borovik, ON THE WAY FROM INDUSTRY 4.0 TO INDUSTRY 5.0: FROM DIGITAL MANUFACTURING

TO DIGITAL SOCIETY, INTERNATIONAL SCIENTIFIC JOURNAL "INDUSTRY 4.0", YEAR II, ISSUE 6, P.P. 307-311 (2017)
https://stumejournals.com/journals/i4/2017/6/307.full.pdf