The Hague Conference on Responsible AI

for Peace, Justice and Security

Conference Report with recommendations

12-13 May 2022,
Peace Palace The Hague

Contents

The Hague Conference on **Responsible AI**

Thank you!

On 12 and 13 May, almost **200 experts** from around the world gathered in the Peace Palace Auditorium in The Hague to discuss responsible, human-centric AI. With a focus on the domains of peace, justice and security the conference gave in-depth insights and led to practical and policy recommendations. Contrary to current practice, this was an exclusively physical conference.

Organizing this conference was a great journey. We chose the path of co-creation. In the early phases of setting up the programme we held partner meetings with a lot of international organizations, within and outside of the Hague. All of these appeared on stage and/or organised subsessions during the conference and in doing so contributed a lot to the success of this conference.

We look back to inspiring discussions, meeting old friends and making new ones. We feel this conference was a good first step in establishing the Netherlands as an international platform for expert discussions on responsible AI.

For all of you who have been there, many thanks for your contribution and we hope to see you next time. And for readers of this report who couldn't attend, let's get in touch!

Michel van Leeuwen,
Director for Artificial Intelligence Policy, Ministry of Justice and Security

Nathalie Jaarsma,
Ambassador for Security Policy and Cyber of the Netherlands, Ministry of Foreign Affairs

Wim Jansen,
Director for International Affairs, Municipality of The Hague

info@thehagueconferenceonresponsibleai.nl

Summary

Artificial Intelligence is one of the most fundamental technologies of our time. Dubbed by some as the electricity of the 21th century, AI will have important benefits for our societies. Europe and the Netherlands are determined to make this a transformation for good. We want to ensure that everybody benefits. To make this happen we have to do so responsibly. Hence, the Hague conference on responsible AI.

The Netherlands believes that the best way to do is, is to exchange knowledge with experts across silos. So paramount to the success of this conference was the diversity of participants. We were happy to see that experts from academia, corporations, ngo's and government attended the conference.

After a warm welcome by the mayor of The Hague, Jan van Zaanen, the conference started off with pitches from NATO, UNICRI and Microsoft. This led to questions that were discussed at roundtables in different rounds. It was inspiring to see everyone immediately diving into the different subjects and a lot of new connections being made.

The Netherlands minister for Digitalisation, Alexandra van Huffelen, gave the opening speech on the second day and stressed the importance of good regulation, to protect people against bad AI. Eric Schmidt (former CEO of Google) of the US Special Competitives Studies Project laid out on video the enormous potential and significance of AI and the challenges ahead, both in geopolitical as in societal respect.

The plenary session continued with a panel discussion with the key stakeholders in the current regulatory landscape. Jan Kleijssen from the Council of Europe, Kilian Gross from the European Commission, Audrey Plonk from the OECD, and Vanja Skoric from the European Center for Non-Profit Law) kickstarted the discussion on the initiatives and challenges in current and upcoming regulation.

Two rounds of interactive sessions followed. In total **17 sessions** on the three main subjects of the conference: AI and regulation, AI and cybersecurity, -norms and diplomacy, AI in the City. In the Annex all sessions are summarized. After sometimes fierce, but always engaging conversations, all sessions led to the above mentioned recommendations.
These recommendations were presented to the panellist at the closing ceremony by Saskia Bruines, vice mayor of the Hague.

During the conference a plethora of principles, tools and reports were mentioned. A lot of these are collected in the online repository for the conference: https://securityinsight.nl/artificial-intelligence-ai-machine-learning

Recommendations

AI and regulation

The regulatory approach in Europe builds upon the development of principles worldwide.
This currently is work in progress. During the conference these recommendations were given:

- We should accept that there is no guarantee that AI decision-making will ever be a 100% infallible.
- There is a need for a more integrated approach on the development of different regulations which affect each other, like the Directives on Due Diligence and the AI Act.
- Protection of human dignity has to be at the center of all development and deployment of technology by authorities.
- AI has no borders, even beyond Europe, do we need a worldwide legal regulation (instead of non-binding principles)?
- The object of regulation, namely AI, is a moving target. We need to reflect together on how we can keep regulation agile enough to keep it effective.
- Technology overtakes governance and legislation. Policy prototyping is a method for assessing new policies e.g. the Draft AI Act.
- Process of standards creation in the AI Act must be more inclusive. It must include for example societal organizations.
- Public authorities must be more involved in the creation of standards.
- When standards are created by standardization organizations, it must be explained how they project fundamental rights. For example with a human rights impact assessment.
- Domain specific frameworks, such as the Policy Framework for responsible limits on facial recognition technology by law enforcement, are crucial to guide users while using AI-tools in a practical way.
- Practical capacity building is needed in more countries.
- Help sme's in developing ethical AI.
  They don't have the means to set up structures and tools for ethical AI as Big tech has.

Recommendations

Implementation

A lot of regulation is already in place, for instance GDPR, principles have been layed out, new legislation is on the horizon. On the question of how to implement this, participants gave the following recommendations:

- There is a need for a good methodology and tools, in combination with the in person dialogue.
- Computer science education has to change, but we don't know what to teach them → Many methodologies and tools available.
- There are best ethical engineering practices (PAIR), but we need make better use of them. How to do this?
- Important to make a clear distinction between social and technical issues at stake.
- Find ways to ensure ex ante (civilian-) stakeholder participation in the design, development, implementation and evaluation regarding AI issues.
- The ELSA Lab approach would fit especially for high-risk applications such as power imbalance, vulnerable groups etc.
- AP4AI contributes to implement the conformity assessment procedures of AI systems for the internal security sector. Conformity assessments are the cornerstone of the risk-based approach to AI systems proposed in the EU AI Act. The Accountability Principles for AI can contribute to the implementation of such conformity assessments.
- AI Accountability implies notions of "citizen empowerment", "answerability" and "risk mitigation" in the enforcement framework. The proposed EU AI Act should reflect these notions.
- From engineering to sales to lawyers. Working on a mindset change (for instance through education, workshops, AI ambassadors) is needed to ensure responsible design and deployment of AI. Commitment of leadership to said mindset change is key.
- Learn from experiences, tools and best practices of big tech companies. Encourage the sharing of best practices.

Recommendations

Cybernorms

- We need to expand the normative framework on cyber and AI beyond the conflict threshold (international humanitarian law).
- Policy-makers need an answer to whether we need particular AI norms on responsible state behavior in cyberspace.
- We need to think of how well the framework can take into account non-human behavior, by a digital autonomous agent that takes decisions that are not necessarily explainable.
- When we talk about particular AI norms, we need to make our interests more explicit. We need to be clear on why we need the human in the loop and on what values we base this.
- Ukraine made clear that political will, context and willingness to stick to values determines how effective these frameworks are.
- We have to be aware of the loss of authenticity in normative frameworks: with AI, it has become very difficult to track the person/state responsible.
- We want to make sure that the state is responsible for its behavior and make that operationable: the problem is not technology or AI, but the state using it to violate the norms we have.
- In regard to the use of AI in autonomous weapons, we need to improve attribution: we fail to say what particular norms were broken.
- Responsibility in AI also in the military domain is to an important extent a design issue. Ethical and legal standards need to be incorporated in the design. Meaningful human control is essential in this process and we need to be very specific about the context in which military AI applications are used.

Recommendations

Diplomacy

- Legally binding rules, such as international humanitarian law, are the basis of creating and using AI responsibly in the military and civil domain, they are the starting point from which governance tools (such as ethical principles) are created.
- When specific enough, these tools can have added value and create responsible behavior amongst actors in the field of AI.
- We need to evolve and process AI while developing legal concepts and continue to try how these technological realities can be incorporated.
- In the context of quantifying mistakes, we are caught in conflict of constraining progress in fear of causing harm. We need to unblock ourselves from setting unreliably high standards. At the same time, we need to consider the playground: what kind of errors are acceptable depending on the field we are in?
- We need to think about explainability, accountability, transparency of AI systems by trying to move into these layers as deeply as possible: we need an actual value, policy goals and incentives to get there. Terms like 'transparency' are just a process layer.
- We need to put things on a spectrum: from high- to low risk: context matters. We need insight and oversight to know what is going on, where we are on the spectrum and to make fact-based decisions.
- We do not always necessarily need to regulate companies, but rather particular markets: getting the values in the systems is more in market regulation, not the layer atop of that.
- Just like policy-makers, companies need to be more explicit about the choices they base their actions on while developing AI-systems
- We have to reconsider what true multistake-holder cooperation means in the AI era.

- We need to reduce the gap between the state-heavy process of international law and places where effective power has already gone. We need political incentives and will to do so.
- If we want to protect our public values, AI in the military domain is needed and we need to have the tools to govern the use and development of such technologies. It's important to consider common security aspects as well as moral values and legal frameworks.

Recommendations

AI and the City

- While recognizing the role of technology as a driver of urban innovation, we must accept their capacity to “de-urbanize” cities.
- It is not feasible simply to top-down implement a new technology in an urban space. There is a long list of failures that comes out of that.
- This means that technology systems that might work in one city might not be desirable in others.
- Therefore involve all local stakeholders in discussions on the application of AI in your city.
- AI is also providing access to groups that are normally difficult to reach (i.e. young people). Big challenge is how to translate this into practical solutions (i.e. being able to reach vulnerable/less literate citizens using AI applications).
- If it turns out that AI is not the right solution for a particular issue, it is OK to be transparent about this as well.
- Protection of human dignity has to be at the center of all development and deployment of technology by authorities.
- Facial recognition for investigation is an opportunity for law enforcement but also represents challenges. For instance: misidentifications lead to discrimination.
- Domain specific frameworks, such as the policy framework for responsible limits on facial recognition technology by law enforcement, are crucial to guide users while using AI-tools in a practical way.
- Independent testing of the technology is fundamental to ensure that it performs well. Independent research and test authorities are necessary to improve the framework and the development of facial recognition technology.
- Involvement of human beings should always be required, preferably well trained examiners. Human biases are at least as important as technology biases.

Summary of discussions in the sessions

The Hague Conference on Responsible AI

AI and regulation

Principles and regulatory proposals

In the past years, a lot of international principles that promote the use of trustworthy AI that respects human rights and democratic values have already been established (e.g. OECD). Right now, these principles are being translated into regulation and within organizations to processes. The European Commission (EC) published their proposal for an AI Act in 2021, which is currently being negotiated, and the Council of Europe (CoE) will follow later this year with a proposal on a regulatory framework on AI. Overall, there is an agreement that rules for AI-systems must take the specific contextual risks into account. Not all AI has severe impact on people. That's why these regulatory proposals follow a risk-based approach. There is also a need for a more integrated approach on the development of different regulations with respect to regulations already in place. This is because AI is often used in an already unregulated context meaning that also existing regulations could apply to the use of AI-systems for a specific use.

AI and regulation

Standardization

These regulations will require concrete standards and tools to put them into practice. The EU AI Act explicitly leaves room for standards to lay down the details of the requirements that AI-systems must meet. However, leaving room for standards also delegates some regulatory power to those who create the standards. Currently these standards are created within international organizations in which large companies are active. There was some discussion about the democratic character of this process. The standardization process must be more inclusive. For example, civil society organizations have to be included and public authorities need to be more involved in the creation of standards. How standards protect fundamental rights needs more clarification. This is important because standards are not only an elaboration of technical requirements, but also of requirements such as transparency and fairness that aim to protect fundamental rights. Communities and underrepresented groups need to be part of the conversation.

AI and regulation

Practical tools and frameworks

Besides horizontal standards and regulation, domain specific policies and frameworks can also prove to be useful. One example is a framework that is currently being developed for the responsible use of Facial Recognition for law enforcement. Another example is the AP4AI framework that helps internal security practitioners to demonstrate the compliance of their AI systems from an accountability perspective. These frameworks, based on best practices, can guide users of AI-tools to deploy it in a responsible way. In general, experiences, tools and best practices must be shared more often because there is a need for good methodology for value driven design techniques. Often, practitioners are very aware of fundamental rights risks around AI, but are not sure how to apply principles in practice.

Besides following regulations, companies and organizations that design and use AI will have to implement their own responsible practices. Microsoft and google shared their responsible AI journey and presented their objectives, guiding principles and practices. This pertains much more than the complexity of technical issues and design. It is all about the social context in which the techniques are deployed in. Working on changing the mindset of people, training engineers, review committees and having clear standards. Apart from having clear principles, it equally important to bring people from different perspectives (lawyers, engineers, policy makers, etc.) to the table and have in-depth discussions on applications. From the design phase to the product launch.

A general concern is the position of SME's. They don't have the means to set up structures and tools for ethical AI as big tech has. They need extra help.

AI and regulation

Creating policies for a fast changing context

One of the biggest challenges of regulating AI is that the regulatory object itself is a moving target. AI applications and the techniques involved are constantly evolving. That's why regulation can't be too detailed since that would require constant regulatory changes, and changing regulation is a lengthy process. We must reflect together on how we can keep regulation agile enough to remain effective.

A possible way to create and assess effective and evidence-based policies is by using a policy prototyping method. Policy prototyping is based on design thinking and it tests the effectiveness of policies by involving various stakeholders and putting policy into practice. Questions that are asked in this method are for example: Are companies and organizations capable of performing the policy interventions and are there unexpected side effects? Is the policy effective? Does the intervention contribute to the outcome? This will consequently result in policy recommendations.

AI and regulation

Civil society and stakeholder participation

Involving stakeholders such as civil society and academia in the process of policymaking and the design and use of AI is necessary to stimulate responsible and human-centric AI.
A concept in The Netherlands that brings this into practice is the so-called ELSA Lab.
In these labs, consortiums of different institutions collaborate in a co-creation process, a bottom-up approach. The aim is to ensure that companies, governmental authorities, centers of expertise, civil society organizations and the general public develop responsible applications of AI jointly. However, involving the public can be a challenge. We need to find the right ways to ensure ex ante (civilian-) stakeholder participation in the design, development, implementation and evaluation regarding AI issues. What are good feedback mechanisms?

https://nlaic.com/wp-content/uploads/2022/02/ELSA-Labs-for-Human-Centric-Innovation-in-AI.pdf

The OECD Artificial Intelligence Policy Observatory - OECD.AI
Platform for information and dialogue on AI (policies, principles, trends and data)

https://pair.withgoogle.com/explorables/

https://ai.google/responsibilities/

AI and cybersecurity, -norms and diplomacy

Impact AI on the cyber domain

There are three ways of AI impacting security in cyberspace: security against AI, security using AI and security of AI-systems. At the moment, the international community is not mature enough in any of these areas. When we look at the impact that AI will have on the cyber domain, it is important to distinguish between the implications of the **technology** itself by disentangling it in its various components (decision-making capabilities, abundance of data, unpredictable outcomes of machine-learning) and the **context** within which the technology is implemented (enhanced military state capabilities, monopolies by large corporations). Because of AI's nature as a general purpose technology, the impact on the cyber domain always has to be connected to particular malicious intent or behavior and the context. Moreover, AI is also a dual-use technology. Take for instance the capabilities of AI to scan enormous amounts of malware: many of these applications can both enhance and deteriorate cybersecurity. At the same time, there is a point where a higher level of cyber-defense might require some offensive actions.

AI and cybersecurity, -norms and diplomacy

AI and UN OEWG Discussions

The current multilateral normative framework on responsible state behavior in cyberspace focuses on malicious use of technology and not on the technology itself. The question is whether there is something unique about AI: do we need specific AI norms on responsible state behavior? The UN Open Ended Working Group (OEWG) concerns responsible state behavior in cyberspace. However, it is not fully clear whether the current normative framework regulating the use of ICTs by states can adequately address the innovation that AI will bring to the cyber domain.

Many activities we worry about with AI are below the threshold of (violent) conflict. This means that we are dealing with norms and other forms of law that are not international humanitarian law (IHL). In the UN, two issues were flagged by states: autonomy vs. automation and information operations. Does automation require us to think about state behavior or individuals? The answer is probably state behavior: the problem is not technology or AI, but the actor using it to violate the norms we have, for instance by attacking critical infrastructure.

Moreover, we have to be aware of the loss of authenticity in these frameworks. Many of the institutions and frameworks we have were created on the assumption that an actor is responsible for the actions they undertake. With AI, we may lose that authenticity: it is very difficult to track the person responsible for actions on the web across the line of the technology or network. Some bots look more real than actual people.

AI and cybersecurity, -norms and diplomacy

The dynamics of regulation

Even though law is not perfect (for instance because we do not have all the tools to stimulate what is going to happen), it is the bottom line or baseline. The bulk of governance is focused on the impact of AI. It is about how risk impacts people and hopefully adds incentive cycles to pull out that risk before it is discovered with uncontrollable outcomes. We need to evolve and process AI while developing legal concepts and continue to try how these technological realities can be incorporated, while wondering: how do we uphold this principle really, when we're dealing with this technology?

But there are problems. The first challenge is having a policy and then try to translate it to the everyday realities of a computer scientist. When writing and adopting principles on the use of AI, it is imperative to reach out to those who actually develop the systems to ensure that principles are practical and realistic. Secondly, in the context of quantifying mistakes, we are caught in the conflict of constraining progress in fear of causing harm. What is the cost of causing a mistake (for an AI-developer)? We need to unblock ourselves from setting unreliably high standards. In other words: it should be taken into account that private sector development is necessary and should not be hampered by too many risks of liability. This requires a clear concept of responsibility, which is complicated by the fact that an accurate AI-facilitated decision could be taken based on the data available, but these data might have been incomplete or false. A third issue is the playground: where do you play out these policies? There is an imperfect condition for knowing what you know ('the fault of war'). What kind of decisions do you make in such a situation? What kind of training is allowed? Moreover, it matters where you are. AI applications in Social Credit Scoring or military contexts are different from liking preferences. What kind of errors are acceptable depending on the field we are in?
And what do you do with systems that are designed to hurt people?

AI and cybersecurity, -norms and diplomacy

The mission for the cybersecurity community

How should the cybersecurity community think about the explainability, accountability and transparency of AI systems? By trying to move into these layers as deeply as possible: you need an actual value, policy goals and incentive to get there. Accountability is just a process. Moreover, not necessarily by regulation of companies, but of some markets: getting the values in the systems is more in market regulation, not the layer on top of that. An example is given by NATO, which actively engages with contractors to check whether systems comply with the NATO principles on AI. This should go further than simply checking the box of compliance, but needs to cover testing, probing and simulating incidents. This way we could move from mere confidence to a stronger, tangible form of trust.

When we talk about particular AI norms, we also need to make our interests more explicit. When we talk about the human in the loop, we need to be clear on why we need the human and on what values we base this. Respect for human rights is already a big differentiator between countries. Companies have also not been as explicit as they could be about the choices they base their actions on, and in many cases they could be more transparent about their failures and the attacks that they have suffered. Building upon this, we also have to reconsider what true multistakeholder cooperation means in this context. Tech companies are now much more than knowledge providers. They are providing the infrastructure, networks, replacing policy decisions (also in policy contexts), but they do not sit around the table. In other words: there is a fundamental mismatch between state-heavy process of international law and places where effective power has already gone. We need to try to reduce the gap between the two. This goes back to the need for political incentive and will.

AI and cybersecurity, -norms and diplomacy

AI in the military domain

In the military domain the use of AI is becoming more and more relevant. AI in the military domain will help us with maintaining international peace and security. At the same time we need to be aware of the dilemmas military AI brings us. Internationally there are concerns on for example accountability and proportionality issues. It calls for tools to govern the use and development of such technologies in the military domain. With the legal basis of international humanitarian law, additional governance tools can be helpful and when specific enough, such tools can create responsible behavior amongst actors in the field of AI.

As goes for the civil use of AI, in the military context the responsible use of AI starts in the development phase. When developing AI enhanced (military) tools, it's important to consider common security aspects as well as moral values and legal frameworks.

All stakeholders need to consider how to incorporate them in the design. Human-machine interaction is essential in this debate and we need to be very specific about the context in which military AI applications are used.

AI and the city

‘Urbanize’ AI

Can AI help us build sustainable, inclusive and dynamic cities? We are coming out of an age where “the solution is in the data”. The hype of the smart city concept has tempted many cities to tackle urban issues with technology such as AI. Optimization of urban services such as water management, urban logistics and infrastructure maintenance can contribute to safer and more efficient cities. However, cities are more than an optimized platform offering a frictionless user experience. Worldwide we have seen many examples of protest, against surveillance, discrimination and loss of privacy. Work of UrbanAI (www.urbanai.fr) shows that in real life we need more awareness that safeguards require us to think more about what kind of data we need.

In addition to optimize cities, we must “urbanize” technology. That is, designing and developing technologies that promote urbanity and cityness. Urbanized technologies are situated (they emanate from a social contract, a culture and a geography), open (they need to be accessible for all and evolutive), decentralized (they need to empower communities and be equally distributed), frictional (they need to encourage exploration through interactions), meaningful (they need to amplify human speech) and ecological (they need to be frugal and low carbon).

AI and the city

Law Enforcement: Facial Recognition Technology

Facial recognition is a technology that is rapidly progressing and also law enforcement agencies use it. It is used for criminal investigations. In Europe there is no live facial recognition in the public domain running at the moment.

The technology represents challenges, such as misidentifications and discrimination. Especially people of color are affected by false positive facial recognition tests conducted in the US. There are also privacy issues: background or compromising pictures need to be filtered out.

To address these issues a policy framework has been presented by Unicri in 2021. This will help improve the work of law enforcement and policy makers to develop national legislation. A wide range of stakeholders has been consulted in putting together this framework. In 2022 the framework will be tested worldwide and a training program will be developed.

Currently there is no independent authority to test tools. Governments have questions about biometrics investigations and vendors make claims about their performances. Universities may play a crucial role in finding answers and gaining knowledge. An expertise center in biometrics is needed

AI and the city

Create a social contract around AI

A city is not only defined by its built environment but its uses and people. This so-called “cite” is a common space coined by people who share interests and values. Few digital spaces follow this principle: most of the platforms and social media are following rules that have been decided unilaterally. Cities that want to implement AI have to create a social contract around AI. Citizens and other stakeholders have to be engaged from the very beginning. Successful implementations of AI in a city context show examples that are suboptimal in terms of efficiency.

The city of the Hague’s data strategy is a useful case study, as it is based around this principle. The strategy is helping understand the complexity of all sorts of societal issues. The Hague wants to make responsible use of data and thereby the privacy and security of putting residents first. Two important factors are transparency and explicability: citizens are able to consult the online algorithm register. This also aligns with the international FAIR principles.

Annex I – Programme and sessions of the conference

Programme 12 may - Preconference / walking dinner

17:00h Network reception

18:00h Welcome speech
Mayor of The Hague, Jan van Zaanen

18:25h Plenary pitches on conference themes
Irakli Beridze, Michael Street en Cornelia Kutterer

18:40h Round table discussion – Part 1

19:00h Networking break with live music

19:25h Round table discussion – Part 2

19:40h Keynote takeaways
Director for Artificial Intelligence Policy, Ministry of Justice and Security
Michel van Leeuwen

Cyberambassador for the Netherlands, Ministry of Foreign Affairs
Nathalie Jaarsma

Director for International Affairs, Municipality of The Hague
Wim Jansen

20:00h Networking drinks

20:30h End of preconference

Annex I – Programme and sessions of the conference

Programme 13 may - Conference

09:30h **Network reception**

10:30h **Plenary programme – part 1**
Welcome & Opening
Keynote speech *Alexandra van Huffelen*
Minister for Digitalisation of the Netherlands

10:50h **Video message by Eric Schmidt**
Ex-CEO Google
Special Competive Studies Project

10:50h **Panel discussion**
Jan Kleijssen - Director of Information Society - Action against Crime, Council of Europe
Audrey L. Plonk - Head of Digital Economy Policy Division, OECD
Kilian Gross - Head of Unit, AI Policy Development and Coordination, DG CONNECT, European Commission
Vanja Skoric - Program Director - European Center for Not-For-Profit Law

11:30h **Coffee break**

12:00h **Break out sessions round 1**

13:00h **Lunch**

14:00h **Break out sessions round 2**

15:00h **Coffee break**

15:30h **Plenary programme – part 2**
Short reflections
Closing speech Saskia Bruines
Alderman for Economy, International, Services and 2nd Deputy Mayor The Hague

16:00h **Networking drinks**

17:00h **End of conference**

Annex I – Programme and sessions of the conference

Programme 13 may - Conference

12:00h **Break out sessions round 1**

Theatre 1 *UNICRI - Irakli Beridze*
Responsible use of facial recognition technology in law enforcement: designing national and international frameworks
AI and the city

Theatre 2 *Google - Johnny Soraker & Ben Zevenbergen*
The application of Google's AI Principles to enable Responsible Innovation practices.
AI technology and its application in the domain of peace, justice and security

Theatre 3 *NATO-NCIA - Michael Street*
How will AI impact cybersecurity?
AI and Cybersecurity

Theatre 4 *Urban AI - Hubert Beroche*
It's time to urbanize Artificial Intelligence
AI and the city - applications for peace and security

Seminar Room *Asser Institute - Berenice Boutin*
The Interface of Ethical and Legal Principles on (Military) AI: Towards Mutually Strengthening Frameworks
AI and international Policy - Law - Diplomacy

Foyer room *UNIDIR - Giacomo Persi Paoli & Chris Meserole*
Navigating technological convergence: does the international community need new norms on Cyber and AI?
AI and Cybersecurity

Lounge room
Ask me anything sessions
Pitch 1: *Katerina Yordanova – KU Leuven, CiTiP*
Pitch 2: *Vanja Skoric – European Center Not-For-Profit Law Stichting*

13:00h **Lunch**
14:00h

Annex I – Programme and sessions of the conference

Programme 13 may - Conference

14:00h **Break out sessions round 2**

Theatre 1 *UNICRI - Irakli Beridze*
Responsible use of facial recognition technology in law enforcement: designing national and international frameworks
AI and the city

Theatre 2 *Microsoft - Cornelia Kutterer & Annemarie Costeris*
Microsoft's internal AI journey
AI and international Policy - Law - Diplomacy

Theatre 3 *EUROPOL & Centric - Ben Waites & Gregory Mounier*
Accountability Principles for Artificial Intelligence (AP4AI): A Universal Framework for the Internal Security Domain
AI technology and its application in the domain of peace, justice and security

Theatre 4 *University of Delft, Leiden University - Bram Klievink, Roel Dobbe*
A learning approach to responsible AI – the ELSA-lab (ethical legal and societal aspects) methodology
AI technology and its application in the domain of peace, justice and security

Seminar Room *Robotics & AI Law Society and Oxford Institute (RAILS) - Martin Ebers*
Transforming ethical norms into standards that help organizations and developers create responsible AI
AI and international Policy - Law - Diplomacy

Foyer room *UNIDIR & Brookings Institute - Giacomo Persi Paoli & Chris Meserole*
The role of norms in AI cyberconflict - Possible gaps in international frameworks and regulations
AI-Cybernorms and Cybersecurity

Lounge room
Ask me anything sessions
Pitch 1: *Ana Chubinidze – Adalan AI*
Pitch 2: *Marloes Pomp – NLAIC*
Pitch 3: *Yi Ling Teo – Centre of Excellence for National Security*

15:00h **Coffee break**
15:30h

Annex 2 Participating organizations

Access Now
Adalan AI
AI for Good Foundation
AI Team - Ministry of Justice and Security
AI Transparency Institute
Alkemio, YES!Delft
Altada
Ambassade van Frankrijk in Nederland
ANEC
Asser Institute
Autoriteit Persoonsgegevens
Belastingdienst
Birch
Booking.com
British Embassy The Hague
Brookings Institution
Burgemeester Den Haag
CEA
CENTRIC
CERT-MU
CFLW Cyber Strategies
CGI Nederland BV
City Council The Hague
City of The Hague
Considerati
Council of Europe
Cyber Resilience for Development (Cyber4Dev)
Delft University of Technology
DG HOME
DG Trésor
Donders Institute for Brain, Cognition and Behaviour, Radboud University
Douane
DROG
Dutch Ministry of the Interior and Kingdom Relations
Dutch Police – National Division
ECP
Elsevier
Embassy of El Salvador in the Kingdom of the Netherlands
ESA
ETH Zurich CSS
EU Agency for Fundamental Rights
EU Innovation Hub for Internal Security
Eurojust
European Center for Not-for-Profit Law (ECNL)
European Commission
European Space Agency
Europol
EY
EY (Ernst & Young), and University of Nottingham
French embassy
Friedrich Schiller University
Fundación Vía Libre
Gemeente Den Haag
GLG
Google
Hague Conference on Private International Law
HZ University of Applied Sciences
IEEE
iHub, Radboud University Nijmegen
iivii.eu / University of Oxford / European Uni Cyprus
Indra
Institute for Accountability in the Digital Age
INTERPOL
JADS/Tilburg University
Korean National Police Agency
KPMG
KU Leuven Centre for IT & IP Law (CITIP)

Annex 2 Participating organizations

Leiden University
Maastricht University
MFA Netherlands
Microsoft
Milieu Law & Policy Consulting
Min J&V
Ministery Internal affairs
Ministery of Foreign Affairs
Ministry for Justice and Security
Ministry of Economic Affairs and Climate Policy
Ministry of Finance
Ministry of Foreign Affairs of the Kingdom of the Netherlands
Ministry of Information Technology, Communication and Innovation
Ministry of Interior and Kingdom Relations
Ministry of Internal Affairs
Ministry of Justice of the Slovak Republic
Ministry of the Interior and Kingdom Relations
Mooncake AI / Hogeschool Utrecht
Municipality of Rotterdam
Nationaal Cyber Security Centrum (NCSC)
Nationale Politie
NATO C&I Agency
NEN
Netherlands Police
NL AIC
NL Ministry of Justice and Security
NL Police
NLAIC
OECD
Patrick J. McGovern Foundation
Politie
Radboud University and TU Delft
RELX
Robotics & AI Law Society (RAILS)
Royal Philips
S Rajaratnam School of International Studies, Centre of Excellence for National Security
Schmidt Special Competitive Studies Project (SCSP)
Security Delta HSD
Special Competitive Studies Project
Stanford
SURF
Swedish Police; National Operations department
T.M.C. Asser Institute
Techniek, Bestuur en Management, TU Delft
Tencent
The Asser Institute
The GovLab
The Hague Centre for Strategic Studiez
The Hague Municipality
Tilburg University
TNO
Transparancy International Netherlands
TU Delft
UbiOps
UN
UNIDIR
Universiteit Twente
University of applied sciences Rotterdam
University of Leiden
Utrecht Data School
Utrecht University
VNO-NCW/MKB-Nederland
VU
ZInspection initiative

The Hague Conference on Responsible AI