Artificial Intelligence in Cybersecurity: *A Survey of National Research, Investment and Policy Implementation*

Taylor Rodriguez Vance[1]

Doctoral Student of Artificial Intelligence and Cybersecurity

Capitol Technology University, District of Columbia, USA

DOI: https://doi.org/10.5281/zenodo.7858980

Published Date: 24-April-2023

Abstract: **As AI technology advances, so do the challenges and risks associated with cybersecurity. To address these challenges, policymakers have been developing AI policies that aim to regulate and govern the development and use of AI in various domains, including cybersecurity. In this paper, we explore the current state of AI policy and its implications for cybersecurity. This paper provides an analysis of the strengths and weaknesses of existing AI policies and an examination of their potential impact on cybersecurity. The goal of this research is to provide insights and recommendations to policymakers and stakeholders on how to develop effective AI policies that promote cybersecurity while fostering innovation and growth in the AI industry.**

Keywords: **Artificial Intelligence; Cybersecurity; international policy, Artificial Intelligence investments, national defense.**

I. INTRODUCTION

The expansion of advanced technology such as Artificial Intelligence and Machine Learning in the commercial industries has led to the interest in research for those technologies in the private industry as well. Much like similar fields such as cloud computing, Artificial Intelligence and Machine Learning has evolved through the industry lifecycle phases. While other advanced technologies are squarely in Stage 1: Market Development and Stage 2: Market Growth, Artificial Intelligence appears to be within Stage 3: Market Maturity [1]. This is due to a variety of factors that prove out an industry's maturity, including the level of research in the field, applications in the field, existing policies in the field, and investments in the field overall. Notably, industries that are in Stage 3 are where public entities begin to seriously invest and develop in the field. More recently, it has been stated that the cyber domain represents one of the most prominent potential application of Artificial Intelligence. Artificial Intelligence (AI) is transforming various aspects of our lives, including cybersecurity.

II. METHODOLOGY

The results of this research were identified through the evaluation of several criteria relating to Artificial Intelligence in Cybersecurity. Scientific research publications published within the last 5 years, the number of policies existing by government type, government spending in Artificial Intelligence, and venture capital investment in Artificial Intelligence. The primary sources for this research were the OECD. AI database, Google Scholar Databases, and National Strategy and Spending Reports. The goal of this research is to identify the current state of Artificial Intelligence in Cybersecurity with the outcomes being identified gaps, opportunities, and areas of focus in this field for government entities.

III. RESULTS

A. *Scientific Research Publications in the Field*

The data trends associated with scientific publications have been noted to indicate an overall field growth or decline. With the assumption that interest in a field begins with scientific research, the trends in the number of publications per key words can be evaluated in this paper. This section of the paper will review the number of publications in various areas of the field to include, Artificial Intelligence, Cybersecurity, and National Security. Several sources were utilized to identify the number of publications to include Google Scholar. The number of publications can be used to determine the funding, interest, maturity, and other significant factors of a field. Throughout this section, it will be evident what the areas of focus within Artificial Intelligence.

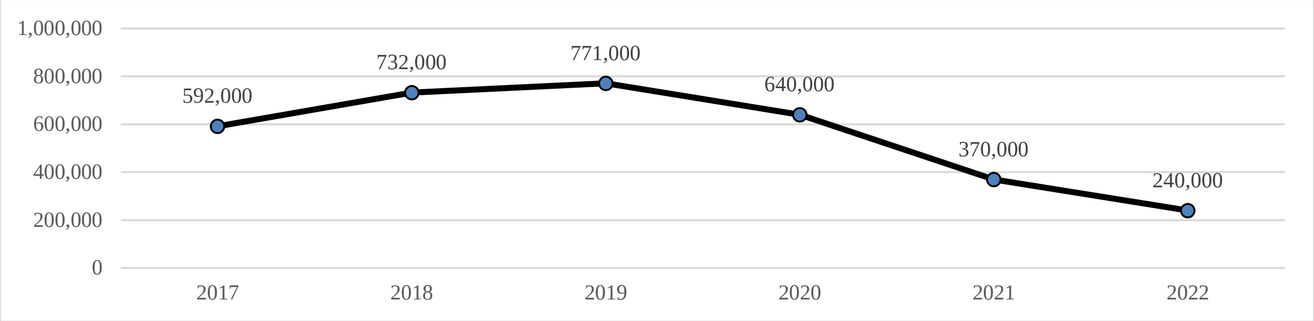

Figure 1 - Number of Publications with Keywords: Artificial Intelligence

Figure 1 shows research publications with the key terms Artificial Intelligence equaled roughly 592,000 publications in 2017 and gradually declined to roughly 240,000 publications in 2022. The number of publications continued to trend downwards. The peak of the publications occurred in 2019 and ended with the lowest number of publications in 2022. When reviewing the number of publications with the specific keywords, there is an increase between 2017 and 2019, then a significant and persistent decline from 2019 to 2022. With such a drastic decrease in scientific publications that are solely focused on Artificial Intelligence, there a few hypotheses that could be made. Firstly, the decrease could indicate that the focus of research deepened to more specific applications and/or areas of the field, which can be reviewed in subsequent analyses.

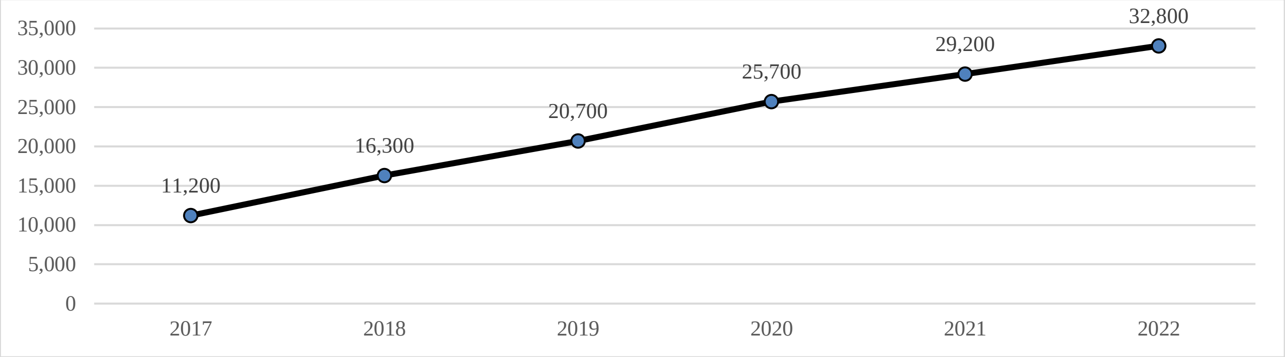

Figure 2- Number of Publications with Keywords: Artificial Intelligence, Cybersecurity

Figure 2 shows research publications with the key terms Artificial Intelligence and Cybersecurity equaled roughly 11,200 publications in 2017 and gradually increased to roughly 32,800 publications in 2022. The number of publications continued to trend upwards. The peak of publications occurred in 2022. In contrast to the data for the key terms of "Artificial Intelligence", there was a steady increase from 2017 to 2022 in scientific publications with the key terms of "Artificial Intelligence, Cybersecurity". The increase aligns with other key terms in fields that are growing in maturity and interest. The steady increase in number of publications represent the interest in research for Artificial Intelligence in Cybersecurity. The steady increase does note an interesting point that there did not seem to be an impact on the scientific publications for these key terms by COVID-19.

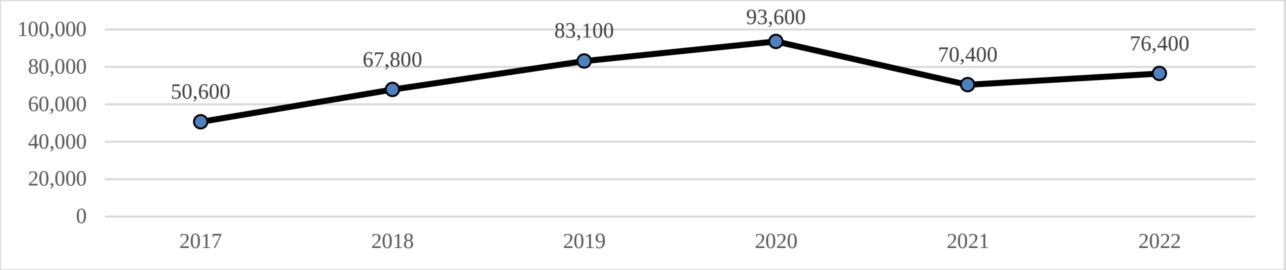

Figure 3 - Number of Publications with Keywords: Artificial Intelligence, National Security

Figure 3 shows research publications with the key terms Artificial Intelligence and National Security equaled roughly 50,600 publications in 2017 and roughly 76,400 publications in 2022. The number of publications trended upwards until 2020, with a steep decline in 2021 with another gradual increase in 2022. The peak of publications occurred in 2020 with over 15,000 more published that year than in 2022. In an interesting data trend, there was a peak of publications with the "Artificial Intelligence and National Security" key words in 2020, with a decrease in 2021 and then another minor increase in 2022. This is an intriguing data point as there was a significant peak in publications in 2020. This does require further analysis than conducted in this research paper as to the core impetus of the peak in research in 2020. Further, the publications increased from 2021 to 2022, seemingly as expected relating to the development of the field of Artificial Intelligence and the interest of governments to focus on how to combat, utilize, and understand this advanced technology. The decline in 2021 could be attributed to the COVID-19 pandemic where there was a decline in funding along with all limitations that accompanied advanced research during the pandemic.

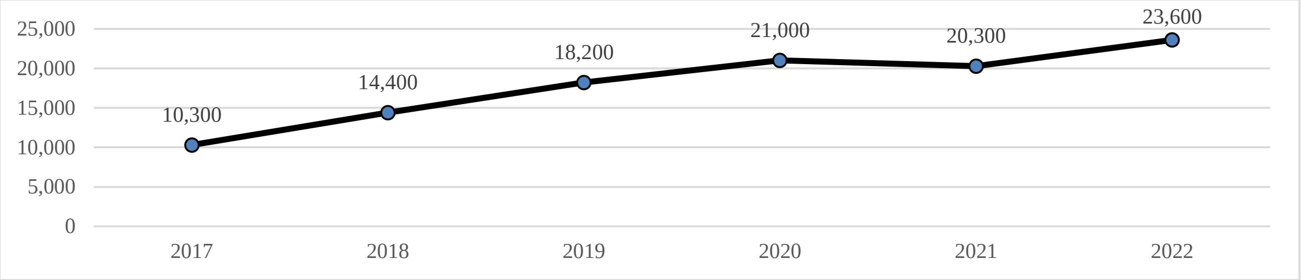

Figure 4 - Number of Publications with Keywords: Artificial Intelligence, Cybersecurity, National Security

Figure 4 shows research publications with the key terms Artificial Intelligence, Cybersecurity, and National Security equaled roughly 10,300 publications in 2017 and roughly 23,600 publications in 2022. The number of publications trended upwards overall but it is important to note the slight decline in publications in 2021. The peak of the publications occurred in 2022. Similar to the publications for the key terms "Artificial Intelligence and National Security", the scientific publications for "Artificial Intelligence, Cybersecurity, and National Security" showed a steady increase from 2017 to 2020, with a slight decline in 2021 and another increase in 2022. The decline in 2021 could be attributed to the COVID-19 pandemic where there was a decline in funding along with all limitations that accompanied advanced research during the pandemic.

B. Existing Policies in the Field

To get to the results of the findings in this section, the policy items that were evaluated solely fall under the Government Entities. The data was pulled from the OECD.AI Policy Observatory database. This database includes a live repository of over 800 AI policy initiatives from 69 countries, territories, and the European Union. Further, the sub-categories of data include policy instruments from National Governments, Sub-national Governments, and International Entities. Overall, there were a total number of 548 policy instruments that are categorized under Governmental Entities. The number, detail, and depth of existing policies can be another indicator as the maturity of a field. Throughout the course of this research, the types of Artificial Intelligence policy instruments were reviewed and evaluated by three categories; National Governments, Sub-National Governments, and International entities. It is important to note that these are policy instruments that fall under Artificial Intelligence and the data is not specific to either Cybersecurity or National Security policy instruments. The results discussed in a previous section will be analyzed below.

1) National Governments

According to the international database, the largest number of policy instruments are associated with National Strategies, Agendas, and Plans, Emerging AI Related Regulation, and Public Consultations of stakeholders or experts. The data is an aggregate of the review of only the participating countries in the OECD study and do not represent all National Governments globally. There is a total of 505 policy instruments that are categorized under National Governments. A national government is a government with members from more than one political party, especially one that is formed during a crisis. In Figure 5, it is evident that the largest number of policy instruments for international entities fall under National Strategies, Agendas, and Plans, Emerging AI Related Regulation, and Public Consultations of Stakeholders and Experts. It can be determined that the largest number of policy instruments belonging to National Strategies, Agenda, and Plans align with the National Governments focus on keeping up with the evolution of advanced technology. Additionally, there are Emerging AI related regulation that are a high number for National Governments due to the focus on international cooperation and the policy development that is occurring globally.

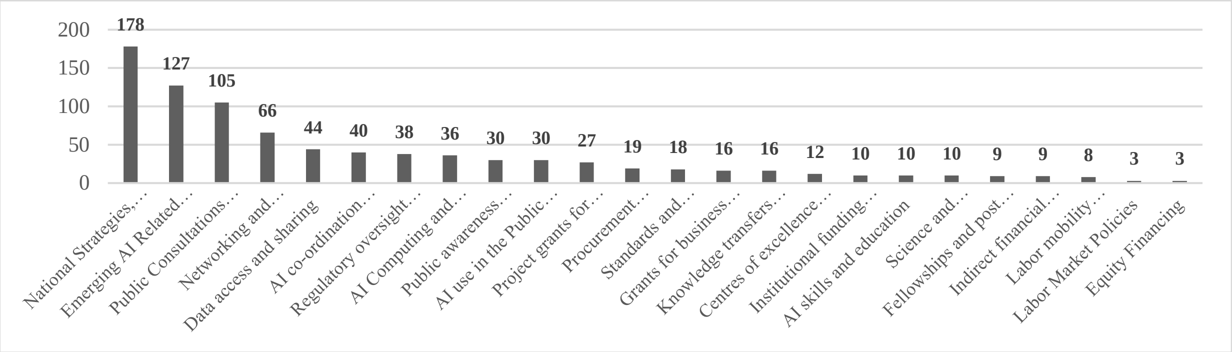

Figure 1 - Types of Policy Instruments by National Government

2) Sub-National Governments

According to the international database, the largest number of policy instruments are associated with National Strategies, Agendas, and Plans, Public Consultations of stakeholders or experts, and Networking and Collaborative Platforms. The data is an aggregate of the review of only the participating countries in the OECD study and do not represent all Sub-National Governments globally. There is a total of 107 policy instruments that are categorized under Sub-National Governments. A subnational government (SNG) is defined as a decentralized entity whose governance bodies are elected through universal suffrage and which has general responsibilities and some autonomy with respect to budget, staff and assets. In Figure 6, it is evident that the largest number of policy instruments for international entities fall under National Strategies, Networking and Collaborative Platforms, and Public Consultations of Stakeholders and Experts. This type of government had a different top of three policy instruments, including Networking and Collaborative Platforms.

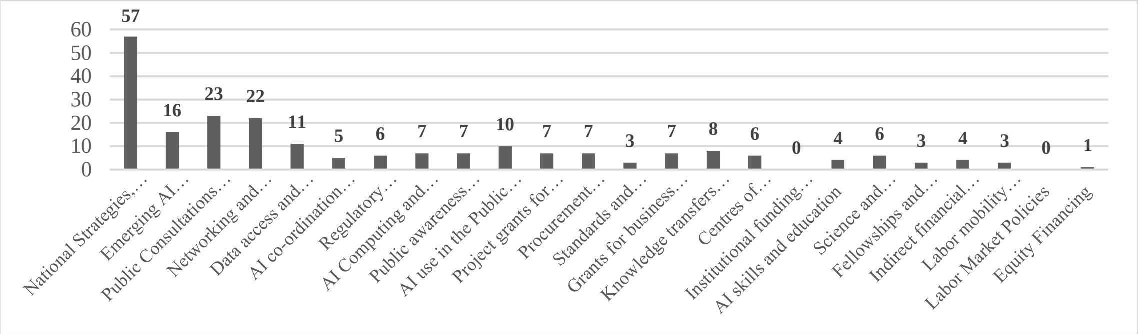

Figure 2 - Types of Policy Instruments by Sub-National Governments

3) International Entities

According to the international database, the largest number of policy instruments are associated with National Strategies, Agendas, and Plans, Emerging AI Related Regulation, and Public Consultations of stakeholders or experts. The data is an aggregate of the review of only the participating countries in the OECD study and do not represent all International Entities globally. There is a total of 101 policy instruments that are categorized under International Entities. International entities are entities established by formal political agreements between their members that have the status of international treaties; their existence is recognized by law in their member countries; they are not treated as resident institutional units of the countries in which they are located. In Figure 7, it is evident that the largest number of policy instruments for international entities fall under National Strategies, Agendas, and Plans, Emerging AI Related Regulation, and Public Consultations of Stakeholders and Experts. International Entities had the same top three policy instruments as National Governments.

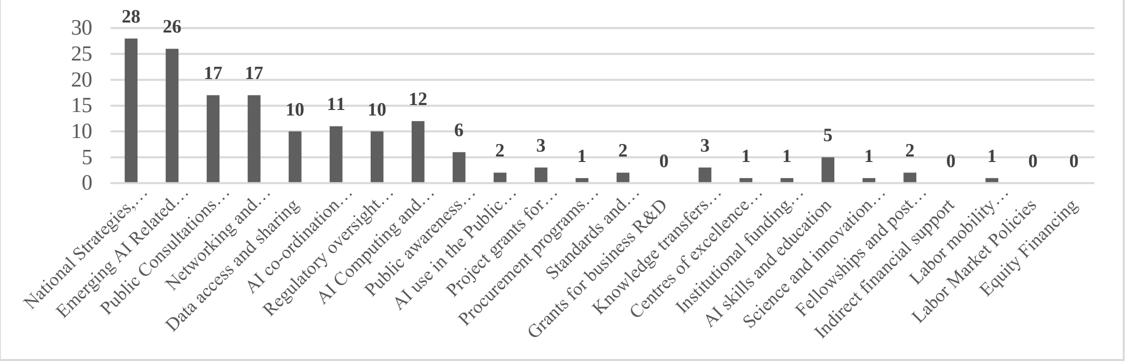

Figure 3- Types of Policy Instruments by International Entities

C. Investments in the Field

The investments that are made into certain fields can be an indicator of the strength, growth, and vitality of an industry. Investments that were reviewed and included in this research included venture capital investments as well as government spending. The investment amounts were primarily focused on Artificial Intelligence by industry or investment vehicle and do not specifically focus on the investment in Cybersecurity or National Security in Artificial Intelligence. The dollar amount invested in fields is a large determining factor in understanding the maturity and focus of that field. With Artificial Intelligence growing a fast rate, the data points to agreement in both the private and public investments into this field. When evaluating the venture capital investment data, it can be seen that there is significant investment in several industries with mobility and autonomous vehicles and healthcare. One key finding that is important to note is that Digital Security has been consistently receiving the lowest amount of venture capital investment. As the amount of the spending by government is evaluated later in the paper, it is typically spent on security and robotics.

1) Venture Capital Investments

According to the OECD.AI database, the worldwide Venture Capital (VC) investments in Artificial Intelligence by industry show that the highest investments by US dollar (USD) is in the Mobility and autonomous vehicles industry. The industry of focus for this study is in Digital Security, which is the lowest investment by USD for all industries. The amount of investments trend upwards for all industries.

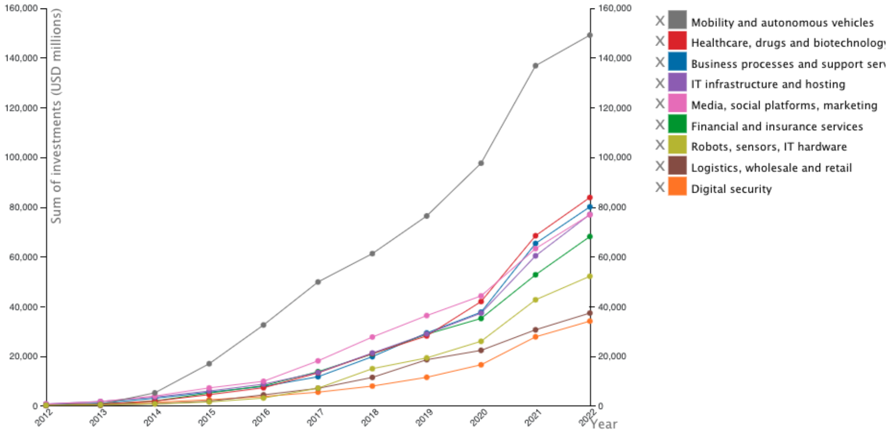

Figure 4 - Worldwide VC Investments in AI by Industry

Further, Venture Capital investments can be an indicator of the growth of this... According to the OECD.AI database, the United States has the largest investment in Artificial Intelligence with Great Britain, European Union, China and Israel. The United States has 13, 062 deals with a 304,449 million in sums of the deals. China closely follows with 7,000 deals with a 304,449 million in sums of the deals.

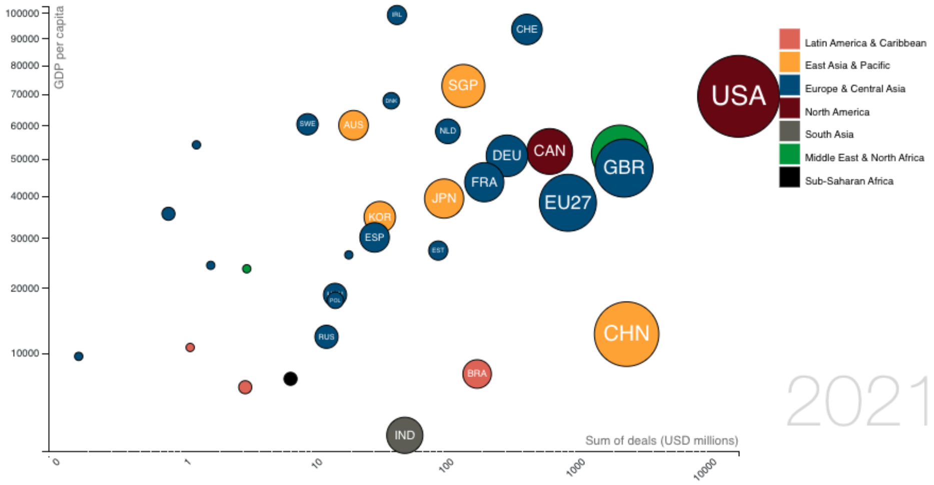

Figure 5 - VC Investments in AI vs. GDP per capita by Country

2) Government Investments

According to the OECD.AI research project, government spending on Artificial Intelligence has also increased at an increased rate. In 2001, funding streams for AI related research and development were around 207 million USD. The funding streams increased over the years to almost 3.6 billion USD in 2019. It is important to note that these numbers do not fully represent the true growth as not all data was available for review at the time of the project. DOD's contract spending on AI and ML is projected to reach $1.4 billion in fiscal year 2020, up 43 percent from the $973 million obligated in FY-19, according to market research published by Bloomberg Government analyst Chris Cornillie.

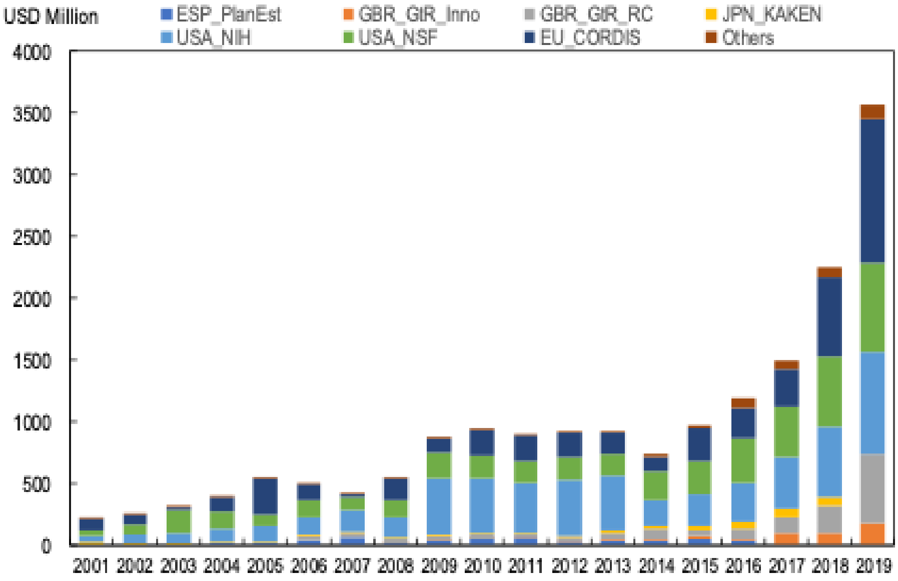

Figure 6 - Spending per Research Group

Thirteen government agencies were examined during the OECD research project. The top three sources for AI-related research and development were the EU's Community Research and Development Information Service (CORDIS), the US's National Institutes of Health (NIH), and the National Science Foundation (NSF). The NIH and NSF, two US agencies account for over three-quarters of the cumulated AI R&D funding that were documented in this project.

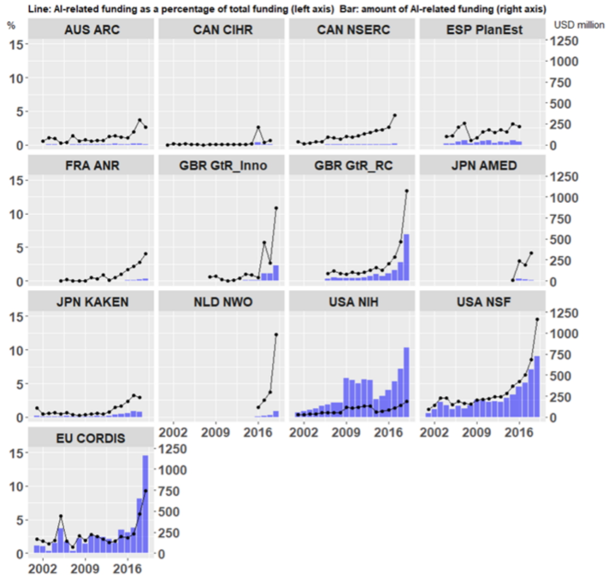

Figure 7 - Spending by Group (Detailed)

The increased investment in research and development in National Science Foundation and National Institute of Health can be seen in Figure 11. This is important to note due to the increased investment in research and development that is evident for the United States for Artificial Intelligence. The National Science Foundation is the primary funding vehicle for the Artificial Intelligence research that this paper focuses on due to research topics needing to focus on Cybersecurity research in AI.

IV. FUTURE WORK

There are opportunities for future research that focuses on the actual applications of Artificial Intelligence in Cybersecurity for national defense. Research may be explored to identify the current applications and prospected future applications to the field. Much like in most policy areas, there are many opportunities for research in the likelihood, interest, current state, and potential issues with international cooperation in Artificial Intelligence in Cybersecurity. There is additional future research that could focus on Artificial Intelligence in Cybersecurity specifically for National Security. There are many areas of focus when Artificial Intelligence is researched, however, one key area should be the ethical utilization of it in National Defense. This will be a key focus of this research as it is important to understand the responsibilities of governments in the ethical use of Artificial Intelligence for National Security. A natural progression to this research are the research opportunities on the overall development of Artificial Intelligence for National Security around the globe.

V. CONCLUSION

In conclusion, this paper has examined the implications of AI policy on cybersecurity. We have highlighted the importance of policymakers and stakeholders in developing effective AI policies that promote innovation, growth, and security. Our analysis has shown that current AI policies have strengths and weaknesses that need to be addressed to effectively govern AI in cybersecurity. We recommend that policymakers prioritize transparency, accountability, and ethical considerations when developing AI policies to ensure that they align with societal values and promote public trust in AI. Furthermore, stakeholders in the cybersecurity industry should collaborate with policymakers to identify potential threats and vulnerabilities associated with the use of AI and develop appropriate measures to mitigate them. As AI technology continues to evolve, policymakers and stakeholders must remain vigilant in adapting policies and practices to maintain cybersecurity while promoting the benefits of AI.

REFERENCES

[1] Berryhill, J., et al. (2019), "Hello, World: Artificial Intelligence and its use in the public sector", OECD Working Papers on Public Governance, No. 36, OECD Publishing, Paris, https://doi.org/10.1787/726fd39d-en.

[2] Jeffrey L. Caton, "Beyond domains beyond commons: Context and theory of conflict in cyberspace", Cyber Conflict (CYCON) 2012 4th International Conference on, pp. 1-11, 2012.

[3] Caitríona H. Heinl, "Artificial (intelligent) agents and active cyber Defence: Policy implications", Cyber Conflict (CyCon 2014) 2014 6th International Conference On, pp. 53-66, 2014.

[4] R. V. Yampolskiy, "Taxonomy of Pathways to Dangerous Artificial Intelligence," in Workshops at the Thirtieth AAAI Conference on Artificial Intelligence, 2016.

[5] F. Pistono and R. V. Yampolskiy, "Unethical Research: How to Create a Malevolent Artificial Intelligence," presented at the 25th International Joint Conference on Artificial Intelligence (IJCAI-16). Ethics for Artificial Intelligence Workshop (AI-Ethics-2016), New York, NY, July 9, 2016.

[6] K. Sotala and R. V. Yampolskiy, "Responses to Catastrophic AGI Risk: A Survey," Physica Scripta, vol. 90, 2015.

[7] E. Yudkowsky, "Artificial Intelligence as a positive and negative factor in global risk," Global catastrophic risks, vol. 1, p. 303, 2008.

[8] R. V. Yampolskiy, Artificial Superintelligence: A Futuristic Approach: Chapman and Hall/CRC, 2015.

[9] S. Morgan. (Jun 2019). Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017–2021. Cybercrime Magazine. Accessed: Dec. 22, 2019. [Online]. Available: https://Cybersecurityventures.com/ Cybersecurity-market-report/

[10] Statista Research Department. (Aug 2019). Spending on Cybersecurity in the United States From 2010 to 2018. Accessed: Dec. 22, 2019. [Online]. Available: https://www.statista.com/statistics/615450/Cybersecurity- spending-in-the-us/

[11] Wall Street. (Aug. 2018). How Artificial Intelligence and Machine Learning Will Impact Cyber Security. Accessed: Jan. 5, 2020. [Online]. Available: https://wall-street.com/how-artificial-intelligence- and-machine-learning-will-impact-cyber-security/