Multinational Capability Development Campaign (MCDC) 2013-2014

Focus Area "Role of Autonomous Systems in Gaining Operational Access"

Policy Guidance
Autonomy in Defence Systems

29 October 2014


MCDC
2013 - 2014
Combined Operational Access

Multinational Capability Development Campaign (MCDC) 2013-2014

Focus Area "Role of Autonomous Systems in Gaining Operational Access"

Policy Guidance
Autonomy in Defence Systems

Supreme Allied Commander Transformation HQ, Norfolk, United States

29 October 2014

PARTICIPANTS & ROLES:

Focus Area Project Lead: NATO Allied Command Transformation
Contributing Nations/Organizations: Austria, Czech Republic, Finland, Poland, Switzerland, United Kingdom and United States
Observers: Germany, European Union, The Netherlands, Sweden
The Netherlands formally joined this project as an observer but also made a substantial contribution.

Authors of this publication are represented by: LtCol Artur Kuptel, MCDC NATO-ACT National Director and Mr Andrew Williams, MCDC NATO-ACT Lead Analyst

Preface

This document is a final product from the Autonomous Systems focus area, led by NATO Headquarters Supreme Allied Commander Transformation (HQ SACT), and conducted under the auspices of the Multinational Capability Development Campaign (MCDC) 2013-14—a collaborative programme between 19 nations, NATO and the European Union. The Autonomous Systems project team adopted a guiding problem statement for the project: "Coalitions need to improve awareness and understanding of autonomous systems, promote interoperability and provide guidance for the development of, use of, and defence against, autonomous systems.

The project conducted five studies: a definitional study led by HQ SACT focusing on the meaning of autonomy; a legal study led by Switzerland, which examined legal issues mainly concerning weapon systems with autonomous capability; a human factors and ethical study co–led by the United States and HQ SACT, which explored future ethical, organisational and psychological implications; a military operations study led by HQ SACT, describing operational benefits and challenges, and lastly; a technology study led by the Czech Republic, which summarised key technological developments and challenges. These study findings and records from the various workshops and seminars are published separately in an MCDC Autonomous Systems Proceedings report, available from the MCDC Secretariat *MCDC_Secretariat@apan.org*.

Drawing from the findings of the MCDC Autonomous Systems focus area work, this document offers policy guidance to senior leadership in government defence organisations, industry, and academia. The guidance aims to facilitate planning and preparation for the design, procurement and operation of systems with autonomous capabilities, and to realise the impressive benefits while avoiding potential challenges. This guidance takes a broader, strategic view of the MCDC Autonomous Systems project findings and covers the implications of the definitions for autonomous systems; key legal issues regarding weaponized systems with autonomous capability; ethical, human factors and military concerns; and gives guidance for future research and capability development.

This document was developed and written by the contributing nations and organisations of MCDC. It does not necessarily reflect the views or opinions of any single nation or organisation but is intended as a guide and an exploration of the subject. For the purposes of clarity source citations have been omitted; readers may refer to the full MCDC Autonomous Systems Project Proceedings report for an extensive list of references.

Contents

Introduction

We are on the verge of a technology revolution in the military environment. Driven partly by the need to manage reduced resources and lessen the danger to personnel, but also to increase military and technological advantages over adversaries, military forces are considering new autonomous technologies to support and augment human capabilities in all domains of operation.

Autonomy refers to the extent to which a system, platform, or specific functions, are capable of operating with varying levels of oversight by a human controller. Autonomy is enabled by computing functions, which interact with the operational environment and involve a variety of higher level information processing such as learning, categorisation, concept formation, decision making, or problem solving. An ability to function autonomously allows systems to reach their goals in unpredictable and unstructured environments. In contrast, automatic functioning requires fixed inputs, rules, and defined outputs. An important consideration for the design and operation of systems with autonomous capability is the **level of human control** in the system. In the military context it is important that autonomy occurs with oversight—"autonomy under human control".

The prevalence of systems with autonomous capabilities is growing in the military sphere; such systems will likely become a permanent feature of military operations and will be adopted by adversary forces. Nonstate groups are likely to seek to acquire this technology, given its expected prevalence in the civilian domain and relatively low cost. There are wide ranging implications on the whole spectrum of military operations and capabilities. For these reasons, the role of autonomy is one of the most important considerations for defence policy makers in the near future.

Many nations have military research and development programs that are increasing the extent of autonomous functions in military systems; a growing civilian sector is also evident, such as recent high-profile "autonomous car" initiatives. Autonomous technology allows unmanned ground, sea or air platforms to perform navigation, situation awareness, and diagnostic functions without reliance on regular control communications. In manned platforms, autonomous functions can be used to independently select and prioritise information, to reduce the burden on operators.

Increasing the autonomy in systems has the potential to confer a range of benefits: higher levels of readiness; faster execution of tasks; higher interoperability between systems; lower error rates; increasing coordination and synchronisation with other platforms; and the increasing use of unmanned platforms, which decreases risk to life and improves operational access. Depending on the particular system and operational use, autonomous functions can either remove the requirement for a human to be physically present on a platform for control

purposes, or augment and compliment human capability to control and operate machines and also assist in decision making.

These benefits, however, are coupled with complex legal and ethical concerns, and many systems design and technical challenges. Increasing autonomy in military systems is likely to have wide-ranging implications and risks, requiring changes in the nature of planning and conduct of operations, organisational structures, command and control, and personnel training and skill sets. An effective, appropriate, and acceptable use of autonomous functions in military systems will depend on anticipation of human impacts and consideration of their effects in the design, development, and procurement of such systems, and the planning and ordering of their deployment. This policy guidance document discusses these issues and risks in more detail.

Purpose

This policy guidance document achieves two objectives.

Raise awareness. First, the policy guidance raises awareness of the importance of autonomy in future defence capabilities, and its potential employment by adversaries. Greater awareness is also required for informed dialogue in national and international policy arenas, especially given the related on-going debates involving potentially ambiguous terminology such as "killer robots."

Explore key issues and risks. Second, drawing from detailed studies, workshops and seminars conducted during the MCDC project work, the policy guidance presents key issues and risks. It then makes recommendations in the areas of definitions, military operational benefits, legal and ethical challenges, public awareness, human factors, organisations, and future capability development. This guidance represents a framework for thinking about the constellation of issues surrounding systems with autonomous capabilities.

Scope

The policy guidance applies to air, land, and maritime domains, although the findings and recommendations are presented in an integrated manner that is not specific to any one domain. The importance of space and cyber domains are recognised, but are not covered.

Primarily, this policy guidance focuses on issues related to the increasing autonomy in military systems that should be addressed within the next five years. This allows policy makers to plan and be prepared for the major implications deriving from the increasing employment of autonomy. Many of the issues identified, however, anticipate long term factors that will only become a reality in coming decades. Given the broad focus of this document, more detailed follow-on studies in the area of autonomous systems are recommended for the next MCDC cycle.

Current policy landscape

While many nations have issued research and development plans concerning unmanned system development and recognised the importance of autonomous technology, few nations have explicitly addressed the issue. The role of autonomy is typically considered in the context of already established national processes of legal reviews and regulations, policy guidance, and capability development procedures.

At the time of this document's publication in October 2014, the United States is the predominate nation in terms of publicly available policy governing autonomous functions in defence systems. The United States' policy on autonomy in weapon systems, for example, is specified in Department of Defense Directive 3000.09 of November 2012. It covers manned and unmanned platforms, as well as guided munitions, but excludes mines, cyber weapons, and manually guided munitions. The policy establishes guidelines to minimise the probability and consequences of failures in autonomous and semi-autonomous weapon systems that could lead to unintended engagements.

Autonomous technology, especially in weapons systems, has been the agenda of several major international policy events. For example, expert groups were convened to discuss policy and governance issues at the United Kingdom's Chatham House think tank in February 2014, and the International Committee of the Red Cross in Geneva, in March 2014. Significantly, the 117 States party to the United Nations Convention on Certain Conventional Weapons (UN CCW) held an unprecedented Meeting of Experts in May 2014 specifically addressing the subject of “lethal autonomous weapons,” and agreed to hold a formal session in November of 2014. In part, this initiative was stimulated by activities of various nongovernmental advocacy groups such as the International Committee for Robot Arms Control, and several high profile reports from organisations such as Human Rights Watch.

In the civilian domain, intergovernmental organisations, nations, and regions are developing rules, guidance and legislation to regulate the introduction of new autonomous transport technology. Several states in the United States, for example, have introduced legislation governing autonomous road vehicles, and the European Union is considering airspace management regulations to deal with the growth of unmanned air systems and their increasingly autonomous nature.

This is not an exhaustive list and the policy landscape is evolving quickly; however, defence policy makers should be aware that this is a subject of growing international importance and debate.

Policy Recommendations

Definitions

When new concepts and ideas are introduced definitions become vitally important. Shared definitions allow meaningful and informed discussion and debate about issues and support standardisation measures and collaborative development. This section addresses the issue that autonomy is both a difficult concept to understand and is used inconsistently and inappropriately in current policy discussions.

Understanding the meaning of "autonomy" is challenging

Autonomy literally means "self-governing." In the context of defence systems, the term is typically used to describe how machines perform certain functions—to varying extents—independently of human control. While attempts have been made to create schemas describing the "level" of autonomy of a machine, and to distinguish "autonomous" from "automatic" or other terms, there is currently no consensus. The definitional challenge is further complicated by the fact that an understanding of autonomous functioning depends on precursor and related concepts such as artificial intelligence and decision-making algorithms.

For the purposes of this discussion, true autonomy should be considered as an intrinsic property of sentient and intelligent creatures. Machines, therefore, are not autonomous in a literal sense, but may exhibit "autonomous-like" functions, relative to a particular level of human control and situational context. Labelling a function as autonomous implies a certain level of ability to adapt to complex or unanticipated situations, which is different from an automatic function occurring according to defined inputs, rule sets and outputs.

The danger of using "autonomous" to describe machine characteristics

When human concepts such as autonomy, intelligence or emotion are used as qualifiers for machines—autonomous robot; intelligent platform etc.—there is potential for several points of confusion.

First, the literal meaning of "autonomy" simply may not be understood. Certainly in the defence sector, evidence shows that "autonomous system" is rapidly becoming a standard term. While many users may understand the notion that machines cannot be autonomous and only exhibit "autonomous-like" behaviours relative to a certain level of human control and task-environment complexity; many others do not and thus either use the term inappropriately or are unnecessarily cautious.

Autonomous functioning refers to the ability of a system, platform, or software, to complete a task without human intervention, using behaviours resulting from the interaction of computer programming with the external environment.

Tasks or functions executed either by a platform, or distributed between a platform and other parts of the system, may be performed using a variety of behaviours, which may include reasoning and problem solving, adaptation to unexpected situations, self-direction, and learning.
Which functions are autonomous, and the extent to which human operators can direct, control or cancel functions, is determined by system design trade-offs, mission complexity, external operating environment conditions, and legal or policy constraints.

This can be contrasted against automated functions, which although require no human intervention, operate using a fixed set of inputs, rules, and outputs, whose behaviour is deterministic and largely predictable. Automatic functions do not permit dynamic adaptation of inputs, rules, or outputs.

Figure : Suggested definition for "Autonomous Functioning"

Second, given that a machine or system in totality cannot be autonomous in a literal sense, the term “autonomous system” is used with the unstated assumption that not all parts or functions of the system exhibit autonomous-like behaviour. This creates scope for ambiguity, as any or all of potentially millions of system functions could exhibit autonomous-like behaviours.

Attempting to create a definition for “autonomous system,” “autonomous platform,” or otherwise, is inherently misleading without appropriate caution. Ideally, the term “autonomous system” should not be used, however, this is an impractical suggestion given the prevalent usage of the term. The key point is that using autonomous + [system / platform / robot / machine etc.] detracts from the real issue most relevant to policy, legal and engineering issues—the level of human control necessary and possible over a machine. Furthermore, it singles out “autonomy” as a descriptor for the machine over and above all the other features and capabilities of the machine. For example, we might use legitimately a particular type of communications as a descriptor for a machine, thus referring to many military systems and machines as “radio-enabled” platforms. When radios were first introduced this may have been logical; however, with the wide use of radio in practically all systems, it is not appropriate.

A recommendation emerging from this analysis, therefore, is that senior policy makers and other relevant personnel should be fully aware of the implications of using the term “autonomous system”, and should be in the practice of caveating documents, presentations and speeches with elements of the text proposed in Figure 1.

Attempting to create definitions for "autonomous systems" should be avoided, because by definition, machines cannot be autonomous in a literal sense. Machines are only "autonomous" with respect to certain functions such as navigation, sensor optimization, or fuel management.

Recommendations – Definitions

- Policy makers should use extreme caution when using the term "autonomous" especially in conjunction with other machine characteristics such as platform, system or robot.
- Rather than emphasising the fact that a system employs autonomous functions, focus should be placed on the level of human control and accountability and the type of decision being autonomised.
- Engage national and international standardisation bodies to issue guidance on appropriate usage of terms.

Military Operational Issues

Understand the operational benefits of autonomy

Recent debate about the utility and opportunities of systems with autonomous capabilities often frames issues in terms of the fact that platforms are unmanned, or emphasises the challenges concerning their weaponization, rather than autonomy as a capability in general. Autonomous functioning may be present in manned or unmanned systems, and may or may not involve weaponized systems.

The specific benefits of autonomy, as isolated from other factors, have not been well-described. This section outlines several of the key benefits that increasing autonomy delivers. How each of these benefits translates into military advantage depends on the particular system or task. Each benefit is associated with a set of accompanying risks and trade-offs, which can only be analysed in specific system-task contexts.

It is important to note that cost is not mentioned as a specific benefit. While cost savings are often claimed as a benefit of increasing autonomy, or of unmanned systems more generally, there is currently very little rigorous cost-benefit analyses on which to draw robust conclusions about potential savings. Significant further research is required on the cost-effectiveness of introducing autonomy into defence systems.

Augmenting operator performance

Autonomisation lowers operator workload, reducing fatigue and increasing the operator's capacity for other tasks. Fewer human errors translate into greater safety for others in the mission space. Increased operator efficiency can be exploited in operational concepts for controlling multiple platforms or for distributed control of platforms.

Simplified human-machine interaction

Under autonomy, the operator need only provide goals to be achieved, rather than detailed instructions. This simplifies human-machine interaction. This is with the aim of reducing operator workload but has implications for the capacity of autonomous systems to operate cooperatively with autonomous manned platforms and the wider command and control systems, for effects synchronisation and battlespace control and management.

Contingency management

Autonomous systems capable of countering unplanned deviations in mission parameters (e.g. loss of datalinks, updated intelligence, attrition of supporting elements, etc.) enhance the probability of mission success and survivability. Autonomous functions may be able to "self-optimise" system responses to adverse conditions, or dynamically re-plan and adjust mission parameters.

Information processing

Autonomy can help to increase the rate of information processing to far exceed the capability of a human. This often is a decisive advantage in conflict such as in cases of time-critical targeting. "He who decides fastest, wins!" Another aspect is the overall complexity of decision making. In the future, autonomous functions will analyse and process complex situations and allow humans to make more informed decisions.

Data link demands

Increased platform autonomy reduces the number of real-time commands from an off-board operator. However, there may be an increased dependence on other types of data links, which depends on the mission type and level of integration with other mission entities and third party sensors, There will be a trade-off between the scope of the system of interest and its autonomy.

Streamlining skill requirements

Applying autonomous systems to reduce operator task complexity can reduce skills requirements, which would yield savings in training, enhance flexibility in recruitment, and potentially reduced manpower costs. For example, unmanned aerial vehicle swarms may soon be controlled by system managers, rather than individual platforms being controlled by trained pilots.

Improved training environments

Given the behaviour of systems with autonomous capabilities is determined by computer algorithms, the same algorithms can be replicated in simulations to provide a realistic training environment, thus reducing the overall training requirement and cost. The same concept can be employed in creating tactical decision aids to run systems through task before operations, allowing early discovery of control flaws or other problems. Much more use of "flight simulator" technology could be envisaged rather than direct use of platforms in the real world.

Operational flexibility

Autonomy is a key enabler of unmanned platform technology. Building sufficient autonomy into a platform can yield all the operational benefits of unmanned platforms; persistence, reach, and endurance, all of which combine to offer potentially greater flexibility in time and space.

Understand that autonomy always involves trade-offs

Autonomy is introduced into systems based on specific design considerations and intended operational uses. For each system and for each use-case, there are a set of accompanying trade-offs that must be made to determine the extent of human control required over certain functions.

Human control versus machine control

Above all, the level of control shared by the human versus the machine is the most important trade-off when considering the use of systems with autonomous capabilities in military operations. The necessary level of human control depends on the particular situation, applicable legal constraints, and the level of tolerable risk. Important factors for policy makers when considering this balance are:

- The type of decision being transferred to the machine
- The command relationship between human and machine
- The type of operating environment
- The type of risk incurred if the machine makes the wrong decision
- The particular military benefit of autonomisation of certain functions (e.g. precision performance, faster decision making, reduction of risk to personnel.)

Optimality versus resilience

Increasing autonomous functions may lead to optimal system operations, which leads to improved reliability, precision, and effectiveness in task accomplishment.

The underlying algorithms that operate the autonomous functions, however, are usually optimised for well-modelled and tested situations. Highly refined and optimal algorithms for one situation may come at the expense of resilience against unanticipated situations.

Efficiency versus responsiveness

Autonomy may be employed by systems to minimise unnecessary computational resources and act efficiently in executing planned actions. Yet this contrasts with the need to dynamically re-plan in the event that circumstances change.

Centralization versus distribution

Autonomy changes the balance between where decision-making and information resources are allocated between platforms and control stations, or between platforms. With remotely piloted platforms, decision making is centralized and highly controlled. Autonomous functions allow greater decentralization of decision making, which may enhance responsiveness, but diminish the ability to centrally control the system.

Recommendations – Military operational issues

- Policy makers must ensure that any claimed benefits of increasing autonomy are accompanied with appropriate analysis of trade-offs and risks.
- Discussion should emphasise autonomy as a capability of systems in general, rather than a feature of predominately unmanned platforms.
- There is insufficient evidence to claim cost-saving as a generic benefit; each system must be evaluated in terms of whole life-cycle costs and compared against multiple baselines.

Legal Issues

Conclusions – Legal Issues

- International law does not prohibit or restrict the delegation of military functions to autonomous systems, provided that such systems are capable of being used in full compliance with applicable international law.
- States are obliged to legally review new weapon technologies and to ensure that any autonomous weapon systems they acquire are capable of complying with the requirements of applicable international law in practice, including, in situations of armed conflict, the Law of Armed Conflict principles of distinction, precaution and proportionality.
- The principles of international law governing State responsibility and individual criminal responsibility appear to adequately regulate the responsibility and consequences of harmful acts resulting from the use of autonomous systems.

The development, production and use of autonomous systems for military purposes raises questions as to whether existing legal instruments apply to such technologies, and if so, how the relevant provisions are to be interpreted and applied in light of the specific technological characteristics, and to what extent international law sufficiently responds to the legal challenges involved with the advent of such technology.

A legal review performed by an internationally recognized panel of subject matter experts assembled for the MCDC study examined a selection of international legal issues that are relevant to the shaping and implementation of military policies concerning autonomy in military systems. This section outlines major conclusions, and lists key issues for further analysis in specific national and international contexts. Given the complexity and contextual nature of the legal issues identified, the scope of this policy guidance does not expand on the full legal analysis, which may be found in the final MCDC proceedings report.

Autonomous systems involve issues that are governed by both national and international law. Legal concerns relevant to national law include for example constitutionality, privacy, technical industry and safety standards, licensing requirements, insurance, and product and corporate liability. Given that national law may differ significantly in terms of approach, substance and sophistication, these issues cannot be examined within the scope of this study.

As far as international law is concerned, the most notable questions are raised under the Law of Armed Conflict and International Human Rights Law, as well as under the UN Charter, the law of neutrality, the law of State responsibility and international criminal law.

Indeed, virtually any branch of international law may become relevant when a State delegates the required performance of a legal obligation from human agents to military autonomous systems. The sections below will only outline the international law issues identified in the underlying study.

Legality of weaponized autonomous systems by their very nature

An important aspect in the development, procurement and use of any autonomous system for military purposes is its international lawfulness based upon the inherent nature or design of the system itself, irrespective of the precise manner in which it is going to be used in practice. Depending on the context, key issues for policy makers concern the legality of weaponized autonomous systems under, most notably, the Law of Armed Conflict and/or under Human Rights Law.

The analysis suggests that, in general, there are no provisions under existing international law that specifically prohibit autonomous functioning in weapon systems. The burden lies with States legally to review new weapon technologies and to ensure that any autonomous weapon systems they acquire are capable of complying with the requirements of applicable international law in practice including, in situations of armed conflict, the Law of Armed Conflict principles of distinction, precaution and proportionality.

Legality of the use of weaponized autonomous systems in combat

Wherever belligerent States delegate certain functions or activities to autonomous systems, such systems must be capable of being used in a manner that respects all relevant Law of Armed Conflict obligations incumbent on the operating State.

The most serious concerns raised are the use of autonomous systems for targeting in combat, because of the risk of indiscriminate attacks on persons or objects with a protected status, and the ability of systems to influence judgements about proportionality and distinction. It is incumbent upon the operating States to ensure that autonomous weapon functions fully comply with all relevant provisions.

Military commanders and operators must fully understand how an autonomous system will respond to battlefield situations. Ultimately, the test will be whether they were reasonably justified in using an autonomous system in the particular environment. While perfection is not required, States bear the heavy burden of ensuring that any use of future autonomous systems will be reasonable and that mistakes or collateral damage could not have been avoided through feasible precautions.

Legality of employing autonomous systems for law enforcement and self-defence

The use of force by autonomous systems may also occur in situations other than armed conflicts and/or military combat. Examples are law enforcement, crowd control, detention and the protection of persons, objects or areas. Depending on the circumstances, such situations may be governed by International Human Rights Law, rather than the Law of Armed Conflict—determination of which requires analysis of the facts specific to each situation.

An important distinction between the Law of Armed Conflict and International Human Rights Law is that the former allows for targeting based on the status of the target, while the latter allows for the use of deadly force only on the basis of the behaviour of the targeted person. Absent the ability to conduct status-based targeting, autonomous weapon systems would be charged with the more complicated task of discerning the immediate danger to human life posed by their potential target, as well as the expected harm that will result from using force. In addition, autonomous weapon systems must determine when lesser means of force have been exhausted. Employment of weapon systems lacking these capabilities will likely result in violations of the employing State's human rights obligations and therefore would require the appropriate involvement of human operators.

State responsibility for harm caused through autonomous systems

Another major concern arising in relation to the military use by States of autonomous systems is the perceived uncertainty as to the attribution of legal responsibility for the potential harm caused by autonomous weapon systems in contravention of international law. The principles of general international law governing State responsibility appear to adequately regulate the international responsibility and consequences of wrongful and harmful acts resulting from the military use of autonomous systems. Most importantly, the fact that military systems can perform certain functions autonomously does not limit the responsibility of States for the harm caused by such systems. The concern that States may try to evade their international responsibility based on their unawareness of the system's faults is mitigated by the fact that States generally cannot avoid responsibility in cases of negligence and/or reckless conduct. In practice, the main problem likely will not be the attribution of legal responsibility, but the actual availability of effective judicial remedies for injured States and individuals.

This problem, however, is not specific to autonomous systems (it may also arise in relation to the use of conventional, non-autonomous, weapons or systems) and must therefore be addressed and resolved on a more general level. In conclusion, there appears to be no need for adopting an autonomous systems-specific treaty in order to address concerns related to the attribution of State responsibility for malfunctioning or misconduct of such systems.

Criminal responsibility for harm caused through autonomous systems

International law provides for individual criminal responsibility for war crimes, crimes against humanity, genocide and the crime of aggression. Military autonomous systems are not entities capable of free will and culpability in a human sense, but machines being used by humans for military purposes. In view of the capacity of autonomous systems to determine, pursue and change their course of action independently from human real-time control, there is a growing concern that it may be difficult to assign individual criminal responsibility for serious violations of international law autonomously "committed" by autonomous systems.

International criminal law is based upon the principle of individual responsibility, including command responsibility, which is likely sufficient to address the context of weaponized autonomous systems. Such systems will be programmed and deployed on missions by human operators and their use will be approved by human commanders and other human superiors in ways that are similar to the weapons currently employed by States.

Weaponized systems are very unlikely to operate without any human direction, supervision or oversight. Subject to the requirements of subjective criminal intent, individual criminal responsibility is not diminished by the fact that breaches of the Law of Armed Conflict were committed by autonomous systems. Human operators, commanders, and other superiors will remain criminally responsible for all breaches of the Law of Armed Conflict, which they commit or order to be committed through the use of autonomous systems, or which they fail to prevent, report, or prosecute according to the doctrine of command or superior responsibility.

Overall Conclusion

Overall, the present study comes to the conclusion that existing international law is fully applicable to the development, proliferation and use of systems with autonomous functions for military purposes. Existing international law does not prohibit or restrict the delegation of military functions and tasks to autonomous systems, provided that these systems are capable of performing their functions and tasks in full compliance with applicable international law. Each State is legally bound to ensure that capability with regard to any autonomous system it intends to develop, procure or employ.

At the same time, there are important ethical reservations which must be taken seriously. Most notably, the idea that autonomous systems could be autonomously deciding on the use of lethal force against humans, is perceived by some as being incompatible with the dictates of public conscience.

It would therefore be recommendable for States to work with one another with a view to establishing a shared set of norms and expectations about how autonomous systems must perform to be compliant with the Law of Armed Conflict and other relevant legal regimes.

Recommendations – Legal Issues

- States must establish and maintain appropriate legal review processes ensuring that any autonomous systems they develop or acquire are capable of being used in full compliance with applicable international law.
- States should cooperate with one another with a view to establishing a common understanding of how autonomous systems must be used to be compliant with the law.
- States should consider embedding autonomous systems with appropriate auditing, verification and data retention means as a way to help show compliance with international law.
- States should affirm that the Law of Armed Conflict would apply to the use of autonomous systems in any armed conflict and that any future autonomous systems they develop must be fully compliant with its rules and principles.

Ethical Issues

Consider the ethical implications of autonomous systems

In addition to the legal perspective, it is important to address the acceptability of autonomous system development and use from an ethical one. Legal and ethical judgments can, and often do, overlap; however, this is not true in all cases. It is possible for a law to be unethical (such as a law allowing slavery), or for an unethical action to be legal (the act of lying). Ethical analysis provides a useful perspective to evaluate current laws, newly developed laws, or the application of current laws to a new technology. Ethical analysis can also address issues not addressed by legal analysis.

While the ability to develop informed legal opinions about technology issues relies on specialist legal knowledge, most people have the requisite ethical reasoning ability to identify the ethical challenges related to an issue such as autonomous system development and use.

The ethical implications of new technology are frequently discussed in the media and are sensationalized in science fiction. Thus, it is essential that policy makers address ethical issues not only because they are important, but also because citizens expect the ethical dimensions of new technology to be considered.

The ethical analysis of autonomous system development and use can be grouped into four categories: malfunction, misuse, unintended consequences, and benefits. It is important to consider and to address issues related to these categories if the development and use of autonomous systems is to be done in an ethical manner.

Ensure autonomous systems can perform tasks in an ethical manner

Malfunction occurs when a system initiates action inconsistent with its intended functioning. The Just War Tradition of military ethics requires combatants to only intentionally target combatants; therefore, it is essential that weaponized autonomous systems be able to properly discriminate between civilians and combatants. From the Just War perspective, this is essential because civilians are thought to have immunity from intentional harm.

A related issue is whether the algorithms that direct autonomous systems will ever reach the level of complexity to allow judgment about the ethical permissibility of foreseen but unintentional harm to civilians (collateral damage). Such judgments are difficult for humans, and it is essential that humans remain in control of such decisions until autonomous systems are able to reliably determine when foreseen but unintentional harm to civilians is ethically permissible—an ambition that is far outside the bounds of current technology. Those developing autonomous technology and the legal requirements for developing new weapon systems should ensure that these systems meet the requirements and are able to integrate with collateral damage estimation methodologies; however, it is still essential that the ethical concerns raised above are prioritized when considering the feasibility of autonomous system use.

Systems with autonomous capabilities do not possess the type of free will that would allow them to be held responsible for their actions. While they should be considered and treated as machines or military equipment, the ability of autonomous systems to perform tasks with limited to no human interaction pushes the limits of our current conception of how to assign responsibility. Determining responsibility for a malfunction resulting in unintended harm or property damage will be more difficult with autonomous systems (both weaponized and non-weaponized) than with traditional systems. It is essential, then, that policy clearly delineates levels of responsibility for unintended harm or property damage caused by autonomous systems by considering how to assign responsibility to the system's designer, commander, and operator.

Autonomous systems will collect a great deal of data when they are performing assigned tasks. This includes data collected while monitoring populated areas or conducting reconnaissance. Individual privacy rights require that this data be properly secured, not used for purposes that they are not intended to be used for, and released only to authorised authorities. Developers and users of autonomous systems have a responsibility to ensure that personal data are secured.

Minimize potential for misuse and address weaponized autonomous system concerns

Misuse occurs when an autonomous system is intentionally used in a way for which it was not designed. An essential ethical concern that must be explored and addressed is the view that many hold, that it is unethical for a machine to "decide" to kill a human. They suggest that it is a misuse of autonomous systems to enable them to target and intentionally harm people. Perception of permissible killing in war is partly grounded in the idea that people may intentionally harm others, even killing them, if this is done for the purpose of self-defence, or other legally sanctioned reason. An additional reason that offers justification for permissible killing in war is that combatants act as agents of the state and are attempting to defend the state or act in accordance with a UNSC Resolution.

The ethical concerns with autonomous systems intentionally killing humans are that machines do not possess the right to life and, therefore, are not entitled to the right to self-defence and the right to harm others. Also, machines cannot be considered as "agents of the State," they are only agent of human controllers. Finally, many consider that human dignity makes it ethically permissible only for a human to intentionally kill another human. These concerns can be partially addressed by considering whether autonomous systems will actually be making targeting "decisions," or whether it is possible to link these decisions to operators or commanders. Additionally, the idea that there is no justification for autonomous systems to target humans, assuming that they do make the decision to do so, should be examined more closely. It is important to engage in public debate about this issue.

Autonomous systems could potentially be used to perform illegal action such as targeting civilians. While other weapon systems could be used for these purposes, autonomous functioning could allow illegal actions to be performed with limited human interaction, which might allow those responsible to escape identification and might allow for a wider scope of actions to occur. Due to the potential misuse of autonomous systems, and the significant harm that could result, developers and users should consider building in constraints so that autonomous systems cannot be used to perform illegal actions. Additionally, requiring that certain types of tasks receive higher level authority before they are performed would be advisable.

Given that these systems are never truly autonomous, they cannot disobey illegal orders as humans have the capacity to do, making a system constraint even more necessary. This should not be limited to weaponized autonomous systems; the misuse of other autonomous systems can have harmful effects as well, such as sending an autonomously-navigated truck into a crowd of people.

Due to the concerns mentioned above, those developing and using autonomous systems should take steps to prevent unregulated proliferation of this technology. Additionally, stringent cyber security standards are needed to prevent the take-over or control of systems by those with harmful or criminal intent.

Consider unintended consequences with ethical implications when making decisions related to autonomous system development and use

The development and use of autonomous systems will have unintended consequences, many of them with ethical implications. If autonomous systems are used in great numbers for humanitarian operations, the recipients of assistance may fear the systems, and the systems may lack human qualities that make humanitarian assistance efforts successful. The interaction between military personnel and aid recipients often plays a significant role in the success of the operation, and this fact should be considered when considering how the systems might be employed in these types of operations.

Given that unmanned systems decrease the risk to military personnel, there is a danger that the willingness of states to use military force may increase. The widespread use of autonomous systems, both weaponized and non-weaponized, might intensify this trend. Policy makers should consider this and ensure that state sovereignty and respect for life are given their proper significance when making decisions to employ military force, even if this force is primarily executed by autonomous systems.

The widespread use of autonomous systems may have another unintended consequence: adversaries may increase their targeting of civilians due to the fact that the destruction of autonomous systems does not have the same impact on national will as does the killing of military personnel. The destruction of a manned convoy or causing significant casualties for a combat unit has an impact on a state's will to fight. Without the opportunity to achieve these sorts of effects, adversaries may turn to inflicting casualties on civilians. The possibility of increased risk to civilians should be taken into account when determining whether widespread use of autonomous systems is ethically appropriate.

Finally, the widespread use of autonomous systems may undermine military professionalism. As military personnel move further from military operations and are not required to physically execute them, the conception of what it means to be a military professional may change. Maintenance of specific skills (combat and non-combat) may be viewed as less important, virtues such as courage and honour may not be as valued, and there may not be as much of a focus on the ethical application of military force. As autonomous systems are increasingly integrated into military plans and organisations, policy makers should consider how this will affect military professionalism.

The consequences noted above are only possibilities; however, their ethical implications are significant enough to include them in any cost-benefit analysis related to the development and use of autonomous systems.

Consider benefits with ethical implications when making decisions related to autonomous system development and use

There are numerous benefits associated with the development and use of autonomous systems. Using these systems for military purposes may minimize risk to civilians due to weaponized systems having the capability to discriminate more accurately than military personnel and due to the fact that autonomous systems make dispassionate targeting decisions rather than being influenced by emotions in a manner that may cause military personnel to target civilians. Also, the removal of human error caused by limited capabilities or fatigue may reduce risk to civilians by having autonomous systems perform certain tasks such as convoy operations.

Using autonomous systems for military purposes has the potential to reduce risks to military personnel. By performing the "dirty, dull, and dangerous" tasks, autonomous systems may reduce military personnel exposure to harm. There is also the possibility that widespread use of autonomous systems will allow states to maintain the same military capability for a lower cost. Whether this reduced risk and cost can be achieved is subject to technological limitations; however, because the possibility exists, policy makers are obligated to consider the feasibility of widespread development and use of autonomous systems.

States are often hesitant to employ military forces for humanitarian purposes, even when it involves stopping genocide. One reason for this is that the public typically views the purpose of military forces as the defence of the state. If the capability exists to deploy a force composed of a high proportion of autonomous systems, states may be more willing to conduct humanitarian operations. Therefore, states should consider the value of autonomous systems as their use may better enable them to fulfil ethical obligations articulated in international norms such as the Responsibility to Protect.

As with the unintended consequences, the benefits identified above are only possibilities; however, their ethical implications are significant enough that they deserve consideration when determining whether to develop and use autonomous systems.

Overall Conclusion

The development and use of autonomous systems present numerous ethical challenges as well as ethical benefits. Policy makers should take these issues seriously as they develop policy about autonomous systems, explore these issues in greater depth, and determine if other ethical issues, not mentioned above, exist.

Recommendations – Ethical Issues

- Policy makers should follow, participate in, and stimulate public discourse about the ethical aspects of the development, proliferation and use of autonomous technology. Policy makers should also be transparent about the ethical benefits and concerns associated with autonomous technology.
- Policy makers should consider and explain how, from an ethical perspective, autonomous technology is different than other technological advances. This includes considering the ethical permissibility of autonomous systems targeting humans and defining levels of responsibility for the intended and unintended consequences of tasks performed by autonomous systems; however, it should not neglect nonlethal tasks performed autonomously.

Human Factors Issues

The primary cause of failure to adopt technology is public sensibility. Technology has to be used by people, for people, and with people. When done well, the combination of technology and people can be one of the most powerful capabilities brought to the area of operations. It can also be the source of deadly failing when done poorly. This section addresses some of the considerations that provide a foundation for effective employment of autonomy in coalition operations.

Address teams of human and machine

As stated in earlier sections, autonomous systems should be understood as systems with autonomous functions. Human control in the system begins at the earliest stages of development and design and though many tasks will be carried out by machines, people will continue to be central to the successful completion of missions.

Future conflicts will be initiated and terminated by humans, not machines, robots or unmanned systems.

Enable effective interaction between autonomous systems and people from different cultures

In today's operational environment, systems with autonomous capabilities will be deployed in areas where people speak different languages, have different views about the acceptable use of machines, and have varied experiences with technology. Autonomous systems being deployed to gain access to denied areas may need to include the ability to interact effectively with people for critical purposes such as search and rescue, medical, explosive ordinance disposal or other lifesaving functions. Options for effective interaction include natural language interfaces, gestures, visual displays, and touch-based interfaces.

Policy makers should understand that physical appearances and naming conventions will influence the way that external audiences and bystanders perceive platforms. An explosive ordinance disposal platform that looks like a toy may attract children or other curious onlookers, creating a risk rather than minimizing it. A medical evacuation platform that is loaded with weapons or appears otherwise threatening might be the right thing in a combat zone, but may scare people away in a disaster area. The same logic applies to naming conventions. Most people will interpret something called PREDATOR as a threat while something called MERCY is likely to be viewed with welcome relief. Put simply, appearance is more than aesthetic appeal when designing objects for effective use. Repurposing a platform for a new mission may require changes to its appearance as well as its capabilities in order for it to be used effectively in a given military task.

Plan for organisational transitions

The hallmark of successful institutions over the centuries has been the ability to adapt its processes to technological advances. The nature of war will never change, however, autonomy will introduce sweeping changes to the execution of military operations. As autonomy matures, the way people conduct business and organise tasks will fundamentally change. This change introduces risks to multinational organisations that (as a whole) change at a much slower rate than the national partners that make up the organisation. Multinational organisations will have to begin planning early to ensure that member nations are able to contribute and benefit in relatively equal fashion as technology advances.

Emphasise the need for situation awareness at the boundaries of operations

Situation awareness is the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status in the future. In the case of coalition operations shared situation awareness is a prerequisite for successful coordination. The use of autonomy often results in a loss of direct awareness of many system activities by the human operator. This loss is potentially compounded in the case where human-machine teams must coordinate with other human-machine teams for safe and successful outcomes.

Determine some agreed standard for describing autonomy implementation

As identified in earlier discussion the level of autonomy or human control in a system and the tasks or roles assigned to human or machine are key elements in many discussions of autonomous systems. Different nations will have different rules about how autonomy is implemented and what is allowed in operations within their borders. In a coalition it is necessary that all parties understand what functions are autonomous, what decision rights are allocated to technology, and how autonomous systems are able to interact with human and machine collaborators.

Recommendations – Human Factors

- Design for effective interaction with those unfamiliar with your own systems and platforms
- Plan to shift resources from outdated capabilities to support new logistics operations and organisational structures needed for managing multiple unmanned platforms
- Evaluate and provide training for the evolving skill sets needed in a higher technology level of operations space.
- Develop coordination processes for transition points to ensure that all actors have a good understanding of the actions and potential actions of their counterparts when engaging in cooperative tasks
- Pursue an agreed standard for expressing level of human control in systems with autonomous capabilities.

Public Awareness

Considerable debate in international policy circles and media surrounds the issue of autonomous systems. Often, the way in which the subject is presented in the public sphere tends to overlook some of the detailed legal and ethical aspects already mentioned in this document, which prevents informed debate.

Public acceptance depends on whether a technology is perceived as legitimate and ethical, not necessarily that it is legal, although legality is typically an important component of acceptance. Given the significant potential implications for conflict and human society in general, development of systems with autonomous capabilities must be regulated and controlled in a transparent manner. Policy makers should ensure transparent public debate concerning the various issues presented in this policy guidance document.

The purpose of this section is to identify areas in which debate could be better informed, and recommend areas in which policy makers need to ensure that issues are appropriately defined and contextualized.

Engage the public and media on the subject autonomous technologies

The development and use of military weapon systems involving autonomous functions is undoubtedly the most controversial issue in this debate, and the area in which policy makers should place the highest levels of scrutiny. Current narratives in media tend to conflate the intended use of systems, with the fact that they may employ autonomous functions. This conflation obscures the more relevant concern of level of human control, especially when lethal action is taken, and the extent to which such action complies with international and national law. Policy-makers should be proactive and engage in transparent public discussion and international cooperation on these issues, rather than reactively counter media headlines.

Emphasise the full range of potential uses of autonomous technology

The debates surrounding autonomous weapon systems may draw attention from or even prevent investigation of the wide variety of positive aspects of this technology. Notwithstanding general legal and ethical concerns about the introduction of new technology, there are real opportunities for reduction of risk to military personnel and civilians, increasing efficiency in systems, and improving the accuracy and reliability of human decision-making.

Recommendations – Public Awareness

- Policy makers must encourage transparent, public debate on the introduction of autonomous technologies into defence capabilities, and engage with appropriate international fora.
- Public awareness campaigns are needed to correctly inform the public about new technologies.

Concluding Guidance

Understand the strategic context of autonomy in military capability development

While this document has focused on issues and considerations for policy makers, it is useful to understand that the strategic factor behind the growth of autonomy is the desire to achieve greater military capability. Military forces are increasingly called to operate in diverse mission types, across multiple theatres, and in rapid operational tempos. Autonomy is a strategic capability that will allow better allocation of military capability and optimal human-machine interaction. An example is the development of remote-split operations in which military personnel can control simultaneously multiple platforms across multiple operational theatres.

It is inaccurate to view the interest in autonomy as driven primarily by the need to reduce military personnel numbers, or to realise cost savings, although these may be relevant factors in policy makers' decisions. In fact, many recent deployments of unmanned systems have resulted in unforeseen manning requirements to process the large amounts of data collected, or to oversee and maintain platforms. Likewise, isolated cost comparisons of manned versus unmanned platforms rely heavily on assumptions about the nature of the military task, which are often conceived in terms of what a manned platform originally performed.

Autonomous capability requires the convergence of multiple technologies

Autonomy is not a discrete technology discipline in itself, but an end result of a constellation of supporting technology areas. The ability to achieve autonomous functioning in defence systems relies upon a diverse set of capabilities such as: sensor system hardware and processing; situation awareness, decision making and planning algorithms and software; pattern recognition and data fusion techniques; and robotics and control technology, amongst others.

Research and development programs concerning autonomy in systems need to consider these supporting technology areas separately, and in integrated programs to maximise capability development potential. Furthermore, in addition to the foundational research areas, a wide variety of systems integration capabilities are affected: system verification, validation, testing, and evaluation methods; reliability and certification standards; machine-to-machine interoperability; training systems; and auditing and control systems.

Emphasise priority research areas

Current development of autonomous capability tends to focus on foundational research in key supporting technology areas, or the development of individual systems. There are several high priority interdisciplinary areas in which efforts should be focused to compliment current research and capability development.

Operational use of systems with autonomous capabilities. Greater understanding is required on the novel and innovative ways in which systems with autonomous capabilities can be used to support operational tasks, and potential new tasks that may be possible. Tools used for defence planning, such as mission-task decompositions, and operational concepts for system will likely change.

Countering systems with autonomous capabilities. It is likely that systems with autonomous capabilities will proliferate and will be found in the future operational environment. There are unique challenges that will be faced in countering these systems, especially without the ability to rely on traditional jamming and communication link disruption methods. Policy makers are advised to encourage research, development, planning and wargaming to counter potential conventional and asymmetric uses of autonomy against friendly States.

Cyber issues and systems with autonomous capabilities. Cyber defence and attack systems represent a subset of autonomous systems that have not been covered by this policy guidance. The expert group assembled for the MCDC study; however, recommended that there are unique issues in this field that warrant further research efforts.

Impact on the character of war. Strategic-level research should be encouraged on the potential of autonomous technologies to impact the nature and conduct of war. In addition, study is required on the likely change in military tactics that new concepts such as swarm operations and joint human-machine teaming will bring.

Command and control. Research is needed on autonomy's impact on traditional command and control concepts. Autonomy will allow highly decentralized command centres located both in and outside of the theatre and more flexible and agile network control systems relying on machine-to-machine communications, rather than direct operator control. This may blur considerably the boundaries between command levels. Future research must focus on battle space management concepts, and operational command.

A view to the future – principles for policy makers

As autonomy grows ever prevalent in defence capability, several factors will remain constant. These factors can be considered as "policy-making principles" that will facilitate the reasonable and appropriately cautious introduction of autonomous capability.

Commander responsibility. Commanders will remain responsible for the actions of personnel and machines under their command, and operators or designers are similarly responsible in certain cases. This will serve as a natural limit to the scope and reach of autonomous functioning. A sound principle for policy makers and developers is to always ensure an option of scalable level of human control and auditability in systems, depending on the military context and the level of risk.

Consideration of compliance and risk. Policy makers and commanders are likely to view the development of systems with autonomous capabilities and their use in terms of compliance and risk. Systems will have to be developed and used in compliance with international and national law, and in compliance with contemporary ethical perspectives and public viewpoints. Operational use of systems with autonomous capabilities will be strongly dependent on the acceptable risk to achievement of mission goals, and the potential risk for not being in compliance with law.

Multidisciplinary capability development. Autonomy should not be considered as a standalone capability, but as a characteristic that will be integral to many future defence systems. Policy makers should ensure that multidisciplinary research programmes are pursued that link technology developers and systems designers with legal and ethical experts. Furthermore, while basic technology areas concerning artificial intelligence and algorithms are key to autonomous functions, human factors and organizational issues should be incorporated in development from the outset.

International cooperation and transparent development. Given the wide ranging implications on the conduct of military operations, and the many cross-over applications in the civilian domain, policy makers should not be dissuaded by the negative media debates and should encourage international cooperation, and open transparent development. This can be achieved by engagement in international academic and intergovernmental conferences, multination research programmes, and supporting publicly funded and published research.


MCDC
2013 - 2014
Combined Operational Access