What Does Resilience-Building to Emerging and Disruptive Technologies Actually Look Like? A Study Addressing the Public Policy Challenges and Socio-Political Implications of the Development of Artificial Intelligence for NATO Security and Defense in Continental Europe

Kulani Abendroth-Dias
Brussels, 1000
BELGIUM

kulanidias@gmail.com

ABSTRACT

Digital technologies have proliferated rapidly over the past two decades, from the spread of mobile broadband networks, to the use of cryptocurrencies, to the use and abuse of artificial intelligence (AI) and machine learning (ML) for security and defence (Spiegeleire, Maas, & Sweijs, 2017). AI now has vast implications for not only defence but also economic and social fairness. Uses and misuses of AI and ML-driven technologies have been made clear during the COVID-19 pandemic, with their use in contact tracing and abuse in the spread of misinformation to sow civic unrest and erode public trust in government institutions. The need to build both military and civilian resilience to AI- and ML-driven malignant attacks has become painfully evident. This research brings together often disparate discussions on the development of AI across European NATO nations to present social, economic, political, legal, and technical ways forward to resilience-building. The study presents interviews with 22 European NATO stakeholders, comprising policy-makers, academics, and industry and non-profit actors, on behaviourally informed ways to build resilience to cyberattacks in military and civilian domains across the EU. Ten policy insights operationalising resilience and civic trust-building are presented, based on a content coding of the role of counter-AI agencies, practical approaches to mitigating risk, addressing bias in datasets, developing human-centered automated systems, and current policy and industry priorities in the economics of the development of AI- and ML-driven technologies. The role of the private sector and the asymmetric development and implementation of AI- and ML-driven technologies across European NATO member states are discussed.

1.0 INTRODUCTION

Artificial intelligence, physical security, and political security are inextricably linked in the Digital Age (Bostrom, & Yudkowsky, 2014). Largely due to advances in computing power, machine learning algorithms, deep neural networks, access to datasets, and gains in standard software frameworks that allow for exponential iteration and replication of experiments, artificial intelligence (AI) and machine learning (ML) have progressed rapidly over the past few years (Brundage et al., 2018). At the core of this growth is expanded commercial investment in developing the capacities that feed AI and ML-driven technologies (Chui, 2017; Jordan and Mitchell, 2015).

AI now drives a variety of widely available technologies, such as automatic speech recognition, facial analysis, contact tracing, search engines, spam filters, and self-driving cars (Das, Dey, Pal, & Roy, 2015). In many countries, the COVID-19 pandemic has loosened the regulations on the use of the data that feed AI and ML driven technologies (Dam, 2020, Raskar et al., 2020). For example, in South Korea, immigration databases were used by health officials to increase population surveillance techniques to contract trace those who may have been exposed to COVID-19 (Migration Data Portal, 2020). This increased access to data can fuel the development of the technologies used as digital assistants for nurses and doctors and drones for expedited disaster and pandemic monitoring and relief (Oliver et al., 2020; Raskar et al., 2020; Zwitter & Gstrein, 2020). AI-powered driverless cars and robotic dogs to encourage social distancing (among other social interactions) can be helpful to combat the effects of a pandemic that is fought with behavioural containment and even social isolation (Bavel et al., 2020). It is, however, easy to see how the developments that drive AI- and ML-driven technologies can easily be used for malicious purposes, e.g. weaponising consumer drones, hacking public services, create privacy-deficient surveillance states, racial profiling, repression, and targeted disinformation campaigns to name a few (Brundage, 2018; Johnson, 2017; Tucker et al., 2018). Just as doctors, patients, and the pharmaceutical industry need to understand how a human body works and the symptoms and diseases that can impact our well-being to develop medicines that can protect against ill health, both the regulators and users of AI-driven technologies (i.e. policy-makers, the military, technological developers, and the public) need a better understanding of what constitutes AI and ML-driven technologies and their current and potential uses and misuses to build resilience to their malignant use (Bahnsen, Torroledo, Camacho, & Villegas, 2018).

The need to build resilience to AI and ML-driven technologies is often discussed in policy circles. However, little attention has been paid to operationalising resilience-building to the rapid development of AI- and ML-driven technologies across the continent. At its core, resilience requires inclusive and forward-thinking regulation and research that can build flexibility to respond to evolving security challenges. Developing resilience to AI- and ML-driven attacks is a central tenet to building citizen trust. Cyberattacks that mine citizen data, for example, lead the public to question the robustness of their political and public structures, and work to undermine trust in governments and political participation (Brkan, 2019). At its core, resilience requires inclusive and forward-thinking regulation and research that can build flexibility to respond to evolving security challenges. Developing resilience to AI- and ML-driven attacks is a central tenet to building citizen trust.

There are several key challenges to developing and regulating AI-driven technologies, including the application of technology developed outside Europe that can threaten its sovereignty, and the legal basis for regulating technology that is re-shaping global political and economic structures (Timmers, 2020). This paper offers insights to address these challenges.

Resilience-building should inform how we design and distribute AI systems, and *who* should design and distribute them. Drawing from a content analysis of 22 interviews, this project presents an analysis of how resilience building with regard to AI- and ML-driven technologies is currently understood by policy-makers, industrial agents, non-profit actors, and academics who work on understanding, developing, and/or regulating AI- and ML-driven technologies for European security and defence. The goal of this research is to contribute to the technology-security research nexus by presenting the cross-cutting effects of the development of AI and ML-driven technologies for European security and defence along national, supranational, economic, and political levels.

2.0 METHODOLOGY

2.1 Participants

Fifty-three individuals were contacted between February and May 2020 via a standard email message that included an outline of the study with the author's background and credentials. The final sample comprised 22 participants (55% female), i.e. of the 53 participants contacted, 22 responded to and participated in the study. Participants' ages ranged from 28 to 70, and were based in Austria, Belgium, Germany, the Netherlands, Poland, Sweden, Switzerland, and the United Kingdom. Participants came from the academic, policy-making, non-profit, and industrial sectors respectively. The final sample of 22 participants were recruited from the United Nations Institute for Disarmament Research (UNIDIR), the International Panel on the Regulation of Autonomous Weapons (iPRAW), the German Council on Foreign Relations, the German

Federal Foreign Office, the German Army (Bundeswehr), the Belgian Royal Military Academy, the University of Namur, the University of Siegen, the Free University of Brussels (VUB), Central European University, ETH Zurich, the Hague Center for Security Studies, Djapo, McKinsey and Company, Compagnie Européenne d'Intelligence Stratégique Sprl (CEIS), the Center for Data Innovation, The Democratic Society, Statewatch, Transparency International, the Stockholm International Peace Research Institute, the European Commission, and the European Parliament. One individual from the European Commission consented to digital interviews on the basis that their interview would not be audio-recorded. Note-taking was allowed in the instances where participants did not consent to being audio-recorded.

2.2 Procedure

Participants were contacted online via cold emails, word-of-mouth, and snowball sampling. Given the onset of the lockdown measures in response to the COVID-19 pandemic, they were interviewed by the author via Skype. The author conducted all interviews in a private room within her home. Participants were either located in a quiet room (alone) within their respective office, or at home. All interviews were conducted in English.

Participants who agreed to take part in the study in response to the emails by the author were sent informed consent forms where they could agree to participate in an exploratory study looking at "The Economics and Sociopolitical Implications of the Development of Artificial Intelligence for European Security and Defence". All but three participants agreed to be audio-recorded during the interview.

The Skype interview began with a brief introduction discussion that was not audio-recorded, where the interviewer explained her background, thanked the participant for being a part of the study, went over the study protocols, and discussed any informal/thematic topics of interest. This was followed by the formal interview, which began with the interviewer requesting consent to begin audio-recording the conversation.

2.1 Materials and Design

The semi-structured interview consisted of 13 pre-determined questions in total, asked in chronological order to reduce experimenter bias. The semi-structured interview allowed for follow-up questions between these 13 questions based on participant responses. The interviews on average lasted one hour.

Given the fragmented development of AI and ML-driven technologies for European security and defence across regions and countries, the breadth of AI as a tool and discipline, as well as the diverse backgrounds of those being contacted and interviewed (from academia, industry, policy, and the non-profit sectors), the questions were wide-ranging and framed in general terms. This was especially important given the technical nature and perception of AI; although everyone who was contacted to participate in the study had published on or worked with AI for European security and defence in some specific capacity, a few of the participants who declined to participate in the study cited the technicality of the subject and their lack of expertise in response to the author's emails requesting their participation in the project. To this end, the wide-ranging and more general framing of the questions was emphasised when reaching out to potential participants. Participants were encouraged to respond to each question based on their own technical expertise and experience. Individuals could skip any question at any time.

The questions comprised mapping the development of AI- and ML-driven technologies for European security and defense in terms of geography and strategic policy/industrial priorities, challenges to policy-makers, cooperation between different actors, and building resilience/mitigating the risks of AI- and ML-driven technologies. Attempts were made to include a discussion of the use of AI in Unmanned Aerial Vehicles (UAVs) and Lethal Autonomous Weapons (LAWS), two key AI-related policy issues emphasised in the literature review.

Participants were informed that the terms “security” and “defence” were meant to be interpreted broadly and include both military and civilian domains. Security therefore included both AI-driven attacks and resilience-building on the battleground, in cyberspace, and civilian life. Therefore, disinformation attacks targeting both civilians and the military as well as cyberattacks and surveillance threats on military personnel, public institutions, and the citizenry were open for discussion.

Eight participants requested the list of questions prior to the Skype call. One participant included in the sample preferred to respond to the questions in writing, and no Skype call was conducted. Participants did not receive any incentives for participating in the study, and were orally debriefed at the end of the interview.

3.0 RESULTS

3.1 Analytic Framework

A content analysis of all 22 interviews was carried out by the author to identify the frequency of themes and overall recommendations (Braun & Clark, 2006). The thematic analysis was based on the prevalence of topics mentioned in the literature (deductive approach) and any new challenges identified and recommendations made (inductive approach). This thematic analysis resulted in ten insights for policy-makers. Only those recommendations that were mentioned by at least 50% of participants are presented. Overall content analysis results are presented below.

3.2 Overall Findings

All participants discussed the importance of regulating the use of data for privacy protection within the EU. Two participants discussed the role of the General Data Protection Regulation (GDPR) in enforcing this privacy (see Chase, 2019). Interestingly, only three participants identified Berlin as a hub for AI development in Europe. Nineteen participants (86% of the sample) mentioned that it was difficult to identify a “hub” for AI development in Europe per se, stating that AI development is quite diffused across member states. Germany, France, the UK, Sweden, and the Netherlands were mentioned as areas of AI development, with references to London (91%), Berlin (68% of the sample), Amsterdam (50%), and Paris (27%) made. In contrast, all participants mentioned the United States and China as hubs for AI development, with two participants mentioning Israel, one participant discussing India, and two participants noting the role of Russia and South Korea respectively. All participants mentioned the dual-use nature of AI-driven technologies, with their use in offensive and defensive campaigns, and in civilian and military domains. All participants mentioned the increased risk in implementing AI-driven solutions developed outside the EU within member states.

All participants were readily able to recall industrial actors working on AI development within European NATO states, including Airbus and Palantir. Only four participants mentioned the role of the European Commission, NATO, and the European Defence Fund by name. All participants emphasised the transnational or international nature of the European defence industry, making references to collaborative projects in the development of AI-driven solutions. Fifty percent of the sample (11 participants) were able to recall the name of an organisation working on responsible AI. Independent references to Statewatch, Transparency International, Algorithm Watch, and the United Nations were made. In response to the role of AI in increased surveillance, 13 participants called on the United Nations or NGOs such as those mentioned above to work with policy-makers to regulate their use. The importance of data protection to combat surveillance was mentioned by all 22 participants.

Nineteen participants emphasised the role of AI in polarising societies via disinformation. Only one was able to recall an organisation working to effectively counter this disinformation. Six participants mentioned the danger of social media platforms such as Facebook in data mining efforts. Ten participants noted the incidence of data mining by the private sector (without explicit references to companies). Four participants noted that sharing one's data was the default of the future, and that an innovative solution would be a centralised space for every citizen to share what types of data they wish to share with, and restrict from, the private sector and public sector respectively. Two participants noted, "There should be an app for that! [To easily grant or restrict access to private data]."

All participants agreed that AI- and ML-driven technologies will contribute to the increase of military budgets and the escalation of arms races. Interestingly, they also noted that this was inevitable. All participants agreed that future wars will not be concluded via the destruction of automated weapons on the field (however developed), but by the death of people, whether civilian or military. They underlined the assistive capacities of AI on the battleground, especially with regard to reconnaissance and carrying out surgical strikes.

Two participants acknowledged the importance of collaboration between the private sector and the military in harnessing AI innovation for defence. Seven participants discussed the role of NATO in already facilitating discussions between the private sector and the military to build AI-driven resilience in Europe.

All participants noted the importance of collaboration across EU member states in developing and regulating AI-driven solutions. All participants were aware of the risk of coding human biases into ML-driven algorithms, and 50% were able to recall examples of such occurrences. Five participants recalled the now famous case of facial recognition technology implemented at the Berlin-Südkreuz train station resulting in a 20% error rate, mostly misidentifying people of colour at the station. A poignant case of biased data training sets resulting in erroneous outcomes, this was the most cited example used by participants acknowledging the algorithmic bias. Two participants identified women as those at risk of this type of bias, whereas 50% of the sample (11 interviewees) noted that people of colour were most at risk of this type of error. Seventeen participants (77% of the sample) mentioned that white males were explicitly not at risk from algorithmic bias. All participants noted the importance of collaboration across EU member states in developing and regulating AI-driven solutions.

4.0 INSIGHTS FOR SECURITY PROFESSIONALS AND POLICY-MAKERS

Recommendations mentioned by at least 50% of participants are presented in this section (i.e. at least eleven participants independently mentioned the policy insights described below during the course of their interviews).

4.1. Adapting the Operationalisation and Regulation of AI- and ML-Driven Technologies to Existing International Human Law (IHL) Frameworks

The principles of distinction and proportionality within existing international humanitarian law were signalled by participants as sufficient and applicable across the implementation of AI-driven solutions in warfare. More than 50% of participants argued that the existing IHL frameworks of proportionality and distinction can be used to govern the use and misuse of AI, as they emphasised the assistive role of AI for military targeting and action versus independent/autonomous action. The framework of distinction was mentioned with regard to providing the best protection possible to civilians in conflict zones, via the analysis of big data to target surgical strikes and avoid civilian casualties in conflict zones.

4.2. Moving Beyond "Meaningful Human Control"

In-depth discussions of what constitutes meaningful human control engaging multi-stakeholder perspectives highlighted the need to develop a human-centred regulatory policy. According to one participant, "We need to build on a meaningful discussion of human control instead of polarising the debate between the acceptance or banning of automated systems. The reality is we need to identify where the benefits of automated systems lie, and how harm can be reduced." The principle of retaining meaningful human control within automated systems has been made clear by the Group of Governmental Experts (GGE) on LAWS, the International Committee of the Red Cross (ICRC), UNIDIR, and a number of actors in the field. More than 50% of participants in this study recommend that the concept meaningful human control is unpacked *along with military, private, and public sector engagement*, with the realistic costs and benefits of these AI solutions in mind. Importantly, 46% of participants called for a focus on discussing how meaningful human control can be included in existing automated systems, from development to testing to implementation, for example in evaluation and target nomination, versus a debate on the use versus ban of automated systems altogether.

4.3. Critical Thinking Skills Versus Digital Literacy

More than 50% of participants responded to the question of "What does resilience actually look like?" with the need to build more critical thinking skills across the population. These participants emphasised the need to build critical thinking skills to understand what constitutes disinformation versus building digital literacy more specifically. They mentioned that in many European NATO member states, critical thinking had been built into school curriculums, which has helped them parse through online and offline disinformation during their lifetimes. Instead of solely investing in AI skill-building which can result in participant self-selection and gender bias, these participants call for an increased divestment into building critical thinking skills among children and populations vulnerable to AI-driven misinformation.

4.4. Increasing AI-Driven Solutions for Military Use

All participants acknowledged that AI is here to stay, and that greater investment and innovation in AI within Europe is required to retain strategic defensive autonomy. More than 50% of participants called for clear distinctions to be drawn between military and civilian uses of AI-driven technologies in terms of data protections, surveillance, etc. While acknowledging that these types of distinctions would be difficult to navigate, they called for greater investment in the military uses of AI, from border protection to biometric data processing. This military use of AI did not cover combating disinformation campaigns, which these participants highlighted more as a political issue. Interestingly, the German Army officer interviewed during this project noted the importance of training soldiers in automation and algorithmic bias, and the role of disinformation campaigns in influencing troop morale.

4.5. Increasing the Technical Awareness of the Development and Capacities of AI- and ML-Driven Within Policy Solutions

All 22 interviewees noted that most policy-makers currently building AI-related legislation lack the technical knowledge to do so. The decisions of policy-makers across European NATO countries should be more informed by expert groups, ideally working in tandem with AI innovators in the private and military sectors. Some participants noted the presence of bodies such as iPRAW which are working within this space. However, all noted that more technical capacity development is required in policy circles. In addition, more collaboration between existing AI-focused bodies and policy-makers was iterated.

4.6. What Does Retaining Human Responsibility for AI-Driven Attacks Look Like?

Increased human accountability in the perpetration of AI-driven attacks may mediate the incidence of these types of offensive attacks. Fifty-five percent of participants noted that the increased anonymity afforded by AI-driven attacks (from cyberattacks to disinformation) can increase the incidence and size of these attacks. Within the military domain, participants called for the operationalisation of IHL among other laws to develop concrete frameworks to increase human responsibility for potential attacks via UAVs and other automated systems.

4.7. Legally Binding Instruments to Regulate the Use of AI in International and EU Versus National Contexts

Ninety-one percent of the sample mentioned the collaborative development of AI-driven technologies across European and international lines. This leads to the question of what legally binding instruments to regulate the use of AI would look like in the EU versus in EU-China relations versus EU-US relations. Participants called for bilateral “rules of the road” to be established along these legally binding frameworks that would govern the development of AI technologies between EU and non-EU states in the future. These frameworks should take into account political, social, and economic concerns while respecting IHL, data protection, and human rights at all times in negotiating the regulation of AI development and application across national and international lines.

4.8. Developing AI Competencies and Regulations Within the European Startup Ecosystem

More than half of the participants of this study mentioned the role of startups in Europe in developing AI-driven solutions for European security and defence. While technological giants such as Airbus and SWP were noted, participants called for regulations to develop and limit the competencies of AI startup industries in order to reduce an “arms race to the bottom”. Seventeen participants noted the importance of startup industries in driving European innovation forward, although twelve of these participants noted that these startups have a long way to go to rival the tech and defence giants such as Google and Airbus.

4.9. Understanding the Risks of Not Using AI

The risks of an AI-enabled arms race are not only imminent, but ongoing. Participants emphasised the need for European NATO member states to develop more localised solutions for defensive structures to AI-driven attacks. One participant noted, “The best defence is a good offence, right?” Refusing to invest in the development of AI would result in undermining European economic competitiveness and strategic political autonomy. European nations would be forced to apply AI solutions developed by non-European actors deep within their defence and security architecture. This could expose European NATO nations to further risks, given potential backdoors and network discrepancies in technology developed by non-European actors who may not see themselves bound to the rules of data integrity, privacy, human rights, or even economic market forces that are inherent within a majority of European processes. European NATO states need to innovate and develop AI-driven solutions, to be able to set the rules for how the game is to be played in the future.

4.10. Developing the Responsible Democratisation of Data

The open-source culture of most AI research and development within the scientific community has brought the concept of data democratisation to the forefront. Data democratisation refers to allowing free access to data that allows even non-technical personnel to understand it. The data can be used to expedite and inform decision making, understand economic, social, and political trends, and find opportunities for innovation in the workplace etc. Data democratisation calls for the removal of bottlenecks to accessing data, and is disproportionately advocated for by the non-profit actors among the people sampled. It is however at odds with European culturally grounded technical data privacy priorities. Data democratisation has pertinent ramifications on identifying the needs of vulnerable populations across regions. Done responsibly, it would protect privacy while making relevant data accessible to all.

5. Concluding remarks

This study illustrates the extent to which AI-driven solutions have become inextricable components of the European defence industry over the past few decades. None of the participants interviewed advocated for a ban on AI. They all acknowledged in one way or another that AI is here to stay, and made recommendations for its regulation and innovation to protect and build resilience against future threats (see also: Geist, 2016). None explicitly subscribed to the notion that increased investment in AI-related technologies to build resilience will only result in the development of more sophisticated future threats. All interviewees identified various vulnerabilities that could be exploited by malignant groups, especially in the case of AI solutions developed outside of Europe, emphasising the need for more EU investment and innovation. All participants noted the need for more robust regulation and were aware of the shortfalls of AI, e.g. algorithmic bias, in advocating for more assistive versus fully automated AI-driven solutions.

Three participants mentioned the security challenges of 5G technologies developed by non-NATO actors on European security and defence. Future research should include a discussion of the policy challenges of, and recommendations for resilience-building against, 5G technology networks built by non-NATO states and implemented across Europe more generally. These challenges and recommendations should be made as a function of national and regional policy and industrial priorities and bottlenecks.

As illustrated by this project, the hubs for developing AI- and ML-driven technologies tend to be located across Western Europe, with participants mentioning London, Berlin, Amsterdam, and Paris as potential centres for innovation. However, NATO carries out defence at its borders, and AI-driven threats such as disinformation attacks are often localised to fit contexts when disseminated in southern and eastern NATO countries, such as Italy and the Baltics (La Cour, 2019; Thomas, 2020). The location of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, is a step in the right direction of including more European perspectives in building resilience to AI-driven threats. Future research should investigate the involvement of experts, and training of personnel, from NATO's southern and eastern borders in developing more localised solutions to AI-driven security threats. Future research should investigate the involvement of experts, and training of personnel, from NATO's southern and eastern borders in developing more localised solutions to AI-driven security threats.

This project is a step in the direction of understanding the interwoven political, social, economic, legal, and technical implications of leveraging the development of AI- and ML-driven technologies to build resilience for NATO security and defence. Building resilience to AI is a phrase often used within policy circles. Yet, much needs to be done to understand what actually constitutes building resilience. This project highlighted ten policy recommendations in building resilience, namely 1) developing the existing frameworks of distinction and proportionality within International Humanitarian Law (IHL), 2) operationalising "meaningful human control" on the basis of the costs and benefits of the assistive use of automated systems, 3) the need to build critical thinking skills to build resilience to disinformation attacks, 4) the need for greater investment in AI within the military and delineation of AI for military and civilian use, 5) the need for technical capacity development among AI policy-makers, 6) increasing human accountability for AI-driven attacks to mitigate the incidence of these offensives, 7) the need to negotiate legally binding bilateral instruments along national and international spaces to regulate the uses of AI keeping European social, legal, political, economic, and technical concerns in mind, 8) regulating the development of AI within the startup ecosystem, 9) understanding the risks of not using or developing AI within European NATO countries and finally, 10) developing the responsible democratisation of data. These AI expert insights should be at the heart of building trust in a human-centred NATO Strategy on AI across Europe and beyond.

3.0 REFERENCES

[1] Bahnsen, A. C., Torroledo, I., Camacho, L. D., & Villegas, S. (2018, May). DeepPhish: Simulating Malicious AI. In *2018 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-8).

[2] Bavel, J.J.V., Baicker, K., Boggio, P.S. *et al.* Using social and behavioural science to support COVID-19 pandemic response. *Nature Human Behavior* 4, 460–471 (2020). https://doi.org/10.1038/s41562-020-0884-z

[3] Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. *The Cambridge handbook*

of artificial intelligence, *1*, 316-334.

[4] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.

[5] Brkan, M. (2019). Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting. *Delphi*, *2*, 66.

[6] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeithoff, T., Filar, B., Anderson, H. Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Heigeartaigh, S., Beard, S., Belfield, H. Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

[7] Chui, M. (2017). Artificial intelligence the next digital frontier?. *McKinsey and Company Global Institute*, *47*, 3-6.

[8] Dam, P. (2020). *Hungary's Authoritarian Takeover Puts European Union at Risk: COVID-19 Is Not an Opportunity to Shelve Democracy*. Human Rights Watch Dispatches.

[9] Das, S., Dey, A., Pal, A., & Roy, N. (2015). Applications of artificial intelligence in machine learning: review and prospect. *International Journal of Computer Applications*, *115*(9).

[10] De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). *Artificial Intelligence and the Future of Defense: Strategic Implications for Small-and Medium-Sized Force Providers*. The Hague Centre for Strategic Studies.

[11] Geist, E. M. (2016). It's already too late to stop the AI arms race—We must manage it instead. *Bulletin of the Atomic Scientists*, *72*(5), 318-321.

[12] Johnson, B. D. (2017). The Weaponization of AI: A Glimpse into Future Threats. *Computer*, (10), 73-73.

[13] Johnson, J. (2019). Artificial intelligence & future warfare: Implications for international security. *Defense & Security Analysis*, *35*(2), 147-169.

[14] Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, *349*(6245), 255-260.

[15] La Cour, C. (2019). Governments Countering Disinformation: The Case of Italy. Retrieved August 24, 2020, from https://disinfoportal.org/governments-countering-disinformation-the-case-of-italy/

[16] Migration Data Portal. (2020). *Migration data relevant for the COVID-19 pandemic.*

[17] Oliver, N., Letouzé, E., Sterly, H., Delataille, S., De Nadai, M., Lepri, B., Lambiotte, R., Benjamins, R., Cattuto, C., Colizza, V., de Cordes, N., Fraiberger, S. P., Koebe, T., Lehmann, S., Murillo, J., Pentland, A., Pham, P. N., Pivetta, F., Salah, A. A., Saramaki, J., Scarpino, S. V., Tizzoni, M., Verhulst, S., & Vinck, P. (2020). Mobile phone data and COVID-19: Missing an opportunity?. *arXiv preprint arXiv:2003.12347*.

[18] Raskar, R., Schunemann, I., Barbar, R., Vilcans, K., Gray, J., Vepakomma, P., Kapa, S., Nuzzo, A., Gupta, R., Berke, A., Greenwood, D., Keegan, C., Kanaparti, S., Beaudry, R., Stansbury, D., Arcila, B.

B., Kanaparti, R., Pamplona, V., Benedetti, F. M., Clough, A., Das, R., Jain, K., Louisy, K., Nadeau, G., Pamplona, V., Penrod, S., Rajaee, Y., Singh, A., Storm, G., & Werner, J. (2020). Apps gone rogue: Maintaining personal privacy in an epidemic. *arXiv preprint arXiv:2003.08567*.

[19] Thomas, M. (2020). Defeating Disinformation Threats. Retrieved August 24, 2020, from https://www.fpri.org/article/2020/02/defeating-disinformation-threats/

[20] Timmers, P. (2020). There will be no global 6G unless we resolve sovereignty concerns in 5G governance. *Nature Electronics*, *3*(1), 10-12.

[21] Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. *Political polarization, and political disinformation: a review of the scientific literature (March 19, 2018)*.

[22] Zwitter, A., & Gstrein, O. J. (2020). Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action* 5 (2020). https://doi.org/10.1186/s41018-020-00072-6