Horizon Scanning Series

The Effective and Ethical Development of Artificial Intelligence: An Opportunity to Improve Our Wellbeing

Defence, Security and Emergency Response

This input paper was prepared by Adam Henschke

Suggested Citation

Henschke, A (2018). Defence, Security and emergency Responses. Input paper for the Horizon Scanning Project "The Effective and Ethical Development of Artificial Intelligence: An Opportunity to Improve Our Wellbeing" on behalf of the Australian Council of Learned Academies, www.acola.org.

The views and opinions expressed in this report are those of the author and do not necessarily reflect the opinions of ACOLA.

Prior to any discussion of the application of drones[1] and artificial intelligence (AI), there are a number of different applications of drones, different roles that AI plays in drones, and different roles of humans in the activities of drones. While these differences and distinctions play a larger role across human society, the discussion here will be focussed on drones and AI in a context of military use and/or national security more broadly construed.

The first point to recognise is that drones whether air (Strawser, 2013), land (Singer, 2009), sea (Lucas Jnr, 2015) or space are used by militaries and others in a huge range of ways. The most common public discussion about drones has been their use in support of military and covert actions for targeted killing/assassinations, this application is by far in the minority of uses. A significant proportion of drone activities, even when constrained military operations, is for surveillance and information gathering. However, there are other applications, such as part of bomb/munitions disposal units (Singer, 2009). This is an important point to draw out at the beginning, as the ethical legal and social concerns with drone use vary depending on whether they are being used to kill targets, gather information, support individuals etc.

The second point to recognise is that AI plays a range of different roles on these drones. Again, one of the most common areas of public discussions cover that of Lethal Autonomous Weapon Systems (LAW). These are typically drones that operate independently of a human operator, and as part of those operations, 'make decisions' that lead to the application of lethal force. Again, however, there are many other operations that AI is involved in. AI targeting, for instance, can refer to identification of a human target for lethal force. However, the decision to use lethal force may remain that of a human operator. Similarly, AI targeting might instead be used to identify the target of surveillance through facial recognition, in an operation that is not a direct part of lethal force. In all three instances, the AI is used in targeting, thought what that targeting means varies. Further, AI is frequently used in drones for the processes of take-off/flight/return. In this sense, some part of the operation (navigating through a communications denied environment for instance, (Lucas Jnr, 2015)) is run by the AI, while other parts of the operation remain entirely in the control of human operators.

Finally, the explicit functional role of humans must be explicated. As the multiplicity of meanings for 'targeting' shows, humans can play range of roles in a drone's operation. These roles are frequently parsed out the human operator being 'in the loop', 'on the loop' or 'out of the loop', described by Human Rights Watch as:

- Human-*in*-the-Loop Weapons: Robots that can select targets and deliver force only with a human command;
- Human-on-the-Loop Weapons: Robots that can select targets and deliver force under the oversight of a human operator who can override the robots' actions; and
- Human-out-of-the-Loop Weapons: Robots that are capable of selecting targets and delivering force without any human input or interaction (Human Rights Watch, 2012)

It is this final version that people may think of when considering AI and drones. "The crux of full autonomy, therefore, is the capability to identify, target, and attack a person or object without human interface. Although a human operator may retain the ability to take control of the system, it is capable of operating on its own" (Schmitt & Thurnher, 2013). However, especially when thinking of drones, AI and lethal force, such 'out of the loop' operations are in the extreme minority. Certain border regions

[1] There are a range of different terms in use in the literature, including drones, remote devices, unmanned vehicles, etc. For the purposes of ease of reading, I will simply refer to the whole cluster of related technologies as 'drones'. Where the decisions relate to weapons used as part of a lethal decision, the acronym LAWS, an abbreviation of 'Lethal Autonomous Weapons System' will be used.

in Israel, for example, have armed weapons systems that will shoot to kill (Singer, 2009), but even with these, it is highly contestable if they qualify as AI proper.

1. In an age of LAWS, what role can Australia play to limit the technological outsourcing of killing to machines?

Australia's role here is most likely limited to international dialogue, discussion and norms promotion. Compared to countries that lead the world in weapons production, our outputs are very limited and so we would be unlikely to have any significant impact on LAWS though technological leadership or innovation. Similarly, the AI world is dominated by China, and to a lesser extent the US. Again, given Australia's paucity in terms of technological leadership or innovation here, any impact we have is likely to be negligible. Should Australia want to become a more active player in a technological context, we have to significantly increase our funding for research by several orders of magnitude.

Where we can have an impact on LAWS, is to use our role and voice at various international dialogues and discussions to promote norms. For instance, Australia has been active in discussions at the United Nations as part of the discussions around the Convention on Certain Conventional Weapons (for more on the CCW), in which drones and LAWS have been a recent point of debate. See: https://www.unog.ch/80256EE600585943/(httpPages)/4F0DEF093B4860B4C1257180004B1B30?OpenDocument. A parallel opportunity for influence at this international level is for Australia to commit funding to the United Nations Institute on Disarmament Research (UNIDR), one of the research arms of the UN that has been closely exploring and shaping debates about LAWS.[2]

Another opportunity for leadership exists for Australia using its international diplomatic capacity for norms promotion. For instance, Australia could vocally support the norm that commanders are held culpable for decisions involving AI that contravene international humanitarian law (IHL). In the early discussions of ethics and drones, a number of philosophers identified what they saw as the risk of a moral gap in AI conducts lethal targeting with humans out of the loop (Enemark, 2013). While there may be some 'moral' gap here (Roff, 2013), military command structures will identify and hold a commander responsible for a decision, regardless of whether the ensuing operations involved a subordinate actor or AI: Should the command decision result in the death of an innocent person and thus a violation of the laws of armed conflict, on a standard legalistic account, the command structures within the military are such that the commander will be *held* responsible. So, though there may be a moral responsibility gap, there seems to be no legal responsibility gap. Insofar as Australia considers its role as ensuring that LAWS are used responsibly, it could pursue this leadership role by advocating for and ensuring that the command responsibility is applied to decisions regarding the deployment of drones, particularly if/when they are being used as LAWS.

2. What high-consequence risks arise from innovations in "parasite UAVs" (MicroBat, SLADF, Black Widow) and the advent of miniaturized, semi-autonomous weapons systems?

Given their small size, they are unlikely to be used as weapons delivery systems, and are likely to have very limited operational range or flight time – though the operational range and battery life is constantly shifting as the technology develops. However, parasite drones (drones that are deployed from larger vehicles) and micro/nanodrones gain their utility from their small size, and this small size means that there will always be practical limitations on what they can do. Given these practical limitations, parasite drones and other micro/nanodrones are most likely going to primarily be of use in information gathering, so for intelligence purpose. The AI will likely be involved in coordinating the flight to the designated target (and perhaps in return from the target), in the recognition of targets/hindrances and in analysis of the data that is gathered.

[2] For more on UNIDIR see: http://www.unidir.org/

Drawing from the opening points, this points to another crucial distinction between AI that *informs decision making* versus AI that *makes decisions*. For the purposes of this submission, I am going to use 'decision' to simply mean some input weighting process that results in a change in the world. This is explicitly tailored to be inclusive of something like AI, as well as the ways that human beliefs and desires act as input weighting decisions that lead to actions.[3] It also fits with a "minimal definition of autonomy vis-à-vis a weapon or weapon system [that is] capable of some significant operation without direct human oversight" (Sparrow, 2016). On this, a drone used for surveillance purposes is ostensibly being used to gather information to *make a decision*, it is specifically an intelligence process that is being used to improve decision making (Omand, 2010). In contrast, a drone that drops a bomb following an AI targeting decision with a human on or out of the loop is *making the decision*. Parasite and micro/nanodrones are likely to have AI that *makes decisions* around flight paths etc., while the main purpose is information gathering. That is, the AI in parasite and micro/nanodrones are largely going to be constrained to *AI that informs decision making*.

This distinction is important as the moral risks of fully autonomous LAWS, with no humans in the loop are significantly different from the risks of an AI parasite drone that is gathering intelligence. However, this does not mean that the parasite and micro/nanodrones are without ethical risk. There are moral concerns about invasion of individual privacy. This is particularly obvious if such surveillance drones are used in a policing/national security context (Henschke, 2017a). However, note that if privacy is a human right, the right to privacy extends to the wartime context too, so privacy is still an issue even in war.

Second, the way the information gathered is presented to operators impacts their decision making (Henschke, 2017a; G. Smith, 2015). That the means and modes communication of information to operators has ethical relevance is an old issue in ethics of technology (Davis, 1991). In this instance, the moral concern is that the operators accept the AI suggestion that the person identified is in fact the correct person to be targeted for follow up actions. Though the AI identification of someone makes them a person of interest our operators are not automatons. It is their *job* is to assess the situation. The AI is simply indicating that a situation needs to be assessed. While this may be true, it does not always represent the reality of how people make decisions. Following Daniel Kahneman's descriptions of cognitive biases and mental effort (Kahneman, 2011), when we're tired, when our cognitive processes are "drawn down", we are more likely to accept an argument *as it is presented*. That is, our capacity to respond to and *challenge defaults* is in part dependent on our state of mind. Stress, tiredness, boredom can play a big role in how effective an operator is at challenging or simply accepting the default settings. Following Kahneman, having had the AI identify an individual as a target, it is now up to the operator to *reject* the suggestion that the target of the surveillance is worthy of suspicion. However, their capacity to reject this is dependent on factors like tiredness, stress, how many other tasks they have running at the time. Given that AI that informs decision making is part of a larger surveillance socio-technical superstructure, any discussion of their application touches on larger issues around surveillance and governance (Henschke, 2017a; Lyon, 1994, 2009).

3. How can AI improve the way the military operates in next decade?

The three main areas where I expect AI to improve military operations are information handling, in the outsourcing of non-mission critical decisions and in cyberspace. On the first issue, one the key challenges that militaries and national security institutions more generally have been facing for at least

[3] This description of decision making is unlikely to satisfy all people. Like AI, the very notion of 'decision making' is conceptually complex and highly contested. First, we need to ask what a decision is. For more on this see https://plato.stanford.edu/entries/decision-theory/. Second, we need to question what the capacity for decision *making* is. For more on this, see: https://plato.stanford.edu/entries/decision-capacity/. Finally, I am sure that many would see my description as too inclusive, as it something about causal activity with causal agency. This may be true, however, if drones, LAWS or any AI does not make something at least functionally equivalent to a decision, then there is no point talking about drones, LAWS or AI at all, as any sensible discussion would remain focussed to humans. And if this is the case, then there should be no need for this report at all.

the last two decades is that operators and institutions are drowning in information. That is, they already have too much information and are unable to use what they have effectively. Parallel to this is the need to make information gathered from multiple sources usable across departments/institutions. One of the recommendations of the 9/11 Commission Report was that the US intelligence agencies needed to make the better use of the information they had on potential terrorists (National Commission On Terrorist Attacks Upon The United States, 2004). In the intervening years, the power of information technologies has increased, and so too have the claims about what these information technologies can do to identify the perpetrators of mass violence before such events occur. Some propose that security agencies could analyse their existing intelligence to predict terrorist attacks (Woollacot, 2015). Others are doing "research on support tools and methods that help law enforcement officers in ongoing investigations of web extremism…[to develop] techniques that can be used to detect indicators supporting that someone has intent to commit a terror attack" (Brynielsson et al., 2013). Following the shooting at Stoneman Douglas High School in Florida in February 2018, US President Trump criticised the Federal Bureau of Investigations for not using social media posts by the shooter to prevent the tragedy (Graham, 2018). Whether it is strictly within the military context or a more general national context, there is a push for those institutions to use the information that they have. And for this AI is likely to play the key role.

As touched on above, just because these process do not directly involve AI making decisions, these information heavy process that inform decision making have significant ethical aspects. Elsewhere, I expanded on these ethical aspects to include a taxonomy of risks based on informational harms:

- Harm, Broad Micro-: Where a certain group is limited in their opportunities by the constant and persistent use of information
- Harm, Broad Standard: Where a certain group are limited in their opportunities by the constant and persistent use of information
- Harm, Closed Identity: Where devalued Virtual Identities negatively impact the target person's identity development
- Harm, Deliberate Informational: When people use personal information to deliberately harm others
- Harm, Incomplete Informational: When information is decontextualised and the loss of the intended meaning results in harm to a person
- Harm, Limited Opportunity: When a specific set of information is used to limit the range of opportunity that an individual might have
- Harm, Narrow Micro-Harm: Where an individual is limited in their opportunities by the constant and persistent use of information
- Harm, Narrow Standard: Where an individual is limited in their opportunities by the constant and persistent use of information
- Harm, Negligent Informational: When information is constructed that targets an individual or group, but the data is not accurate, resulting in harm to a person (Henschke, 2017a).

A second area where AI is likely to play a significant role for the military is in the outsourcing non-mission critical decisions and/or non-morally relevant decisions. For instance, the use of AI for logistics and resource distribution, coupled with the use of AI for driverless vehicles in non-mission critical contexts etc. That is, AI is likely to play an increasing role in decisions around military practices

that are neither mission critical or those involved in the actual application or use of force. As discussed above, the command structures of militaries are likely to ensure that mission critical decisions and those around the use of lethal force are likely to remain within the realm of humans.

The third general area concerns AI and cyberspace. While cyberspace covers the collection and application of information, and logistics etc., given that cyberspace is simply playing a larger role in all levels of human activity, it is a fact that this is true for militaries as well. One of the key areas where AI is likely to play a more active role in cyber involves the speed at which cyberattacks can occur. In certain attacks, it is possible that AI may be needed to respond as the attacks may be faster than a human can respond to. So, in addition to the use of AI to identify and categorize an informational event as a cyberattack (or not), AI's capacity to respond in time to prevent/minimise harms make cyberspace/cyberdefence etc. a further area of AI/military application.

4. What are the challenges AI brings to military's traditional procurement cycle and how can we increase adoption of new technologies like AI?

No idea.

5. If AI is to be developed, or at least specialised in Australia and New Zealand, what are the requirements with respect to the need for experts to handle the software systems?

The basic requirements here are that Australia and New Zealand need people who know the AI systems and applications. That experts are needed for AI etc. is a banally obvious claim. Where Australia and New Zealand can play an interesting and perhaps pivotal role is in pursuing and supporting cross disciplinary expertise. That is, technologies like AI are used in a human context so any development and effective applications need to be well aware that these developments and specialisations are only going to be maximally utilised if those around them understand what's happening on technical and human/social levels. That is, the experts with the technical expertise require training and education in the human/social applications and implications of their research. Likewise, lawyers, ethicists, policy makers, psychologists etc. need to interact with and work with the technical specialists. In short, there is a dearth of active research support for science and technology studies in Australia and New Zealand, and if we want to be future leading, we need to significantly lift these areas of study at both the research and education levels.

6. What are the implications for defence procurement, to ensure that any hardware comes with the knowledge around the specific AI software?

One of the main implications of AI is that it creates 'black boxes' in decision making processes, it is opaque. This opacity comes in at least three sorts – technical opacity, legal opacity and actual opacity. On technical opacity, this is simply the ignorance that one person has in relation to how a given AI 'tool' works. If I am to purchase a drone that relies on AI to target terrorists for use in Australian cities, for example, but I have no idea how that drone targets the terrorists, then we have a technical opacity.

On legal opacity, many of these technical products have their processes opaque as a matter of law operate with proprietary software. For instance, the software program Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is in use in the US determine if an offender is at high risk of committing new crimes. The software's proponents claim the success of such approaches. COMPAS would allow law enforcement officers to:

> quickly screen an offender's risk level at the point of arrest, with subsequent decisions about community release, pretrial diversion, sentencing, and probation supervision further guided by COMPAS to assess the existence of criminogenic factors and how best to address them at every step… For example, research supports that if practitioners use an empirically based assessment tool (i.e. COMPAS) they will be more accurate in their prediction of the risk of an

individual's propensity to commit a crime in the future than their professional judgment alone. The evidence based practice is the use a of risk/needs tool to determine the appropriate amount of intervention, rather than the use of professional judgment alone (Equivant, 2017).

These products rely on proprietary software: "The key to our product is the algorithms, and they're proprietary… We've created them, and we don't release them because it's certainly a core piece of our business" (COMPAS executive, quoted in Liptak, 2017). Insofar as this software is proprietary, the process of decision-making is opaque. This is a concern: in order for us to be sure *that* justice is being done, we need to know *how* justice is being done. Closing the decision-making elements off from scrutiny can prevent us from knowing just how the decisions were made.

Finally, certain AI process are 'actually' opaque. Rather than the lack of understanding deriving from technical ignorance or legal constrain, once certain AI processes meet a given level of complexity, even those with expertise in machine learning are unable to explain how a certain decision was attained. Though the general way that machine learning functions might be known, certain of these decisions are inscrutable. Essentially, there is no audit trail that specifies exactly how a sufficiently complex AI decision process made a particular decision or led to a particular outcome. These three forms of opacity are all relevant in that if the procurement process requires that certain decisions arising from the application of a given AI product require scrutability/explicability – any of these forms of opacity should prevent purchase.

A parallel concern for military and national security procurement is in supply chain and informational integrity. A key cybersecurity vulnerability for military and national security agencies is if the security of communications of devices they use can be ensured and assured. This becomes increasingly important where the military etc. are using third party vendors to provide products from states whose strategic interests either do not align or are in direct conflict with Australia and New Zealand. AI complicates things as any of the three forms of opacity may present information security vulnerabilities. That is, any device that uses AI in an area where there is need for information security, if there is technical, legal or actual opacity, the procurement process will require an awareness of any of these opacities and a well-=reasoned judgment that the given opacity cannot and will not lead to information security issues in the future.

7. What are the implications of AI for "counter-terrorism-AI", "cyber war fare" and "network centric warfare"?

The following is a list of the main likely uses of AI in these contexts:

- Use of AI in flagging 'abnormal' or 'antisocial behaviour' etc. See Gavin Smith more on this (G. Smith, 2015).
- Use of AI for facial recognition. See Microsoft for more on this (B. Smith, 2018)
- Use of AI take down/remove illegal and/or offensive material online. See Twitter for more on this (Breland, 2018; Leetaru, 2018)
- Use of AI to recognise foreign influence operations. See Muller for more on this (Mueller, 2018)
- Use of AI in a context of criminal law for sophisticated spearphishing

A final comment is on the Internet of Things. "[T]he core concept is that everyday objects can be equipped with identifying, sensing, networking and processing capabilities that will *allow them to communicate* with one another and with other devices and services over the Internet *to achieve some useful objective* (Emphases Mine Whitmore, Agarwal, & Da Xu, 2015, p. p. 261). Rather than human to human communication, the IoT builds from the simple notion of objects in our world being able to

communicate with each other. “In fact, it is this ability for objects to communicate that delivers the power of the IoT” (Fletcher, 2015, p. p. 20). Moreover, this is not simply producing and collecting information for the sake of it – it is *to achieve some useful objective*. Whether it is simply about logistics or controlling your house, the IoT derives its importance from the fact that the information produced by the communicating objects is intended to bring about some change in the physical world. The size of the IoT is expected to be immense – by 2020, 20 – 50 billon things are estimated to be connected as part of the IoT (Mohammed, 2015), leading some to predict an investment of 1.7 trillion dollars US by 2020 (International Data Corporation, 2015). Common elements to the IoT are sensors (Li, Xu, & Zhao, 2015), informational processors (Agarwal & Dey, 2016; Whitmore, et al., 2015) and actuators (Stankovic, 2014) – some way of bringing about physical change. For more on ethics and the IoT see (Henschke, 2017b).

The IoT is relevant to both AI and cyberterrorism and cyberwar. To date, there has been no real cyberterrorism (Droogan & Waldek, 2016) or cyberwar (Rid, 2013). To be clear, terrorist use the internet and militaries engage in offensive cyberactivies. But do date, cyberspace has either been a vector for some other behaviour or the direct military impacts have been largely limited to cyberspace. AI changes this in that the coordination needed to achieve the promises of the IoT will likely require AI. The actuators in the IoT means the virtual becomes physical. This capacity to use/exploit cyberspace to bring about physical impacts means actual cyberterrorism will become likely if not certain. Similarly, the IoT means that actual cyberwar will become more likely, where contra Thomas Rid, militaries use cyberspace to bring about significant physical destruction.

Agarwal, Y., & Dey, A. (2016). Toward Building A Safe, Secure, And Easy-To-Use Internet Of Things Infrastructure. *IEEE Computer 2016: IEEE Computer Society, April*, 40 - 43.

Breland, A. (2018). Week ahead: Tech giants to testify on extremist content. Retrieved 17 Jan http://thehill.com/business-a-lobbying/368775-week-ahead-in-tech-youtube-twitter-and-facebook-to-face-senate-commerce

Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C., & Svenson, P. (2013). Harvesting And Analysis Of Weak Signals For Detecting Lone Wolf Terrorists. [journal article]. *Security Informatics, 2*(1), 11. doi: 10.1186/2190-8532-2-11

Davis, M. (1991). Thinking Like An Engineer: The Place Of A Code Of Ethics In The Practice Of A Profession. *Philosophy And Public Affairs, 20*(2), 150-167.

Droogan, J., & Waldek, L. (2016, 2-4 Aug. 2016). *Where Are All The Cyber Terrorists? From Waiting For Cyber Attack To Understanding Audiences.* Paper presented at the 2016 Cybersecurity and Cyberforensics Conference (CCC).

Enemark, C. (2013). *Armed Drones And The Ethics Of War: Military Virtue In A Post-Heroic Age*: Routledge.

Equivant. (2017). Enhancing Public Safety Through Community Collaboration, Coordinated Leadership, And Innovative Criminal Justice Programs Retrieved 25 October, 2017, from http://www.equivant.com/assets/downloads/EauClaireCounty_final_resources.pdf

Fletcher, D. (2015). Internet Of Things. In M. Blowers (Ed.), *Evolution Of Cyber Technologies And Operations to 2035* (pp. 19-32). Dordrecht: Springer.

Graham, C. (2018, 18 February). Florida Shooting: Donald Trump Blames FBI's Russia Probe For Failure To Spot Suspect's Warning Signs, *Telegraph*. Retrieved from https://www.telegraph.co.uk/news/2018/02/18/florida-shooting-donald-trump-blames-fbis-russia-probe-failure/

Henschke, A. (2017a). *Ethics In An Age Of Surveillance: Virtual Identities And Personal Information*. New York: Cambridge University Press.

Henschke, A. (2017b). The Internet Of Things And Dual Layers Of Ethical Concern.

In P. Lin, K. Abney & R. jenkins (Eds.), *Robot Ethics* (Vol. 2). Oxford: Oxford University Press.

Human Rights Watch. (2012). Losing Humanity: The Case Against Killer Robots Human Rights Watch.

International Data Corporation. (2015). Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020, According to IDC

Kahneman, D. (2011). *Thinking, Fast And Slow*. New York: FSG.

Leetaru, K. (2018, January 12). Is Twitter Really Censoring Free Speech?, *Forbes*. Retrieved from https://www.forbes.com/sites/kalevleetaru/2018/01/12/is-twitter-really-censoring-free-speech/#3b3416ea65f5

Li, S., Xu, L. D., & Zhao, S. (2015). The Internet Of Things: A Survey. *Information Systems Frontiers, 17*(2), 243-259. doi: 10.1007/s10796-014-9492-7

Liptak, A. (2017, May 1). Sent To Prison By A Software Program's Secret Algorithms, *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html

Lucas Jnr, G. R. (2015). The Weaponization Of Increasingly Autonomous Technologies In The Maritime Environment: Testing The Waters. Geneva: United Nations Institute for Disarmament Research.

Lyon, D. (1994). *The Electronic Eye: The Rise Of Surveillance Society*: University Of Minnesota Press.

Lyon, D. (2009). Surveillance, Power, And Everyday Life. In C. Avgerou, R. Mansell, D. Quah & R. Silverstone (Eds.), *The Oxford Handbook Of Information And Communication Technologies*: Oxford University Press.

Mohammed, J. (2015). 5 Predictions For The Internet Of Things in 2016 Retrieved 20 May, 2016, from https://www.weforum.org/agenda/2015/12/5-predictions-for-the-internet-of-things-in-2016/

Mueller, R. S. (2018). *United States Of America V. Internet Research Agency*. (Case 1:18-cr-00032-DLF). District Of Columbia.

National Commission On Terrorist Attacks Upon The United States. (2004). *The 9/11 Commission Report: Final Report Of The National Commission On Terrorist Attacks Upon The United States*. Washington DC: US Government.

Omand, D. (2010). *Securing The State*: Oxford University Press.

Rid, T. (2013). *Cyber War Will Not Take Place*: Hurst & Company.

Roff, H. M. (2013). Killing In War: Responsibility, Liability, And Lethal Autonomous Robots. In F. Allhoff, N. G. Evans & A. Henschke (Eds.), *Routledge Handbook Of Ethics And War: Just War In The 21st Century*: Routledge.

Schmitt, m. M. N., & Thurnher, J. S. (2013). "Out Of The Loop": Autonomous Weapon Systems And The Law Of Armed Conflict. *Harvard Law School National Security Journal, 4*.

Singer, P. W. (2009). *Wired For War*. New York: Penguin.

Smith, B. (2018, 13 July). Facial Recognition Technology: The Need For Public Regulation And Corporate Responsibility. Retrieved from https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

Smith, G. (2015). *Opening The Black Box: The Work Of Watching*: Routledge.

Sparrow, R. (2016). Robots And Respect: Assessing The Case Against Autonomous Weapon Systems. *Ethics And International Affairs, 30*(1), 93 - 116.

Stankovic, J. A. (2014). Research Directions For The Internet Of Things. *IEEE Internet of Things Journal, 1*(1), 3-9. doi: 10.1109/JIOT.2014.2312291

Strawser, B. J. (Ed.). (2013). *Killing By Remote Control: The Ethics Of An Unmanned Military*: Oxford University Press.

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet Of Things—A Survey Of Topics And Trends. *Information Systems Frontiers, 17*(2), 261-274.

Woollacot, E. (2015, 24 September). The Algorithm That Can Predict Isis's Next Move – Before They Even Know What It Is. *New Statesman*.