Mission Support for Drones:
A Policy Based Approach

Alan Cullen
BAE Systems
Chelmsford
CM2 8HN, UK
alan.m.cullen@baesystems.com

Bill Williams
BAE Systems
Chelmsford
CM2 8HN, UK
bill.williams@baesystems.com

Elisa Bertino
Purdue University
West Lafayette
IN, USA
bertino@purdue.edu

Saritha Arunkumar
IBM UK
Hursley
SO21 2JN
saritha.arun@uk.ibm.com

Erisa Karafili
Imperial College
London
SW7 2AZ, UK
e.karafili@imperial.ac.uk

Emil Lupu
Imperial College
London
SW7 2AZ, UK
e.c.lupu@imperial.ac.uk

ABSTRACT

We examine the impact of increasing autonomy on the use of airborne drones in joint operations by collaborative parties. As the degree of automation employed increases towards the level implied by the term 'autonomous', it becomes apparent that existing control mechanisms are insufficiently flexible. Using an architecture introduced by Bertino et al. in [1] and Verma et al. in [2], we consider the use of dynamic policy modification as a means to adjust to rapidly evolving scenarios. We show mechanisms which allow this approach to improve the effectiveness of operations without compromise to security or safety.

1. INTRODUCTION

Drones are often discussed for their use in both military operations (e.g. for surveillance) and in non-military applications such as pipeline inspection, highway monitoring and filming [3].

A drone may be viewed as a platform with a specific capability, such as carrying a payload and flying between waypoints. The payload itself may have capabilities, such as a sensor with the ability to search for targets. The capability of the combined system can be further increased by operation in swarms and also by introducing a degree of autonomy. Consider for example a search and rescue operation where the only human interaction is the pre-flight preparation (e.g. loading fuel) and providing information about search area and the nature of the emergency. We wish to ensure that missions will continue to be efficient and effective even as the level of human intervention is decreased.

Given this vast potential for drones, policy management is a way of constraining the system of systems so that it does what is required, as efficiently as possible, whilst avoiding anything undesirable. For example we may require a search and rescue mission to prioritise search in one area whilst staying away from a disputed zone.

This paper introduces a policy management approach to address such requirements. The discussion takes place in the context of military drone operations for a number of reasons including the relative maturity of the technology, and the corresponding maturity of the safety, security, and operational planning regulations which are employed. The paper gives a background by covering current operation planning processes (section 2) and the planning of drone missions (section 3). Autonomy has a specific meaning in the context of airworthiness certification and the paper distinguishes automated and autonomous functionality in section 4. Finally the paper introduces a generative policy based approach within a policy management framework in section 5, drawing upon examples from a scenario at the start of the section.

2. JOINT MISSION PLANNING

This section outlines the wider context in which a drone mission is planned and carried out. We assume that the drone mission forms part of a larger mission which, in turn, is part of a joint operation, and subject to the rules of engagement laid down for the operation and to the operating practices of the country or coalition which sets its strategic objectives.

2.1 Doctrine and Standards

Military campaigns are, in general, large scale affairs and their planning requires a large staff to ensure that all the detailed objectives and deployments are captured. However, to paraphrase Moltke the elder: "No plan survives first contact with the enemy". Because an initial plan will be both incomplete and ephemeral there is a continual need to revise and extend it, and this involves the need to both communicate and analyse its content so that it can be modified to take account of changing events and revised objectives.

In order to support initial planning, and also the communication, analysis, and revision of a plan, most governments have established a series of doctrines to govern the planning process and to train commanders. Within NATO this doctrine exists in [4] which has been adopted by both the U.S. and the UK (although with some national caveats).

DroNet'17, June 23, 2017 Niagara Falls, NY, USA.

ACM 978-1-4503-4960-4/17/06…$15.00
http://dx.doi.org/10.1145/3086439.3086444

For drone operations a NATO standardization agreement [5] is available to support interoperability. This goes some way toward defining a common operating model for a drone platform and defines five levels of interoperation:

1. Indirect receipt and/or transmission of sensor and associated metadata.
2. Direct receipt of sensor and metadata from the drone.
3. Control and monitoring of the drone payload.
4. Control and monitoring of the drone – except launch and recovery.
5. Control and monitoring of the drone launch and recovery.

Note that complete control of the drone, including launch and recovery is not listed as an option because these 'levels' are intended to be 'independent' and so, presumably, can be combined as required for a specific mission.

The UK view of drone operations, to the extent that it is publicly visible, appears in [6] which discusses current and near-future capabilities, the legal and ethical issues involved in drone operations, and technical issues such as the distinction between automation and autonomy.

In a conventional view of mission planning and management, policy is a specific interpretation, tailored to the mission itself, of the prevailing doctrine and standards. In our dynamic policy perspective, doctrine and standards serve as boundaries for a region within which a dynamic policy decision can be made, and, within these constraints, the policy may be modified in response to changing conditions.

2.2 Resources and Constraints

A significant factor in the detailed planning of a drone mission is the resources available to, and the constraints on, the execution of the mission. For this discussion the term 'constraint' will be used for restrictions on drone activity imposed by capability, tactical, and operational issues, and derived from external factors. Among these might be:

- Selecting the flight path to avoid detection or attack.
- Congested airspace over target or operating base.
- Airspace segregation to avoid collisions between manned and unmanned aircraft.
- Ensuring a satisfactory level of communications where the spectrum may be congested and contested.
- Navigation in areas where GPS may be denied.
- Weather conditions and day/night illumination differences.

In addition to the constraints imposed by external factors, operations may also be subject to limited resource availability. The necessary resources might include:

- Personnel, e.g. pilots, surveillance operators and analysts, maintenance staff. With several missions operating at the same time, ensuring the right people have the necessary availability can be difficult.
- The pilots and other ground staff need access to equipment to run the mission, the right people need to be matched with the necessary equipment.
- The drone itself is a vehicle and needs fuel, spare parts, and perhaps other supplies to meet its mission requirements. Particularly in a forward base, these may be in limited supply.

From our perspective the role of policy in managing the resources and constraints of a drone mission is to select, at each policy decision, an action which optimises the performance of the mission within the boundaries laid down to ensure the success of the operation and the strategic principles which govern the entire campaign.

3. PLANNING A DRONE MISSION

The NATO joint doctrine for operational planning [4] sets out the principles for planning at the joint force command level. The conduct of air operations is dealt with in greater detail by the supplementary document [7], which also contains a short section on planning for drone operations.

In general a drone operation is similar to manned air operations, at least for larger platforms, and is defined through Air Tasking Orders (ATO) and Airspace Control Orders (ACO) which specify, respectively, the function to be performed, and the routes to and from the target area, and station keeping at the target area. The smaller drones, those less than 15kg in weight, are often operated at low altitude and within line of sight of the operator. In this situation, where operation will not impinge on normal air operations, the formality of ATO and ACO is often omitted and control is left to the unit commander to deploy them as required.

The larger drones differ in a number of respects from manned aircraft, and this has an impact upon planning:

- Typically drones will have longer endurance, but lower speed, than comparable manned aircrafts. Allocation and tasking will vary from the norm for manned systems.
- Current technology requires some level at least of continuous, or almost continuous, communication between the drone and its controller.

A common practice with drone operations is remote-split operation (RSO) where the drone itself is based in the theatre of operations, perhaps at a Forward Operating Base (FOB), but, other than take-off and landing, the platform is piloted remotely from, for example, the U.S. or UK over a satellite link. This minimizes the resources required at the FOB, but has a critical reliance on the communication path, which may be vulnerable to attack by a sophisticated adversary.

There are three fundamental guidelines to planning at any level within a campaign:

- Understand the higher commander's intent, objectives and desired end-state, i.e. the purpose of the military action.
- Understand the operational environment including factors such as terrain, communications, and any relevant civil or other authorities.
- Focus on linking the current mission objectives to the objectives and desired end-state of the higher operational level.

Typically some form of optimization process has been performed at the higher level to partition the objectives at that level into a set of more detailed (but perhaps narrower scope) objectives at the current level.

Drones, at present, have little or no ability for self-defence and are therefore vulnerable in contested airspace [6, p. 1_4] and [8]. At an early stage of development of drone capability they were promoted as suitable for tasks which were 'dull, dirty and dangerous'.

Dull: Tasks with low workload and low intensity such as surveillance over a fixed location. These tasks assume a degree of automation, but without continuous direct control, or sophisticated autonomy, any high-priority opportunity which arises may be missed.

Dirty: Operations in environments which are hostile to a manned aircraft or its crew. An example of this would be observation related to chemical, biological, radiological, or nuclear detection.

Dangerous: Tasks where, for example, there is a high ground to air threat which does not merit the risk to aircrew or soldiers on the ground.

4. THE IMPACT OF AUTONOMY

Many drones are directly controlled by ground-based pilots. However, more advanced systems have pre-planned behaviors that reduce the need for pilot intervention, for example by automating take-off and landing, as well as station-keeping. Improvements in navigation capability allow routes to be specified in terms of waypoints, with automated flight between waypoints.

Chapter 2 of [6] defines and distinguishes between automated and autonomous drone systems. The need for such a distinction arises mainly from considerations of safety. An automated system selects each action from a fixed palette following a static decision process and based on its immediate state, surroundings, and goals. Under these conditions it is relatively straightforward to calculate the drone's behaviour under any circumstances, and thus to guarantee its safe operation.

By contrast an autonomous system will attempt to pursue an 'optimal' plan, selecting its actions to maximize returns and minimize cost. Typically this will involve dynamically choosing the decision criteria to apply based on a number of additional factors such as its state history and its weighted predictions of possible future options. The additional complexity makes achieving an equivalent level of confidence in any guarantee of safe behaviour more onerous.

Nevertheless, we believe that in the future there will be an increasing emphasis upon autonomous systems. Suppose that a squad of drones is on a mission, e.g. gathering information from a particular area, where each of them should perform its assigned tasks and continuously send information to each other for coordination. If one of the drones finds an obstacle, it should be able to avoid it and define a new trajectory for reaching the goal state. Thus, the drone should choose between the station-keeping, following the defined trajectory, gathering information as required by mission planning, and avoiding collision with an obstacle. Such decisions must be made promptly.

Drones may lose communications for a number of reasons, such as stealthy operation, equipment failure, loss of line of sight, and interference. Thus, the decision of what action to take should be made by the drones themselves, or sometimes by a squad of drones, without requiring remote support as far as possible.

5. POLICY BASED MANAGEMENT

In this section we introduce the key elements of our policy based approach for drone mission assurance. We start with a fictitious example scenario that we will use to illustrate the discussion. We then introduce the fundamental notions of our policy approach, and the components of our proposed policy model. We conclude with a discussion of the policy enforcement mechanism.

5.1 Scenario

UK and U.S. forces are in a coalition operating in a hostile environment. The UK and U.S. dispatch drones from their FOBs (see Figure 1). Both nations deploy drones on surveillance missions, and the policy is to inform each other of missions as a part of airspace management. The UK has planned a mission for drones to loiter over area C, with an outward route via waypoints A1, A2 and A3, and a return via B1, B2 and B3. This route planning has considered issues such as terrain, threats, communications availability and weather, and emergency landing sites have been identified.

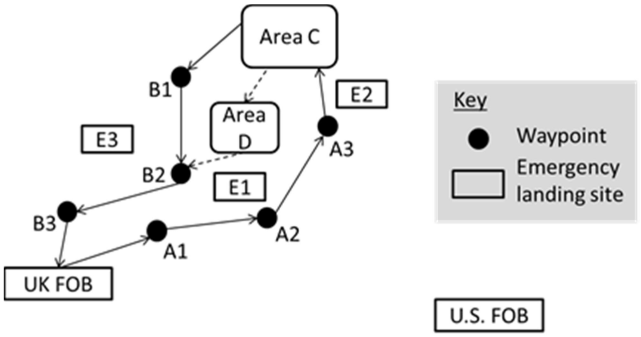

Figure 1: Scenario

The UK drones carry out surveillance as a group, with one drone operating as a leader and the other drones operating a mix of wide area and high resolution sensing.

The U.S. has just lost a manned aircraft in area D and wishes to extract the crew who fortunately have survived. The U.S. requires imagery of the area to confirm the location and select a landing site. Confidentiality is important to minimise the risk to the aircrew and the rescue mission. The U.S. considers three options for collecting this imagery:

- Via a U.S. drone mission. This has a risk of alerting opposing forces, and will be relatively slow.
- Task U.S. special forces operating near D. This puts further lives at risk, and there will be a delay before they are in a position to transmit the images securely.
- Ask the UK to retask a drone currently operating at C. This has the benefits of a fast response and appearing to opposing forces as a routine part of a routine mission. However tasking the UK risks leaking aspects of a classified operation.

The U.S. decides that the benefits of tasking a UK drone outweigh the risks. The UK accepts a tasking request from the U.S. after confirming that the safety of the ongoing mission at C will not be compromised.

The most suitable UK drone is identified, the choice being based upon sensor fit, current location and fuel status, etc. The drone is retasked, and new policies are sent so that it will obey sensor control from the U.S. and communicate according to NATO policy via its software defined crypto. The drone hands its current mission to its peers and flies towards D, automatically selecting a route that gives the earliest line of sight. Selected elements of the drone payload output – for example, excluding UK-eyes-only content – are made available to the U.S. controllers. Meanwhile the remaining drones autonomously take on an additional role of observing forces in C moving towards D that may constitute a threat to the forthcoming extraction of the aircrew.

5.2 Generative Policy-based Architecture

The illustrations and terminology in this section are taken from Verma et al. [2]. Common architectures for policy based management systems (PBMSs) are based on a policy life cycle under which policies are specified by a human administrator via a high level interface, and then translated into a machine policy language through a process of refinement and transformation (see Figure 2). The machine level view of policies is used by a policy decision point (PDP), an automated component taking decisions governing the actions of the managed drones. The PDP is invoked by the managed drones in order to obtain directives before executing actions. For example in our scenario, the UK drone should invoke the PDP to decide which features to share. Such invocation is performed via the policy enforcement component (PEP) which represents the interface between the managed entities and the PBMS.

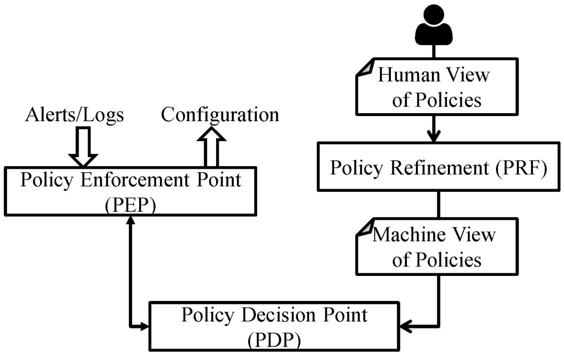

Figure 2: High level reference architecture for PBMS

Such a conventional approach may not be suitable for situations in which the drone is unable to communicate with the PBMS hosted on the FOB or when the drone may dynamically acquire novel information and does not have time for transmitting such information to the FOB.

The generative policy approach aims at addressing such shortcomings by allowing the managed entities more autonomy in policy refinement and decisions. The diagram in Figure 3 shows the evolution required for next-generation PBMS.

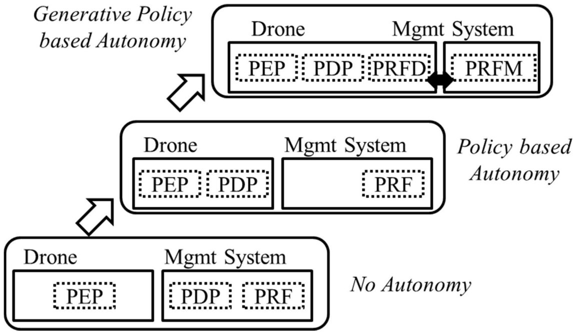

Figure 3: Evolution of PBMS architectures

In the architecture referred to as *policy based autonomy* the policy based decisions are taken by the drones, whereas the policy refinement is still executed by the PBMS. Therefore the managed drones have still limited autonomy. By contrast, in *generative policy based autonomy*, drones are provided a partially specified policy, referred to as *generative policy*. In such an architecture, a refinement component is included in the software aboard each drone, referred to as policy refinement at drone (PRFD). Each drone can then (dynamically) refine and adapt the generative policy, and based on its own 'customized' policy take decisions about its own actions.

5.3 Policy Domains for Mission Assurance

The definition of a PBMS specific for drone mission assurance also requires identifying the various types of policies related to drone mission assurance. Each type of policy, referred to as *policy domain*, covers different aspects related to assuring the given missions. Key domains, also shown by our scenario, include:

- Navigation policies: They concern decisions about drone navigation, for example changes to the initial navigation plan. With reference to our scenario, an example of navigation policy is the one stating that: (a) a drone must follow the pre-defined navigation plan; (b) however the drone can dynamically change the plan if requested to do so by an authorized source. This requires in turn specifying criteria for determining whether a source is authorized.
- Landing policies: They concern decisions about landing. Such policies are very dynamic in that they require up-to-date trusted information about landing areas. A landing area which is 'secure' may become 'insecure' within a short time. Mechanisms must be provided by which a drone can rapidly acquire such information that can drive its landing decision.
- Data management policies: They concern decisions about the management of collected data. With reference to our scenario, the drone can also continuously check if other drones (perhaps owned by other NATO countries) are near-by and in case of failure the drone may off-load the data to another drone provided that: (i) the data is strongly encrypted before being off-loaded; and (ii) the latter drone has enough storage capacity or can free storage by removing less critical data.
- Sensor management policies: They concern decisions such as revealing sensor quality to third parties, authorisation for sensor commands, and privacy issues related to potential targets. Note that drones may carry different sensor payloads so the applicable policies will vary between drones.

It is important to notice that each policy domain is related to the handling of specific events and that the various policy domains are interrelated. In many cases the main refinement required by the drone concerns conditions indicated in policies, such as a 'secure' landing area or an 'authorized' source.

5.4 Policy Models

Our policy model consists of four key elements:

- Self-describing entities: As our policies often use conditions about entities, such as drones, landing sites, and waypoints, it is critical that each such entity making policy decisions has access to all necessary information, referred to as *attributes*, for evaluating the conditions. Notice that some attributes may be 'derived' from other attributes by means of functions, and that some attributes are static, whereas others are dynamic. For example, in our scenario the self-description of each drone would include the following attributes: the country of the drone (static attribute), and the current position and available storage capacity (dynamic attributes). We expect that drones will be able to collaborate with other drones and other devices, such as robots and autonomous vehicles on the ground. Thus drones will be pre-loaded with an ontology of capabilities of the various types of drones and devices. However notice that supporting self-describing entities for mission assurance in potential hostile environments is quite challenging. We refer the reader to **[1]** for a discussion on challenges and approaches.
- Preference graph: It indicates preferences among the possible actions. Such preferences guide the determination of which policies to consider according to which order. A fragment of a preference graph for our scenario is given in Figure 4. Notice that alternative approaches for specifying preferences can be adopted. We refer the reader to **[9]** for an introductory discussion.
- Generative event-condition-action (ECA) rule: A rule that specifies that if a certain event happens and certain conditions are true, then the action is executed. Triggers used

in relational databases are a well-known example of ECA rules. In our context, the condition part of an ECA rule is a Boolean combination of predicates against attributes of the drones and other entities. In a generative ECA rule one or more predicates are replaced by 'placeholders' indicating that they have to instantiated before the rule can be applied. Placeholders can be seen as functions that return three different truth values: true, false, and unknown. The unknown value is used to indicate the case in which a predicate cannot evaluated. In addition to contain placeholders, conditions can be specified as modifiable or fixed (denoted as MOD and FIX, respectively). A modifiable condition is one in which specific predicates and/or placeholders can be removed and new predicates and placeholders can be added.

An example of generative ECA rule follows:

Event Request-to-Emergency-Land
(X: landing site)

Condition Secure(X) **MOD**

Action Land(X)

Notice that the event component of the rule has a variable, indicating the event parameter and a domain for the parameter. In the above example, the variable indicates that as part of the event a landing site will be indicated. The rule is open meaning that the condition can be modified.

- Instantiated ECA rule: It is an ECA rule in which all placeholders have been instantiated with actual predicates expressed in terms of attributes. Also variables indicated in the event of a generative ECA rule can be instantiated. In our scenario, for example, one can determine in advance and automatically all possible landing sites based on a static knowledge of the flying area and the planned route of the drones.

  As an example consider the landing sites in our scenario (Figure 1). Suppose that E1 is always considered insecure while E2 is considered secure. By contrast, the security status of E3 must be evaluated dynamically. Our example generative ECA rule is instantiated into the following three instantiated rules, where CURRENTTIME is a system variable indicating the current time:

1. *Event:* Request-to-Emergency-Land(E1)
   Condition: False
   Action: Land (E1)
2. *Event:* Request-to- Emergency-Land(E2)
   Condition: True
   Action: Land (E2)
3. *Event:* Request-to- Emergency-Land(E3)
   Condition: E3.SecStaus = OK AND CURRENTTIME - E3.SecStatus.NotifT <10m AND E3.SourceNotif.Trust = High
   Action: Land (E3)

The condition in the third rule specifies that landing site E3 is considered fine for emergency landing if: its security status is okay; the status has been notified to the drone less than 10 minutes ago; and the source of the status notification has high trust. Notice that a critical condition is the one concerning the trust level of the source of the notification. Therefore other policies must be specified for the computation of such trust level. An example of trust policy is as follows. The trust level of the source notification is considered high if: (i) the notification has been received from the FOB over an encrypted communication channel; or (ii) the notification has been received from another drone, the notification has been transmitted encrypted, and the other drone has been authenticated.

We want to emphasize that our policy model is complemented by an incremental and dynamic rule instantiation mechanism. Such a mechanism allows a drone to incrementally add to its instantiated ECA ruleset. These additional rules can be acquired from other drones (in case of collaborative drone missions). For example suppose a drone has no instantiated ECA rule concerning landing site E3; however another drone may have such a rule and provided that the latter is trusted by the former, the instantiated ECA rule can be shared.

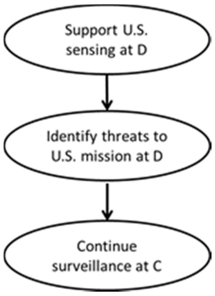
Support U.S. sensing at D
Identify threats to U.S. mission at D
Continue surveillance at C

Figure 4: Example of preferences for the retasked surveillance mission

5.5 Policy Enforcement

Policy enforcement refers to the process according to which the various instantiated ECA rules are evaluated. The evaluation is driven by the preferences (see Figure 4). In our scenario the preferred action is to support the U.S. imagery requirement, so ECA rules will be evaluated to assign a drone to the mission with minimal impact upon the existing surveillance. Moreover, because the U.S. has shared information about a forthcoming extraction operation at C, the rules also give priority to supporting this mission by identifying new threats.

Notice that the policy evaluation process must be executed in real-time and thus the time required must be estimated. For example, if a drone has only two minutes available for determining the action to be executed, the enforcement engine may decide to bypass the evaluation of certain rules if information needed to evaluate these rules is not readily available and it has to be acquired. Approaches to address such problem can be developed based on query optimization approaches developed for database systems [10].

6. CONCLUDING REMARKS

This paper contains a vision for future drone operations where policy management is used to ensure a best possible outcome for operations with drones that may include autonomy.

A benefit of autonomous operations is the reduction in manpower and thus an increase in the scalability of these operations. This reduces cost as well as minimising the danger to personnel. However this benefit will only be delivered if safe operation is guaranteed with minimal human interaction.

Policy covers many areas, including use of airspace, handling aircraft emergencies, authorisation of commanders, handling of sensitive information, trust in cooperating drones, prioritising different aspects of a mission, and when a man in the loop is mandated for decision making. A policy framework is required to deliver this information to each drone, along with policy to constrain operation if communications are lost.

The security of the policy framework will be critical. It is clear that an integrity attack could produce undesirable behaviour, and confidentiality attacks could result in predictability and hence vulnerabilities. Wireless communications to drones are open to attack, and may be constrained by congested spectrum, so autonomy to prevent this becoming an Achilles heel is important.

The ITA project is creating a generative policy model that is well matched to the challenges of autonomous drone operation in uncertain and contested environments. This paper has introduced the model and explained its use and benefits within a coalition scenario. Research in generative policy models has commenced and a roadmap is to be found in [1].

Detection and resolution of policy conflicts is an important area in the roadmap. Conflicts can arise for many reasons, such as different sources for policy, contention for resources, and delayed propagation of updates. We refer interested readers to work on argumentation-based techniques for dynamic policy prioritisation [11], [12], and [13] as an example of a current approach.

Although this paper has focused on drones, the ITA is researching the generative policy model in a wide variety of other systems ranging from land vehicles to a future generation of smart firewalls. This paper has also introduced the policy domain concept in which, where appropriate, a policy may become independent of its 'host platform' and, for example, define an aspect of common behaviour shared across many different platforms.

7. ACKNOWLEDGMENTS

This research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence under Agreement Number W911NF-16-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

8. REFERENCES

[1] E. Bertino, S. Calo, M. Touma, D. Verma, C. Williams and B. Rivera, "A Cognitive Policy Framework for Next-Generation Distributed Federated Systems," in *ICDCS (to appear)*, 2017.

[2] D. Verma, S. Calo, S. Chakraborty, E. Bertino, C. Williams, J. Tucker and B. Rivera, "Generative Policy Model for Autonomic Management," in *1st Int. Workshop Dist Analytics Infrastructure & Algorithms, IEEE Smartworld Congr, 2017 (to appear)*, 2017.

[3] EASA, "Concept of Operation for Drones: a risk based approach to regulation of unmanned aircraft," European Aviation Safety Agency (EASA), 2015.

[4] NATO, "AJP-5: Allied Joint Doctrine for Operational-Level Planning," North Atlantic Treaty Organization (NATO), 2013.

[5] NATO, "STANAG 4586 Standard Interfaces of UAV Control System for NATO UAV Interoperability," North Atlantic Treaty Organization (NATO), 2012 (ed.3).

[6] MoD, "Joint Doctrine Note 2/11: The UK Approach to Unmanned Aircraft Systems," UK Ministry of Defence (MoD), 2011.

[7] NATO, "AJP-3.3: Allied Joint Doctrine for Air and Space Operations," North Atlantic Treaty Organization (NATO), 2016.

[8] JAPCC, "Remotely Piloted Aircraft Systems in Contested Environments," Joint Air Power Competence Centre (JAPCC), 2014.

[9] F. Rossi, K. B. Venable and T. Walsh, "Preferences in Constraint Satisfaction and Optimisation," *AI Magazine,* pp. 58-68, 2008.

[10] P. G. Selinger, M. M. Astrahan, D. Chamberlin, R. Lorie and T. G. Price, "Access path selection in a relational database management system," in *Proc. Int. Conf. Management of Data, SIGMOD'79*, 1979.

[11] E. Karafili, A. Kakas, N. Spanoudakis and E. Lupu, "Argumentation-based Security for Social Good," http://arxiv.org/abs/1705.00732, 2017.

[12] E. Karafili and E. Lupu, "Enabling Data Sharing in Contextual Environments: Policy Representation and Analysis," in *Proc. ACM Symp. Access Control Models and Technologies, SACMAT'17*, 2017.

[13] A. Bandara, A. Kakas, E. Lupu and A. Russo, "Using Argumentation Logic for Firewall Configuration Management," in *IFIP/IEEE Int.Symp. Integrated Network Management, IM'09*, 2009.