CIFAR

WORKSHOP BRIEF

BEYOND ARMS CONTROL: REGULATORY OPTIONS FOR AI TECHNOLOGIES

Artificial intelligence (AI) technologies are growing more prevalent in security and defense applications, but there are growing concerns about their potential to disrupt relations between nations. To date, discussions among experts have focused primarily on developing international conventions for using these technologies in military contexts. However, there is a need for practical and operational outcomes as AI is deployed more widely.

On January 30-31, 2020, in partnership with the workshop leadership team, CIFAR convened 21 experts from academia and civil society to move forward on insights from the first workshop in this series that took place July 2019: Regulation of Defense and Security AI Technologies: Options Beyond Traditional Arms Control. These experts shared their perspectives to determine actionable regulatory options for AI-powered defense and security technologies.

IMPACTED STAKEHOLDERS

- Humanitarian organizations and civil society
- Technologists and engineers
- State security and military organizations
- Non-state and paramilitary actors
- Private technology corporations
- Academics and researchers

KEY INSIGHTS

1. Setting norms and conventions across different stakeholder groups for use of AI in security and defense systems could lead to superficial recommendations, but could be a starting platform for more meaningful conversation and engagement.
2. Corporate self-regulation and corporate social responsibility are options for ensuring responsible applications of AI technologies, but should be coupled with legal frameworks, government oversight, and mission standards to be effective.
3. Sharing information and collaborating openly are key to fostering trust and transparency between stakeholders. These exchanges are already happening within the scientific community, which can serve as a model for how to engage policymakers and military communities.
4. Defense and security agencies are secretive and adversarial by nature, which poses an obstacle to international and cross-sector cooperation. This creates an opportunity for other sectors and actors to set an example for a more collaborative dynamic.
5. Civil society is an important stakeholder and should be engaged, but its role and influence varies across jurisdictions so it is important to understand these nuances.
6. Explainability is widely considered important for recognizing the fallibility of machines, but these explanations can only be interpreted by experts and are not always useful for non-technical operators.
7. Directives bring together communities, encourage a diversity of perspectives, are transparent, add definitional clarity, and assign responsibility to stakeholders. They are important documents that can help set policies and actions in motion and should consider different communities in their development to ensure trust and buy-in.

RECOMMENDATIONS AND NEXT STEPS

1. Conversations about armament should be structured with all primary actors in mind, including defense and security agencies and vendors, at international, national, and sub-national levels. Conversations should acknowledge the responsibility and roles of the private sector, civil society, and academia.
2. Incentives for students and companies like scholarships and awards can be established to encourage participation amongst stakeholders who would otherwise be disengaged. This can also be a mechanism for international cooperation, and for inviting students and academics to create solutions.
3. Creating opportunities for introductory dialogues in more open forums can act as a foundation for more sensitive discussions in the future. More sensitive dialogues between states take place behind closed doors, but working with other communities in a transparent way can encourage engagement from security and intelligence agencies.
4. Governments should engage the private sector to develop norms to ensure AI technology is implemented and integrated in ways which won't cause escalation or destabilization of issues. This can be done through national labs, which traditionally have good relationships with relevant industries. Engaging professional societies rather than companies themselves could offer another route by which to engage with the private sector.
5. Professional bodies should set professional standards and on-going certification for AI practitioners to ensure that applications are implemented ethically and effectively as the technology evolves. Engaging end users in this process, creating transparency, and sharing best practices could have a stabilizing effect.

LEADERSHIP TEAM

- David Danks, Carnegie Mellon University
- Ambassador (ret) Paul Meyer, Simon Fraser University
- Giacomo Persi Paoli, UN Institute for Disarmament Research (UNIDIR)
- Kerstin Vignard, UNIDIR

FURTHER READING

- Workshop Brief: Beyond Arms Control: Regulating Defense and Security Technologies
- National Security Commission on Artificial Intelligence: March 2020 First Quarter Recommendations
- How Would Future Autonomous Weapon Systems Challenge Current Governance Norms?
- The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume III, South Asian Perspectives
- Artificial Intelligence: A Revolution in Strategic Affairs?

CIFAR

RÉSUMÉ DE L'ATELIER

AU-DELÀ DU CONTRÔLE DES ARMES : OPTIONS RÉGLEMENTAIRES POUR LES TECHNOLOGIES D'IA

Les technologies d'intelligence artificielle (IA) sont de plus en plus répandues dans les applications de sécurité et de défense, mais on s'inquiète de plus en plus de leur potentiel à perturber les relations entre les nations. Jusqu'à présent, les discussions entre experts ont principalement abordé l'élaboration de conventions internationales sur l'utilisation de ces technologies dans un contexte militaire. Toutefois, à mesure que l'IA se déploie plus largement, une approche pratique pour obtenir des résultats sur le plan opérationnel doit être envisagée.

Les 30 et 31 janvier 2020, en partenariat avec l'équipe responsable de l'atelier, le CIFAR a réuni 21 experts du milieu universitaire et de la société civile afin de faire progresser les réflexions du premier atelier de cette série qui a eu lieu en juillet 2019, Au-delà du contrôle des armes traditionnelles : Réglementation des technologies de défense et de sécurité basées sur l'IA. Ces experts ont partagé leurs points de vue afin de dégager des options réglementaires applicables aux technologies de défense et de sécurité basées sur l'IA.

INTERVENANTS TOUCHÉS

- Organisations humanitaires et société civile
- Technologues et ingénieurs
- Organisations militaires et chargées de la sécurité de l'État
- Acteurs non étatiques et paramilitaires
- Sociétés technologiques privées
- Universitaires et chercheurs

FAITS SAILLANTS

1. L'établissement de normes et de conventions sur l'utilisation de l'IA dans les systèmes de sécurité et de défense par les différents groupes de parties prenantes pourrait conduire à des recommandations superficielles, mais cela pourrait aussi constituer une plateforme de départ pour des discussions et un engagement plus substantiels.
2. L'autorégulation et la responsabilité sociale des entreprises sont des moyens de garantir l'utilisation responsable des technologies d'IA, mais, pour être efficaces, elles doivent être associées à des cadres juridiques, à une supervision gouvernementale et à des normes de fonctionnement.
3. Le partage d'informations et la collaboration ouverte sont essentiels pour favoriser la confiance et la transparence entre les parties prenantes. Ces échanges ont déjà lieu au sein de la communauté scientifique et pourraient servir de modèle sur la manière de mobiliser les décideurs politiques et les communautés militaires.
4. Les agences de défense et de sécurité sont discrètes par nature, ce qui constitue un obstacle à la coopération internationale et intersectorielle. Cela offre l'occasion à d'autres secteurs et acteurs de donner l'exemple d'une dynamique plus collaborative.
5. La société civile est une partie prenante importante et devrait être mobilisée, mais son rôle et son influence varient d'une région à l'autre. Il est important de comprendre ces nuances.
6. L'explicabilité est considérée comme un facteur très important pour déterminer la faillibilité des machines, mais ces explications ne peuvent être interprétées que par des experts et ne sont pas toujours utiles aux opérateurs non techniques.
7. Les directives rassemblent les communautés, stimulent la diversité des points de vue, sont transparentes, clarifient les définitions et responsabilisent les parties prenantes. Il s'agit de documents importants qui peuvent aider à mettre en place des politiques et des actions. Leur élaboration devrait tenir compte des différentes communautés afin de favoriser leur confiance et leur adhésion.

RECOMMANDATIONS ET PROCHAINES ÉTAPES

1. Les discussions sur l'armement doivent être structurées en tenant compte de tous les acteurs principaux, y compris les agences et les fournisseurs dans les domaines de la défense et de la sécurité aux niveaux international, national et infranational. Les discussions doivent reconnaître la responsabilité et le rôle du secteur privé, de la société civile et des universités.
2. Des mesures incitatives pour les étudiants et les entreprises, telles que des bourses et des prix, peuvent être mises en place pour encourager la participation de parties prenantes qui, autrement, seraient peu enclines à s'engager. Il peut également s'agir d'un mécanisme de coopération internationale invitant les étudiants et les universitaires à créer des solutions.
3. De nouvelles possibilités de dialogues préliminaires dans des forums plus ouverts peuvent servir de base à des discussions plus délicates à l'avenir. Les échanges plus confidentiels entre États se déroulent à huis clos, mais le fait de travailler avec d'autres communautés de manière transparente peut favoriser l'engagement des agences de sécurité et des services de renseignement.
4. Les gouvernements doivent inciter le secteur privé à élaborer des normes pour assurer que les technologies d'IA sont mises en œuvre et intégrées de manière à ne pas provoquer une escalade des problèmes ou une déstabilisation. Cela peut se faire par l'intermédiaire des laboratoires nationaux, qui ont traditionnellement de bonnes relations avec les industries concernées. Mobiliser des sociétés professionnelles au lieu des entreprises elles-mêmes est une autre façon de s'engager avec le secteur privé.
5. Les organismes professionnels devraient établir des normes professionnelles et instaurer une démarche continue de certification pour les praticiens de l'IA afin de garantir que les applications sont mises en œuvre de manière éthique et efficace au fur et à mesure que la technologie évolue. La participation des utilisateurs finaux à ce processus, la promotion de la transparence et le partage des meilleures pratiques pourraient avoir un effet stabilisateur.

ÉQUIPE

- David Danks, Université Carnegie Mellon
- Paul Meyer (ex-ambassadeur), Université Simon Fraser
- Giacomo Persi Paoli, Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR)
- Kerstin Vignard, UNIDIR

LECTURES COMPLÉMENTAIRES

- Résumé de l'atelier Au-delà du contrôle des armes : Réglementation des technologies de défense et de sécurité basées sur l'IA
- National Security Commission on Artificial Intelligence: March 2020 First Quarter Recommendations
- How Would Future Autonomous Weapon Systems Challenge Current Governance Norms?
- The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume III, South Asian Perspectives
- Artificial Intelligence: A Revolution in Strategic Affairs?