# AI for Good Governance and Cybersecurity in the Western Balkans: Opportunities and Challenges

By: Ornela Sollaku,

DCAF Young Faces 2023 participant

**Abstract:**

In a world where new technology trends are rapidly moving, governments face many challenges related to emerging threats that came along with fast digitalization. This situation uncovers new challenges for the governments, which are under pressure to prove that they can meet any challenge and adapt quickly by minimizing losses. As governments face complex challenges, from cybersecurity threats to effective service delivery, the use of state-of-the-art tools to address these complex issues is essential. This policy paper delves into the use of Artificial intelligence in good governance and how it can improve cybersecurity techniques in the Western Balkans region. The WB region has, like other countries, become the target of cyber-attacks in increasing and more complex forms. This policy paper will attempt to show how the current situation relates to the search for practical solutions achieved with technologies such as AI as well as the challenges that may be encountered in its use, whether it has been applied elsewhere, and whether it has succeeded.

Keywords: Western Balkans, Good Governance, AI, Cybersecurity, Cyber Threats, EU legislation, Ethics.

**The current state of cybersecurity in the Western Balkans:**

The WB region, much like other countries, has become a target for increasingly complex cyber-attacks. This section provides an overview of the cybersecurity challenges and vulnerabilities specific to the region. It examines existing cybersecurity frameworks, policies, initiatives, identifies gaps and limitations in the current cybersecurity governance landscape. Furthermore, it discusses the shortcomings that hinder the implementation of robust cybersecurity protection systems. Cybersecurity was rightly defined as "coming of age"[1] back in 2021. The COVID era brought technology even more into our lives and it has shown that despite the positive impact that it may have, both private and public sectors, as well as individuals, are in danger and vulnerable.

This is considered to be the trend worldwide and the Western Balkans is no exception. The region has been subject to numerous instances of cyber attacks over the past decade, with the frequency and severity of attacks escalating in recent years. Such attacks have exposed the vulnerabilities of state mechanisms and raised questions regarding their effectiveness in safeguarding against emerging cyber threats. The consequences of these attacks have been significant, with critical infrastructure, government agencies, and private companies being impacted.

According to the PwC Cybersecurity ecosystem report for the Western Balkans. The biggest shortcomings that prevent the further implementation of better cybersecurity protection systems are *the administration techniques* of each government, *technical capacity*, and *social awareness.*

[1] Global Digital Trust Insights PwC, 2021

In terms of governance, national frameworks about cybersecurity are either incomplete or lack enforcement. The region's technical capacity is not as advanced as it should be, with outdated systems and equipment creating vulnerabilities, especially in the public sector, which attracts malicious actors. Additionally, there is a general lack of awareness about cyber risks and threats across all sectors of Western Balkans societies, which makes it more difficult to develop a resilient and less security-vulnerable society.

Finally, according to the Global Cybersecurity Index 2020, which categorizes member countries based on 82 questions related to cybersecurity commitments into five key areas: a) Legal Measures, b) Technical Measures, c) Organizational Measures, d) Measures for capacity development, and e) Measures for Cooperation, the situation in Western Balkans countries is as follows:

1. **Albania:** Ranked 80th out of 132 countries worldwide and 40th out of 46 European countries. The evaluation of cybersecurity measures taken by the country suggests that Albania has performed relatively well in legal measures, indicating it as a strength. However, there is room for improvement in suitable measures and capacity development.
2. **Bosnia-Herzegovina:** Ranked 110th out of 132 countries globally and 43rd out of 46 European countries. It is worth noting that Bosnia-Herzegovina is the only country in the Western Balkans region without a cybersecurity strategy at the state level, which highlights an area of concern.
3. **Kosovo:** Information about the current cybersecurity situation in Kosovo is not available in the Global Cybersecurity Index or the National Cybersecurity Index. However, it is mentioned that the country's situation is similar to that of the rest of the region, with an action plan that is still in draft form and not fully implemented.
4. **Montenegro:** Ranked 87th out of 132 countries globally and 41st out of 46 European countries. Montenegro' has shown relative strength in cooperative measures but needs further work in terms of capacity development.
5. **North Macedonia:** Ranked 38th out of 132 countries globally. The country's key strengths lie in legal and cooperative measures, while technical measures are considered weak points.
6. **Serbia:** Serbia ranked 39th out of 132 countries globally. Serbia has demonstrated relative strength in legal and technical measures. However, there is a need for significant improvement in capacity development.

The results of the Global Cybersecurity Index, as well as the increasing number of breaches that have occurred in the Western Balkans in recent years, show the need for the use of new technologies that can reduce threats to both countris and individuals. This approach should include effective cybersecurity strategies and the integration of advanced technologies, including artificial intelligence. In other words, WB countris should strengthen their enhanced civilian cybersecurity initiatives.

**Introduction to AI Enhancing Cybersecurity:**

Artificial intelligence (AI) has made its presence felt in the field of cybersecurity and, consequently that in people's daily lives. From searching machines like Google to generating AI tools such as chatbots, all use AI to operate. One of the most common uses of AI in the field of cybersecurity is malware and phishing detection. While AI offers significant opportunities for enhancing cybersecurity in the WB, challenges, and barriers to its adoption and implementation exist. This section discusses the opportunities of using AI in strengthening cybersecurity, such as advanced threat detection, vulnerability management, and continuous operation without time limitations. Additionally, it highlights challenges such as ethical considerations, legal frameworks, and societal implications that must be addressed to ensure responsible AI governance in cybersecurity.

AI has the potential[2] to significantly enhance cybersecurity. Some of the biggest positive effects AI can provide to cybersecurity include:

a. **Advanced threat detection:** AI can analyze vast amounts of data at any point, which enables the security system to detect quickly emerging threats. AI can identify patterns and anomalies, improving threat detectors' accuracy and speed.

b. **Enhance the vulnerability in the management:** The fact that AI algorithms can learn from historical data and user feedback allows the identification of vulnerabilities in the system. This proactive approach improves the overall security posture by reducing vulnerabilities of both system and human actors.

c. **No time limitations:** Unlike humans, AI operates 24/7 without any distractions. That gives AI the benefit of never getting tired and always being able to operate under any circumstances. Not only that, but also minimizes human error.

Even though AI can improve cybersecurity effectively, there are also some downsides that should be considered.

a. **Limited AI models:** AI models are only as good as the data they are trained on. If the training data is biased, incomplete, or not representative of the threat in question AI systems may make incorrect or biased decisions.

b. **Dependency and Over-Reliance[3]:** Over-reliance on AI systems can create a false sense of security. Human expertise and oversight remain essential to validate and interpret the output of AI algorithms, ensuring that critical decisions are not solely based on machine-generated results.

c. **Ethical and Privacy Concerns[4]:** The use of AI in cybersecurity raises ethical concerns related to privacy, transparency, and the potential for unintended consequences. Data privacy must be carefully managed, and AI systems should be developed and implemented with ethical frameworks and accountability.

[2] AI for Cybersecurity, Egnati team, 2023

[3] The hidden dangers of over-reliance on smart technology, Ilya Kalagin, 2023

[4] Pros and Cons of AI in Cybersecurity: Balancing Benefits and Ethical Concerns, CodeX, 2023

Regarding the latter, the most worrying drawbacks when referring to the Western Balkans s are the concerns about ethics and privacy. In order to fully exploit the benefits that AI can offer, it is essential to address the potential negatives that may arise. Implementing AI practices in the region is undoubtedly a challenge, but it is also a necessity to keep up with new advanced practices that are currently spreading worldwide. The right conditions must be created to ensure its optimal implementation.

The existence of highly effective technologies that can transform people's lives does not guarantee their ethical operation. To achieve ethical AI, a combination of factors is necessary, including the establishment of legal frameworks and technical measures to prevent the misuse of AI and ensure the safety of citizens.

Furthermore, it is important to adopt a human-centered[5] approach when implementing these practices. Citizens are most affected when it comes to cyber threats and their well-being should remain at the heart of AI development and implementation efforts.

## Legislation process: The EU case

In order to ensure all the above mentioned a strong political will combined with effective legal measures, shall eventually ensure the best performance of AI in the cybersecurity space. It is widely recognized that all Western Balkans countries are in the process of pursuing EU membership, with some countries being further along in this process than others are. In order to meet the criteria, set forth by the EU for membership, it is imperative for these countries to align their policies with those of the EU. This includes the integration of AI into cybersecurity practices, where the EU serves as a valuable example for the Western Balkans. However, how the EU performs on that?

The EU is taking steps to regulate artificial intelligence (AI) as part of its digital strategy, with the aim to ensure safe and beneficial development of this technology. In April 2021[6], the European Commission proposed the world's first regulatory framework for AI, which is currently under review. The European Parliament supports the initiative and has outlined its priorities for AI legislation, including the need for *safe, transparent,* and *accountable* AI systems. They advocate for human oversight and a uniform definition of AI. The proposed **AI Act** introduces different regulations based on the risk levels associated with AI systems. *a) Unacceptable risk* AI systems, such as those involving cognitive manipulation or social scoring, will be banned. b) *High-risk* AI systems will be categorized into two groups: those used in specific products and those operating in critical areas like biometric identification, education, and law enforcement. All high-risk AI systems will undergo assessment before and during their use. Generative AI systems, like ChatGPT, will have to meet transparency requirements, including disclosure and prevention of illegal content generation. c) AI systems with *limited risk* should meet minimum transparency standards, enabling users to make informed decisions. The European Parliament adopted its negotiating position on the AI Act in June 2023, and negotiations with EU countries are underway with the aim of reaching an agreement by the end of the year.

## Conclusions and policy recommendations:

[5] Cybersecurity and Human Rights in the Western Balkans: Mapping Governance and actors, DCAF, 2023

[6] European Parliament, 2023

The European Union's proposed regulations on AI carry significant implications not only for EU member countries but also for regions beyond its borders, such as the Western Balkans. As the EU takes the lead in establishing the world's first comprehensive AI rules, it sets a precedent for responsible and ethical AI development. Given the increasing integration of the Western Balkans with the EU, it becomes crucial for countries in the region to align their AI policies with the EU's framework. By doing so, they can foster a harmonized approach to AI governance, ensuring the safe and beneficial deployment of AI technologies, that can also lead to more efficient cybersecurity policies. This alignment would promote regional collaboration, facilitate the exchange of expertise, and enable the Western Balkans to leverage AI for their socioeconomic development. Therefore, it is imperative for the Western Balkan countries to proactively embrace AI regulations and actively participate in shaping the future AI landscape. With this in mind, the following policy suggestions aim to guide the development of an effective AI policy framework for the Western Balkans. These policy suggestions refer to both private and public sectors, while governments and civil society have the biggest role in promoting all the suggestions below:

1. **Enhancing cybersecurity infrastructure.** a) Invest in modernizing cybersecurity infrastructure including hardware, software, and network capabilities. b) Invest in academia and research. The main supporters of this proposal are the governments themselves. There should be a strengthening of public sector cybersecurity policies and practices, through various investments. Public sectors' computer systems and online services are a public good and their security, transparency, and efficiency must be ensured for all the citizens. In order to make this possible, modern hardware, software and network are essential to have an up to date and efficient systems. Also, there should be tax relief for private cybersecurity centers. Encouraging private companies to set up cybersecurity hubs, as a practical way to promote the development of cybersecurity skills among young people. The formation of a skilled workforce benefits not only the companies, but also young people. Both private and public sector should join forces, to share information and practices related to effective cybersecurity practices.
2. **Promoting collaboration and information sharing both domestically and internationally,** by encourage cross-border cooperation within the region to address cyber threat effectively. Civil Society from all over the region can play a significant role in the promotion of collaboration between the countries via seminars, workshops and research publication. All these initiatives, can bring together stakeholders form various sectors to exchange knowledge on cybersecurity policies. In addition, by strengthening cooperation with international partners, such as the European Union, NATO, and neighboring countries is vital to align cybersecurity policies and share best practices.

3. **Ethical considerations and data privacy.** Governments across the Western Balkans need to formulate clear guidelines and regulations governing the ethical use of AI in cybersecurity. These guidelines should prioritize transparency, fairness and accountability. To achieve this, it is necessary to establish legal frameworks that are in line with international standards, especially as all countries in the region are in the process of joining the EU. Adherence to established EU standards, such as the General Data Protection Regulation (GDPR), becomes imperative to ensure individuals' privacy rights and responsible data governance.
4. **Public awareness and education.** Both governments and civil society, should pay attention on the awareness of the citizens as they are the most affected any form of cyber threat. This can be achieved by launching public awareness campaigns to educate citizens, businesses, and governmental institutions about the importance of cybersecurity and the role of a responsible using of AI, in enhancing cybersecurity measures.

**Bibliography:**

Egnati Team (2023). 8 benefits of using AI in cybersecurity. [online] Engati. Available at: https://www.engati.com/blog/ai-for-cybersecurity. [Accessed 4 May 2023].

European Parliament (2023). EU AI Act: first regulation on artificial intelligence. Available at: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?&at_campaign=20226-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=RSA&at_goal=TR_G&at_advertiser=Webcomm&at_audience=ai%20regulation&at_topic=Artificial_intelligence_Act&at_location=GR&gclid=CjwKCAjw-vmkBhBMEiwAlrMeF7TbOeurULUOq2DH47SdqIKXOKmmf43t9si2cZMRc2mJAA4yRPg5BhoC1ywQAvD_BwE [Accessed 16 June 2023].

Global Cybersecurity Index 2020 International Telecommunication Union Development Sector. (2021). Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. [Accessed 15 May 2023].

Kalagin, I. (2023). The hidden dangers of Over-reliance on Smart Technology and AI. [online] www.linkedin.com. Available at: https://www.linkedin.com/pulse/hidden-dangers-over-reliance-smart-technology-ai-dr-ilya-kalagin [Accessed 4 May 2023].

Merali , L. and Bavčić , E. (2022). Cybersecurity and Human Rights in the Western Balkans: MAPPING GOVERNANCE AND ACTORS. [online] DCAF. Available at: file:///C:/Users/ornel/Downloads/CybersecurityHumanRightsWesternBalkans_EN_March2023.pdf [Accessed 15 May 2023].

NCSI (n.d.). National Cyber Security Index. [online] ncsi.ega.ee. Available at: https://ncsi.ega.ee/. [Accessed 15 May 2023].

PricewaterhouseCoopers (2021). Global Digital Trust Insights 2021. [online] PwC. Available at: https://www.pwc.com/jg/en/publications/digital-trust-insights.html [Accessed 4 May 2023].

PWC (2022). Cybersecurity Ecosystem Report Western Balkans: Emerging Cyber threats. [online] PWC. Available at: file:///C:/Users/ornel/Downloads/PwC-Cybersecurity-Ecosystem-Report-WB.pdf [Accessed 15 May 2023].

Today, A. (2023). Pros and Cons of AI in Cybersecurity: Balancing Benefits and Ethical Concerns. [online] CodeX. Available at: https://medium.com/codex/pros-and-cons-of-ai-in-cybersecurity-balancing-benefits-and-ethical-concerns-6a37d98835a0 [Accessed 15 May 2023].