Artificial Intelligence, Vulnerabilities, and Autonomous Weapons

Diego Latella

Consiglio Nazionale delle Ricerche
Istituto di Scienza e Tecnologie dell'Informazione 'A. Faedo', Pisa (CNR-ISTI)
Lab. on Formal Methods & Tools for system design and analysis
- - - o o o - - -
Segretario Nazionale of Unione degli Scienziati Per Il Disarmo ONLUS (USPID)
- - - o o o - - -
International School On Disarmament And Research on Conflicts (ISODARCO)
o o o - - - o o o

ISODARCO winter course 2019
Andalo (TN), IT, 6-13 January 2019

BIBLIOGRAPHY

References

[AI 2017] S. Abaimov, P. Ingram.
HACKING UK TRIDENT: A Growing Threat.
BASIC. 2017.

[AC 2017] G. Allen and T. Chan.
Artificial Intelligence and National Security
HARWARD Kennedy School.
BELFER CENTER for Science and Int. Affairs. STUDY 2017

[ASSST 2018] D. Amoroso, F. Sauer, N. Sharkey, L.Suchman and G.Tamburrini
Autonomy in Weapon Systems
The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy
Heinrich Boell Stiftung.
Publication Series on Democracy. Vol 49. 2018.

[AT 2017] D. Amoroso and G.Tamburrini
The Ethical and Legal Case Against Autonomy in Weapons Systems.
Global Jurist.
De Gruyter. Vol. 18, Issue 1. 2017.

[ALRL 2004] A. Avižienis, J-C. Laprie, B. Randell, and C. Landwehr
Basic Concepts and Taxonomy of Dependable and Secure Computing
IEEE TRANS. ON DEP. AND SEC. COMPUTING. VOL. 1, NO. 1, JANUARY-MARCH 2004

[BBL 2015] C. Baylon, R. Brunt, D. Livingstone.
Cyber Security at Civil Nuclear Facilities.
Understanding the Risks.
Chatham House Report. Chatham House. 2015.

[BV 2017] V. Boulanin and M. Verbruggen.
Mapping the Development of Autonomy in Weapon Systems
SIPRI. 2017

[BM 2017] B. Buchanan and T. Miller.
Machine Learning for Policymakers
What It Is and Why It Matters
HARWARD Kennedy School.
BELFER CENTER for Science and Int. Affairs. PAPER 2017

[DII+ 2017] J. Davis II, B. Boudereaux, J. Welburn, J. Aguirre, C. Ogletree, G. McGovern, M. Chase.
Stateless Attribution.
Towards International Accountability in Cyberspace
RAND 2017

[Din 1987] A. Din (Ed.).
ARMS AND ARTIFICIAL INTELLIGENCE.
Weapon and Arms Control Applications of Advanced Computing
SIPRI 1987

[Deshpande 2018] A. Deshpande.
A Beginner's Guide To Understanding Convolutional Neural Networks.
https://adeshpande3.github.io/adeshpande3.github.io/A-Beginner's-Guide-To-Understanding-Convolutional-Neural-Networks/ (acc. on Nov. 28, 2018)

[DSB 2013] DOD Defense Science Board
Resilient Military Systems and the Advanced Cyber Threat.
Task Force Report 2013

[EP 2018] European Parliament.
European Parliament resolution of 12 September 2018
on autonomous weapon systems.
Text Adopted. Provisional Edition. (2018/2752(RSP)).
https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/50465/autonomous-weapons-must-remain-under-human-control-mogherini-says-european-parliament_en (acc. on Nov. 22, 2018)

[EUEA 2018a] EU External Action.
Autonomous weapons must remain under human control, Mogherini says at European Parliament.
News Stories. Sep. 14, 2018.
https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/50465/autonomous-weapons-must-remain-under-human-control-mogherini-says-european-parliament_en (acc. on Nov. 22, 2018)

[EUEA 2018b] EU External Action.
About the Global Tech Panel.
News Stories. Sep. 21, 2018.
https://eeas.europa.eu/headquarters/headquarters-homepage/50886/about-global-tech-panel_en (acc. on Nov. 23, 2018)

[Futter 2016] A. Futter 2016.
Cyber Threats and Nuclear Weapons.
New Questions for Command and Control, Security and Strategy.
Occasional paper
Royal United Services Institute for Defence and Security Studies. 2016.

[GL 2018] E. Geist and A. Lohn.
Security 2040. How Might Artificial Intelligence Affect the Risk of Nuclear War.
Perspective. Expert Insights on a Timaly Policy Issue. RAND, 2018

[GAO 2017] Government Accountability Office.
INTERNET OF THINGS. Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD.
Report to Congressional Committees, GAO-17-668, 2017

[GAO 2018] Government Accountability Office.
WEAPON SYSTEMS CYBERSECURITY. DOD Just Beginning to Grapple with Scale of Vulnerabilities.
Report to the Com.te on Armed Services, U.S. Senate, GAO-19-128, 2018

[KAFKMH 2018] G. Klein, J. Androvick, M. Fernandez, I. Kuz, T. Murray, G. Heiser
Formally Verified Software in the Real World. Verified software secures the Unmanned Little Bird autonomous helicopter against mid-flight cyber attacks.
Communications of the ACM. VOL. 61, NO. 10, Oct. 2018

[NPR 2018] DOD Office of the Secretary of Defense.
Nuclear Posture Review. DOD 2018.
via `https://fas.org/issues/nuclear-weapons/nuclear-posture-review/`
`(acc. on Dec. 6, 2018)`

[NTI 2018] Nuclear Threat Initiative.
Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons (BTWC).
https://www.nti.org (acc. on Nov. 20, 2018)

[Sanderson 2017] G. Sanderson.
But what *is* a Neural Network?
3Blue1Brown. October 5, 2017
https://www.youtube.com/watch?v=aircAruvnKk

[Schneier 2018] B. Schneier.
Click Here to Kill Everybody.
W.W. Norton & C. 2018 .

[SF 2014] P. Singer, A. Friedman.
Cybersecurity and Cyberwar.
What Everyone Needs To Know ®
Oxford U.P. 2014

[UL 2018] B. Unal, P. Lewis.
Cybersecurity of Nuclear Weapons Systems.
Threats, Vulnerabilities and Consequences.
Research Paper. ISD - Chatham House. 2018.

[UNIDIR 2018] UN Institute for Disarmament Research.
The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence
a primer for CCW delegates
UNIDIR RESOURCES. No. 8, 2018

[UNODA 2018a] UN Office for Disarmament Affairs.
The Biological Weapons Convention
https://www.un.org/disarmament/wmd/bio/ (acc. on Nov. 20, 2018)

[UNODA 2018b] UN Office for Disarmament Affairs.
Developments in the field of information and telecommunications in the context of international security.
https://www.un.org/disarmament/topics/informationsecurity/ (acc. on Dec. 7, 2018)

[WMN 2016] R. Watson, S. Moore P. Neumann
CHERI: A Hardware-Software System to Support the Principle of Least Privilege
ERCIM News 106, July 2016.

[Wiki 2018a] Wikipedia
Deep Learning
Wikipedia.
https://en.wikipedia.org/wiki/Deep_learning (acc. on Jun. 9, 2018)

[Wiki 2018b] Wikipedia
Tensor Processing Unit
Wikipedia.
https://en.wikipedia.org/wiki/Tensor_processing_unit (acc. on Jun. 10, 2018)

[Wiki 2018c] Wikipedia
Future Combat Systems
Wikipedia.
https://en.wikipedia.org/wiki/Future_Combat_Systems (acc. on jun. 11, 2018)

[Wiki 2018d] Wikipedia
IAI Harop
Wikipedia.
https://en.wikipedia.org/wiki/IAI_Harop (acc. on Jun. 12, 2018)

[Wiki 2018e] Wikipedia
Brimstone (missile)
Wikipedia.
https://en.wikipedia.org/wiki/Brimstone_(missile) (acc. on Jun. 12, 2018)

[WMW 2018] Wolfram MathWorld.
K-Means Clustering Algorithm
Wolfram MathWorld.
http://mathworld.wolfram.com/K-MeansClusteringAlgorithm.html (acc. on 9 giugno 2018)

More on the subject . . .

Unione degli Scienziati Per Il Disarmo (USPID)

[Union of Scientists for Disarmament]

Web Site

www.uspid.org

$\longrightarrow$ Link

$\longrightarrow$ Computers: National security, War, and Civil Rights

(http://www.uspid.org/compwa.html)

- o - o - O o - o -

USPID is member of the