Women In International Security

POLICYbrief

WIIS POLICYbrief May 19, 2020

WEB | www.wiisglobal.org

EMAIL | info@wiisglobal.org

1301 Connecticut Avenue NW, Suite 750
Washington, D.C. 20036

Artificial Intelligence Is Already Transforming the Alliance.

It's Time for NATO and the EU to Catch Up.

Kulani Abendroth-Dias and Carolin Kiefer

If World War III will be over in seconds, as one side takes control of the other's systems, we'd better have the smarter, faster, more resilient network.[1]

For delivery within the European Union, Amazon now sells facial recognition cameras for door locks, webcams, home security systems, and office attendance driven by artificial intelligence (AI) and machine learning (ML)—powerful tools with civilian and military purposes.[2] Germany, France, Spain, Denmark and Romania have tested and often deployed AI and ML facial recognition tools, many of which were developed in the United States and China, for predictive policing and border control.[3] AI and ML systems aid in contact tracing and knowledge sharing to contain the COVID-19 virus.[4] However, the civilian and military strategies that drive use of AI and ML for the collection and use of data diverge across the member states of the European Union and the North Atlantic Treaty Organization (NATO).[5]

Growth in the development of AI-driven technologies has been exponential, but strategies to regulate their implementation have yet to catch up. The European Union and NATO need to develop coordinated, comprehensive, and forward-looking strategies based on data protection protocols to regulate AI use and deployment to counter myriad threats. Such strategies will be critically important if the transatlantic alliance is to adapt a common defense system to evolving threats in the digital age.

Data, the food of all algorithms, lie at the core of cohesive EU and NATO AI strategies. Such strategies must encompass the regulation of data in high- and low-risk technologies with dual uses. They should guide policies governing predictive policing, border surveillance, facial analysis and recognition and countering disinformation.[6]

To regulate data use effectively, policymakers need to better understand the technical, political, economic and social risks and biases in data collection methods. Without a greater understanding of how data feed AI and ML technologies and systems, the results they produce become skewed. For example, a facial analysis and recognition system insufficiently trained to analyze and recognize women or people of color will often misidentify people in these populations, which could lead to inaccurate criminal profiling and arrests.[7] Machines don't make errors, but humans do. Policymakers need to rapidly identify parameters and systems of governance for these technologies that maximize their efficiency while protecting civilian rights.

Beyond Definitions

AI and ML are changing the security landscape—for example, by the deployment of disinformation to undermine political participation or of unmanned autonomous vehicles (UAVs), which may or may not operate as lethal autonomous weapons systems (LAWS). The states that are party to the Group of Governmental Experts (GGE) on Lethal Autonomous Weapons

(LAWS), which aligns its work with the Convention on Certain Conventional Weapons (CCW), have devoted considerable attention to defining autonomous weapons. Unfortunately, the group has not yet paid enough attention to the data. Prolonged focus on what constitutes LAWS rather than the data that drive them impedes the important investigation of how best to regulate the technologies' rapid development and use for security and defense. Discussion of the types, limits, and biases of data that drive AI and ML is pertinent throughout the myriad sectors in which they find application.[8]

Recently, the GGE took steps to move the debate from definitions of autonomous systems to why data matter. In 2020, it decided that the 11 guiding principles that frame the development and use of LAWS needed no further expansion.[9] The group agreed to give greater attention to how the principles can be unpacked. It decided to distinguish between high- and low-risk AI technologies and gain a better understanding of dual-use technologies.[10] Differentiating between uses for civilian and military operations should focus on how data will be mined and drive algorithms at both levels.[11] NATO and the European Union should lead in facilitating these discussions and regulations.

Data Governance

According to the European Commission's February 2020 white paper on artificial intelligence, "Europe's current and future sustainable economic growth and societal well-being increasingly draws on value created by data.... AI is one of the most important applications of the data economy."[12] However, the report concludes, for AI to "work for people and be a force for good in society" it must be trustworthy.[13] It highlights "trustworthy AI" 27 times in its 26 pages.

Governance of data is key to this trust.[14] The EU General Data Protection Regulation (GDPR) was a step in the right direction, but it needs to be expanded to cover AI and ML data collection and use in national and international security contexts. Close consultation and data coordination between the European Union and NATO is integral in this regard.

An understanding of who drives the development of AI-driven technologies for European security and how they are funded can illuminate the political, technical, and social, and legal bottlenecks confronting EU and NATO data regulation, both in the member states and at a supranational level. While the defense sector has traditionally driven technology innovation, private companies have taken the lead in recent years. [15] According to the OECD, Google, Microsoft, Amazon, and Intel have spent more than $50 billion a year on digital innovation.[16] This sum dwarfs the €13 billion budgeted by the European Defense Fund (EDF) for 2021–27 - for defense spending in general, not solely for AI-driven technologies.[17] NATO and the European Union should pay particular attention to these private-sector actors when developing policies for data protection and strategies to encourage US and European technological innovation. NATO and the European Union should work with the CCW GGE to determine clear operational distinctions between the commercial and military uses of data for AI-driven technologies.[18] NATO and the European Union need comprehensive, legally enforceable AI strategies to regulate the use of data and the integrity of information networks to better protect their citizens while keeping the Alliance agile.

The Way Forward

In EU and NATO contexts, the development and implementation of dual-use technologies and cyber-protection policies remain fragmented. This fragmentation could undermine the ability to respond to evolving threats to European security and stability. Examples abound: Cambridge Analytica's involvement in Britain's Leave Campaign, radicalization via social media, the politicized use of data via hybrid-use platforms to influence behavior (from political participation to violent action), and targeted cyber-attacks and disinformation campaigns in the Visegrad Four and the Baltic states.[19] Therefore, coherent EU and NATO AI strategies require the regulation of the data that drive emerging technologies. Regulation to promote network integrity and protect data access must be key tenets of EU and NATO strategies to deploy AI that can react faster and more effectively in the face of new security threats.

AI and ML systems are valuable, as demonstrated by their use in contact tracing and knowledge sharing in the search for a cure during the Covid-19 pandemic.[20] For the transatlantic relationship to thrive, NATO and the EU must work together to develop coordinated AI strategies that address appropriate use and misuse of data. As the EU and NATO develop these strategies, they should focus on five activities:

Govern the use of data in dual-use technologies.

While AI strategies may sound exciting and innovative to policymakers and the general public, responsible data use sounds less so. Yet it is essential. EU and NATO strategies need to distinguish between high- and low-risk technologies, dual- and hybrid-use platforms, and the types, limits, and mediums by which data can be collected and anonymized (or at least kept confidential) for civil and military uses. These limits need to be developed and regulated in discussions with civilian and military actors who are mining data across sectors, from the traditional security and military arena to healthcare, logistics, and entertainment companies. Discussions should include how the rights of citizens and those residing in NATO and EU countries—e.g., lawful migrants, asylum seekers, refugees—will be protected.

Acknowledge bias in datasets.

There should be a comprehensive discussion on how bias in datasets influences the training of algorithms, which in turn influences security targets and undermines the integrity of a system. Policymakers, human rights actors, and technology developers should be in the room for this discussion. An awareness of these biases within security forces can help them better evaluate the outcomes the algorithms produce, interpret targets with caution, avoid errors, and generate more effective responses.

Ensure purpose-limited data collection and sharing.

Personal data collected and tracked for specific purposes (e.g., contact tracing during a pandemic) should generally not be shared and used for other purposes. Where an overlap in data collection is deemed necessary for EU-NATO security purposes, tight regulations for civilian protection should spell out where, with whom, and for how long the data can be stored, with strong legal and operational deterrents for backdoor access to data. Private-sector companies should limit how data are used to influence behavior: Should they be used in political campaigns the same way that they are used to nudge consumer behaviors on what to buy? The European Union's GDPR sets up important rules in this regard. It can be viewed as the cornerstone of an EU-NATO strategy for the development and regulation of AI for security and defense.

Adapt traditional defense and deterrence strategies to the digital age.

The evolving nature of security threats in the digital age calls into question traditional strategies of defense and deterrence. Collaboration between NATO, the European Commission, the European Defence Agency (EDA), the Permanent Structured Cooperation (PESCO), the Coordinated Annual Review on Defense (CARD) and technology developers should focus on efficiency—trimming current weapons systems and technologies used by the European Union on the battlefield and in the cyber realm while using AI and ML to inform strategy. The weaponized use of social media data must be addressed, not solely via counternarratives but by working in concert with social media companies to develop AI and ML techniques to identify and shut down fake news at the source. The integrity of networks set up by actors outside of NATO member states needs to be raised as a security concern as well, including incentives to drive the local business development of such networks.

Build trust via counter-AI agencies to protect citizen rights and detect AI-driven forgeries.

Agencies that currently promote the responsible use of AI need to work in tandem with NATO and EU agencies to develop comprehensive AI strategies. The strategies should promote digital literacy, advance critical thinking through online modules, and publicize the precautions NATO and the European Union are taking to protect citizen data in order to build public trust. Partnerships between EU, NATO, and such agencies need to go beyond traditional NGO–security agency relationships to integrate AI protection mechanisms into security policy itself. Ideally, these organizations would work with NATO partner countries to better identify targets, weaknesses, and priorities to build resilient intelligence architectures.

Map the development and use of AI-driven technologies across EU and NATO member states.

NATO security operations are in place at member state borders. However, most of the AI technologies being developed, test, or adapted are deployed within France and Germany, key EU member states. AI-driven security threats differ across states, especially disinformation. For example, the content, medium, and speaker of disinformation shared in the Czech Republic may differ considerably from disinformation shared in Germany. Adapting traditional deterrence strategies to the digital age requires an understanding of the context-based nature of these threats. It is therefore integral to include experts across the EU and NATO member states in the development and implementation of AI strategies. A comprehensive mapping of the security threats faced—and development and use of AI-driven technologies to combat such threats across EU and NATO member states—can help better train personnel and develop more targeted solutions and localized data protection policies.

Conclusion

The digital industry is already transforming the Alliance. NATO is essential to setting up a coordinated structure to develop and regulate AI- and ML-driven technologies for NATO members' security and defense. While sociopolitical and economic priorities in the development and regulation of AI vary across sectors and countries, awareness of the use and misuse of data in driving AI-and ML-driven technologies is a common thread that binds these debates together. The use of data fed into a system run by AI and ML technology can have vast implications for the nature of future security threats and the development of technologies to combat them. Cohesive EU and NATO strategies for AI will determine how strong and agile the Alliance will become.

References

1. Pedro Domingos, *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World* (New York: Basic Books, 2015).

2. See Daniel S. Hoadley and Nathan J. Lucas, *Artificial Intelligence and National Security* (Washington DC.: Congressional Research Service, 2018); Greg Allen and Taniel Chan, *Artificial Intelligence and National Security* (Cambridge, MA: Belfer Center for Science and International Affairs, 2017). Artificial intelligence comprises a vast number of fields, including machine learning, natural language processing, robotics, computer vision, and knowledge representation and reasoning. In this policy brief, the authors largely refer to the use of AI- and ML- driven technologies for EU and NATO security and defense.

3. Steven Feldstein, *The Global Expansion of AI Surveillance* (Washington, DC: Carnegie Endowment, September 2019).

4. The Cybersecurity Strategy of the Visegrad Group Countries *Coronavirus,* Artificial Intelligence web page (April 12, 2020).

5. Raluca Csernatoni, *An Ambitious Agenda or Big Words? Developing a European Approach to AI,* Egmont Security Policy Brief No. 117 (Brussels: Egmont Royal Institute for International Relations, November 2019).

6. Michael Chui et al., *Notes from the AI Frontier: Insights from Hundreds of Use Cases* (New York: McKinsey Global Institute, 2018).

7. Philipp Grüll, "Germany's Plans for Automatic Facial Recognition Meet Fierce Criticism," *EURACTIV* (January 10, 2020).

8. Ajay Agrawal, Joshua Gans and Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence* (Cambridge, MA: Harvard Business Press, 2018).

9. See the UN's 1980 Convention on Certain Conventional Weapons.

10. German Federal Foreign Office, *Chair's Summary: Berlin Forum for Supporting the 2020 Group of Governmental Experts on Lethal Autonomous Weapons Systems* (Berlin: German Federal Foreign Office, April 2020).

11. United Nations Institute for Disarmament Research, *The Human Element in Decisions About the Use of Force* (Geneva: UNIDIR, March 2020).

12. European Commission, *On Artificial Intelligence: A European Approach to Excellence and Trust*, white paper, COM (2020) 65 final (Brussels: European Commission, February 19, 2020), p. 1. See also European Commission, *A European Strategy for Data*, COM (2020) 66 final (Brussels: European Commission, February 19, 2020).

13. EC, *On Artificial Intelligence*, p. 25.

14. Ibid.

15. Dieter Ernst, *Competing in Artificial Intelligence Chips: China's Challenge amid Technology War*, Special Report (Center for International Governance Innovation, March 26, 2020).

16. Organization for Economic Cooperation and Development, *Private Equity Investment in Artificial Intelligence* (Paris: OECD, December 2018).

17. European Commission, *European Defence Fund* (Brussels: European Commission: March 20, 2019). Arguably, Washington would do well not to view the EDF with suspicion and skepticism but rather as a vehicle to stimulate more transatlantic discussion on "home-grown" innovation and development.

18. Daniele Amoroso et al., "Autonomy in Weapon Systems: The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy," *Democracy* Vol. 49 (Heinrich Böll Foundation, 2018).

19. Marek Górka, "The Cybersecurity Strategy of the Visegrad Group Countries," *Politics in Central Europe* Vol .14, No. 2 (2018), pp. 75–98. See also Alistair Knott, "Uses and Abuses of AI in Election Campaigns," presentation, N.d.

20. Council of Europe, *AI and Control of Covid-19.*

Authors

Kulani Abendroth-Dias is Masters candidate at the Institute for European Studies, Vrije Universiteit Brussels (VUB) in Brussels, Belgium.

Captain Carolin Kiefer serves as an officer in the German Armed Forces and is currently posted as Technical Officer in the Support Battalion of EUROCORPS, Strasbourg. Her contribution to this brief is in a private capacity.

This publication is the result of a joint WIIS DC, WIIS Brussels, WIIS France, and WIIS UK project focused on new challenges for the NATO alliance and showcasing the expertise of the Next Generation women defense experts. Through a competitive selection process six Next Generation experts were invited to participate in programs on the sidelines of the 2019 December NATO Leaders meeting. We would like to thank our six experts for their thoughtful contributions to this initiative, WIIS Global for publishing their research and the US Mission to NATO for providing the generous grant without which this project would not have been possible. With this support, we were able to turn an idea to promote greater cooperation among our affiliates and cities into a reality. We hope this project encourages more collaboration across borders and helps bolster the overall WIIS mission of supporting women in the international security field.

The NATO Consortium Team: Michelle Shevin-Coetzee, WIIS-DC; Armida van Rij, WIIS UK; Florence Fernando and Pauline Massart, WIIS Brussels; Ottavia Ampuero and Jessica Pennetier, WIIS France.

WIIS DC
WOMEN IN INTERNATIONAL SECURITY

wiis WOMEN IN INTERNATIONAL SECURITY BRUSSELS

WIIS
Women In International Security France

WIIS Women in International Security United Kingdom

RECENT WIIS PUBLICATIONS

POLICYbrief

Chantal de Jonge Oudraat and Michael E. Brown, *The Gender and Security Agenda: Strategies for the 21st Century* (London: Routledge, June 2020)

Nad'a Kovalčíková and Gabrielle Tarini, *Stronger Together: NATO's Evolving Approach toward China,* WIIS Policy Brief (May 2020)

Shannon Zimmerman, *The Value of a Feminist Foreign Policy*, WIIS Policy Brief (February 2020)

Sarah Kenny, *Women of the Alt-Right: An Intersectional Study of Far-Right Extremism, Gender, & Identity in the United States*, WIIS Policy Brief (August 2019)

Pearl Karuhanga Atuhaire & Grace Ndirangu, *Removing Obstacles to Women's Participation at the Peace Table and in Politics*, WIIS Policy Brief (March 2019)

Chantal de Jonge Oudraat & Soraya Kamali-Nafar, *The WIIS Gender Scorecard: Washington, DC Think Tanks*, WIIS Policy Brief (September 2018)

Pearl Karuhanga Atuhaire & Grace Ndirangu, *Sexual and Gender Based Violence in Refugee Settings in Kenya and Uganda*, WIIS Policy Brief (June 2018)

Luisa Ryan & Shannon Zimmerman, *Gender Parity in Peace Operations: Opportunities for US Engagement*, WIIS Policy Brief (June 2018)

Velomahanina T. Razakamaharavo, Luisa Ryan, & Leah Sherwood, *Improving Gender Training in UN Peacekeeping Operations*, WIIS Policy Brief (May 2018)

Spencer Beall, *Missing Figures: The Cybersecurity Gender Gap*, WIIS Working Paper (May 2018)

Chantal de Jonge Oudraat and Michael E. Brown, *WPS+GPS: Adding Gender to the Peace and Security Equation*, WIIS Policy Brief (November 2017)

Hamoon Khelghat Doost, *Women in Jihadist Organizations: Victims or Terrorists?*, WIIS Policy Brief (May 2017)

Jeannette Gaudry Haynie and Chantal de Jonge Oudraat, *Women, Gender, and Terrorism: Understanding Cultural and Organizational Differences*, WIIS Policy Brief (April 2017)

Ellen Haring, *Equipping and Training Modifications for Combat Arms Women*, WIIS Policy Brief (January 2017)

Fauziya Abdi Ali, *Women Preventing Violent Extremism: Broadening the Binary Lens of "Mothers and Wives,"* WIIS-HoA Policy Brief (February 2017)

Jeannette Gaudry Haynie and Chantal de Jonge Oudraat, *Women, Gender, and Terrorism: Policies and Programming*, WIIS Policy Brief (January 2017)

Jeannette Gaudry Haynie, *Women, Gender, and Terrorism: Gendered Aspects of Radicalization and Recruitment*, WIIS Policy Brief (September 2016)

Antonieta Rico and Ellen Haring, *Combat Integration Handbook: A Leader's Guide to Success* (September 2016)

Chantal de Jonge Oudraat and Michael E. Brown, *Women, Gender, and Terrorism: The Missing Links*, WIIS Policy Brief (August 2016)

Chantal de Jonge Oudraat, Sonja Stojanovic-Gajic, Carolyn Washington and Brooke Stedman, *The 1325 Scorecard: Gender Mainstreaming Indicators for the Implementation of UNSCR 1325 and its Related Resolutions* (Brussels,Washington, DC and Belgrade: NATO-SPS Programme, WIIS and Belgrade Centre for Security Policy, October 2015)

Ellen Haring, Megan MacKenzie and Chantal de Jonge Oudraat, *Women in Combat: Learning from Cultural Support Teams*, WIIS Policy Brief (August 15, 2015)

WIIS Policy Roundtables and Policybriefs are supported by the Embassy of Liechtenstein in Washington, DC.

WIIS Next Generation efforts are supported by Carnegie Corporation of New York.

ABOUT WIIS

Women In International Security (WIIS) is the premier organization in the world dedicated to advancing the leadership and professional development of women in the field of international peace and security. WIIS (pronounced "wise") sponsors leadership training, mentoring, and networking programs as well as substantive events focused on current policy problems. WIIS also supports research projects and policy engagement initiatives on critical international security issues, including the nexus between gender and security.

To learn more about WIIS and become a member, please visit http://wiisglobal.org/.

WIIS
WOMEN IN INTERNATIONAL SECURITY