



---

Annie Searle & Associates LLC

## Research Note

October 2015

### Artificial Intelligence as a Weapon

By Jorge Borunda

Copyright © 2015, ASA Institute for Risk & Innovation

Applicable Sectors: Defense

Keywords: Artificial Intelligence, Defense Sector, International Regulations, Human Rights, Weapons, New Technologies

*Abstract: This paper examines some of the concerns that are on the horizon around the development, implementation, and regulation of autonomous weapon systems. The U.S. Infrastructure Plan employs the Defense Industrial Base Plan, and while the Plan serves as a good resource to address risk and mitigate potential threats, but there is something the DIB does not cover, particularly the development of new technologies as weapons, such as artificial intelligence. When it comes to military artificial intelligence, Lethal Autonomous Weapons Systems (LAWS) select and engage targets without human intervention; they become lethal when those targets include humans. The International Committee of the Red Cross (ICRC) has raised concern on lethal autonomous weapon systems since 2011, arguing that there are no regulations to assess potential risks around how these new technologies will be used, as well as a lack of standards and methodologies.*

Every day, the world is in a constant and imminent threat of war, whether it is a nuclear war, a terrorist attack, a political coup, or simply a social uprising due to differences of opinions. Each country, within their laws and regulations, can defend their people from internal and external attacks. A key component for a defense plan is complex but efficient risk assessing and resiliency programs that will allow countries' armed forces to analyze and tolerate possible war or attack threats. To gain an edge in terms of war and attacks, technology has played such an important role – but it can also be considered as a wild card. Armed forces around the world are developing very sophisticated military technology and for the past few years, artificial intelligence has been the front-runner as the new modern warfare technology.

The U.S. Infrastructure Plan employs the Defense Industrial Base Plan (DIB), a unique plan that sets the U.S. apart from other countries in terms of developing a weapon system. The U.S. Department of Defense (DoD) uses the DIB as medium for its Risk Assessment Program, which it is very comprehensive yet it does not have regulatory requirements for companies to implement the risk assessment program into

their operations. This seems very inconsistent because as the U.S. is trying to assess possible risks and threats, the DoD is ignoring potential threats from within. The start of security and defense starts internally, then it can be rolled out to assess and mitigate outside threats.

Sector-specific agencies are required to focus on four important consequences: public health & safety, economic, psychological, and the impact on mission assurance. As stated in the DIB, “the last category is most relevant for the DIB as it relates to the impact on DoD’s ability to execute its roles, responsibilities, and mission under the Constitution and as assigned in statute and Executive Orders, policy, and national and defense strategies.”<sup>i</sup> However, the DIB or DoD should not solely focus on the impact on mission assurance, since these four consequences are interrelated and one leads to another. At the very least, they can affect each other at any given time, and the DoD should not shy away from the other three consequences. Therefore, they should adapt the DIB to better address these consequences as a whole. Diving deeper into how the DIB assesses consequences, vulnerabilities and risks, the DIB focuses on implementing its plan on a business, economic and technology level. It appears to be a well thought out process, but war and defense against possible threats are very sensitive subject matters, and the DIB needs to take into consideration the inclusion of ethical matters into its plan. Making or adding ethical changes to a plan, specifically to a government protection plan could become a very elaborate and difficult process but in order to achieve such result, Moeller says “as part of building an effective ethical culture in an enterprise, the ‘tone of the top’ messages of senior executives to others in the enterprise are very important.”<sup>ii</sup> Unfortunately, with the constant battles in the White House, the finger pointing among this country’s representatives and the frizz between Republicans and Democrats, an ethical shift at this level could be very lengthy and a messy one.

Aside from government’s structure and organization - and the political battles - the DIB does an amazing job at outlining its levels of defense. The DIB states five levels of defense starting with the First Level of Protection where asset owners are responsible for the risk. The Second Level is entitled to the local civilian law enforcement authorities, and as risk escalates, the Third Level is managed by the State and Federal law enforcement authorities. The Fourth Level is handle by the State Governor, and the final Fifth Level of protection escalates to the President. Although these are not similar to what Girling suggests with the first line of defense being the business line where “business owns operational risk should be managing it as it arises,”<sup>iii</sup> the DIB expanded Girling’s first line of defense into a more structural approach to have a better and more efficient chain of command system. Girling’s second line of defense is at the corporate level, for the DIB case, its Second Level of defense depends on its partnerships with DoD contractors. The Third Level of defense, an internal audit, the DIB employs a Sector Performance Measurement System in the form of scorecards that allow for review of sector performance.

Overall, the DIB - like the rest of the Department of Homeland Security - is a good resource to address risk and mitigate potential threats, but there is something the DIB does not cover. This is the creation or development of new technologies, in terms of weapons. Every country wants to have a competitive advantage, and wants to get ahead to be well prepared when it comes to protecting its people from a potential attack, whether it is internally or from a foreign country. Currently, the debate of the use of nuclear power for military purposes from North Korea and Iran has been a very heated topic. The United Nations and countries around the world have voiced concerns about the potential next “Third World

War,” whether in the form of a nuclear war or just the fight against extremists such as the ISIL (Islamic State in Iraq and the Levant). But there is something that has not been talked about, because it is an emerging technology with implications that have not been thought out yet: the use of artificial intelligence to produce weapons and be fully autonomous weapons.

Now, the use of robots in military settings has been researched for quite awhile, as countries want to reduce soldier casualties. But with the newest advancements in technology, artificial intelligence can be a game changer for better or for worse. This is a very thin line between trying to prove what the advantage or disadvantages of using robots are; the problem is how the armed forces will deploy them. Firstly, it is important to clarify a term that has been problematic and misused. When it comes to military artificial intelligence, “Lethal Autonomous Weapons Systems (LAWS) select and engage targets without human intervention; they become lethal when those targets include humans. LAWS might include, for example, armed quad-copters that can search for and eliminate enemy combatants in a city, but do not include cruise missiles or remotely piloted drones for which humans make all targeting decisions.”<sup>iv</sup> Remote-controlled systems such as drones or guided missiles are not considered LAWS as they are operated by humans.

LAWS are what the world needs to pay attention to, because the current research has raised the following fundamental ethical and principle questions:

- Can the decision over death and life be left to a machine?
- Can fully autonomous weapons function in an ethically “correct” manner?
- Are machines capable of acting in accordance to international humanitarian law (IHL) or international human rights law (IHRL)?
- Are these weapon systems able to differentiate between combatants on the one side and defenseless and/or uninvolved persons (noncombatants)?
- Can such systems evaluate the proportionality of attacks?
- Who can be held accountable?<sup>v</sup>

But instead of answering each question, countries interested in implementing or developing LAWS into Defense plans should consider if they are acting in accordance with international humanitarian law. The International Committee of the Red Cross (ICRC) has raised concern on lethal autonomous weapon systems since 2011, arguing that there are no regulations to assess potential risks around how these new technologies will be used, as well as a lack of standards and methodologies. In 2014, the ICRC facilitated a discussion among 21 countries and only two - the U.S. and the United Kingdom - have implemented national policies on lethal autonomous weapon systems. The U.S. policy states “autonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force,”<sup>vi</sup> and the UK policy states that autonomous weapons will not be permitted and should be under human supervision. Even though these are only two countries, there is still agreement on how to deploy autonomous weapons. Yet, the ICRC does not have a clear definition for LAWS, so this author is assuming that the disagreement amongst other countries is due in part to the lack of clarification on terminology.

The ICRC has raised several talking points on which countries should think about when they implement

autonomous weapon systems and the talking points are as follow:

- Civilian robotics and developments in autonomous systems
- Military robotics and drivers for development of autonomous weapon systems
- Autonomy in existing weapon systems
- Research and development of new autonomous weapon systems
- Military utility of autonomous weapon systems in armed conflict
- Current policy on autonomous weapon systems
- Autonomous weapon systems under international humanitarian law
- Accountability for use of autonomous weapon systems
- Ethical issues raised by autonomous weapon systems

These are great points to start a discussion but if the ICRC or any international governing body does not enforce any of them, then autonomous weapons systems will be developed without the accordance of IHL and these systems will become unlawful and illegal.

In conclusion, ethical problems can lead to endless discussions but they should not be left unattended. If ethical problems are being considered, the outcomes of discussions can be closer to resolving social problems. At this time, the ethical questions identified by the research community and the concerns of the ICRC are very valid. However, these kinds of weapon and defense systems are an extension of the armed forces and they should still funded, but they must monitored very closely to adhere to international humanitarian laws. The U.S., as a military power house and as one the leading researching countries, should lead the way for a more regulated implementation and development of programs of lethal autonomous weapons. While every country wants to earn the edge in terms of military power, this kind of technology can lead to another kind of war.

---

<sup>i</sup> *Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. Department of Homeland Security, U.S. Department of Defense. May 2010. Accessed 1 Jun. 2015 <[www.dhs.gov](http://www.dhs.gov)>.

<sup>ii</sup> Moeller, Robert R. *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (CRC) Processes*. Hoboken, New Jersey: John Wiley & Sons. 2011.

<sup>iii</sup> Girling, P. (2013). *Operational Risk Management A complete Guide to a Successful Operational Risk Framework*. Hoboken, New Jersey: Wiley & Sons.

<sup>iv</sup> Russell, Stuart. "Ethics of Artificial Intelligence." *Nature*. 27 May 2015. Accessed Jun. 2015 <[www.nature.com](http://www.nature.com)>.

<sup>v</sup> Acheson, Ray and Beatrice Fihn. *Fully Autonomous Weapons*. Jul. 2013. Accessed Jun. 2015 <[www.reachingcriticalwill.org](http://www.reachingcriticalwill.org)>.

<sup>vi</sup> "Report of The ICRC Expert Meeting On 'Autonomous Weapon Systems: Technical, Military, Legal And Humanitarian Aspects.'" International Committee of the Red Cross. 9 May 2014. Accessed Jun. 2015 <[www.icrc.org](http://www.icrc.org)>.