Front. Eng. Manag. 2019, 6(1): 102–116
https://doi.org/10.1007/s42524-019-0008-5

RESEARCH ARTICLE

Andrew LOCKLEY

Security of solar radiation management geoengineering

Abstract Solar Radiation Management (SRM) geoengineering is a proposed response to anthropogenic global warming (AGW) (National Academy of Sciences, 2015). There may be profound – even violent – disagreement on preferred temperature. SRM disruption risks dangerous temperature rise (termination shock). Concentrating on aircraft-delivered Stratospheric Aerosol Injection (SAI), we appraise threats to SRM and defense methodologies. Civil protest and minor cyberattacks are almost inevitable but are manageable (unless state-sponsored). Overt military attacks are more disruptive, but unlikely – although superpowers' symbolic overt attacks may deter SRM. Unattributable attacks are likely, and mandate use of widely-available weapons. Risks from unsophisticated weapons are therefore higher. An extended supply chain is more vulnerable than a secure airbase – necessitating supply-chain hardening. Recommendations to improve SRM resilience include heterogeneous operations from diverse, secure, well-stocked bases (possibly ocean islands or aircraft carriers); and avoidance of single-point-of-failure risks (e.g. balloons). A distributed, civilian-operated system offers an alternative strategy. A multilateral, consensual SRM approach reduces likely attack triggers.

Keywords security, geoengineering, solar radiation management, SRM

1 Introduction

AGW is a primary challenge for the world, over the coming centuries (Intergovernmental Panel on Climate Change, 2013). Major financial expense will be needed to deal with the previously-unaddressed social cost of carbon (Yang et al., 2018), and to address resulting physical, geopolitical and social issues (Stern, 2006). Already, great international and domestic negotiation efforts have been made to make the political deals (United Nations Framework Convention on Climate Change, 2014) necessary to restrict expected global temperature rises. Ongoing difficulties experienced in completing a rapid transformation of world energy systems (to break links between energy production and CO_2 emissions) have resulted in a revisiting of discussions of geoengineering— as an alternative or complement to the more traditional interventions of mitigation and adaptation. Geoengineering, in its current usage, is ordinarily interpreted as meaning deliberate modification of the climate system.

There are two principal types of proposed geoengineering:

(1) **CDR:** a group of techniques described either as Carbon Dioxide Removal, or (more generally) Greenhouse Gas Removal (GGR) (Lomax, 2015). GGR includes removal of secondary Greenhouse Gases (GHGs) (methane, etc.), as well as carbon dioxide. CDR offers a theoretically-complete solution to CO_2 emissions – but only if conducted rapidly. Delays in conducting CDR leads to interim temperature increases, which can cause permanent harm (e.g. extinctions). Cost is the major barrier to CDR deployment at scale (a figure of 50 EUR/ton CO_2 is suggested by IEAGHG (Kornneef et al., 2011),.

(2) **SRM:** Solar Radiation Management works via modification of the Earth's radiation balance, i.e. by reflecting sunlight. Example SRM proposals include local measures, such as crop albedo modification and white roofs. However, our concern is security – and the more global SRM measures are therefore of much more relevance, as their direct transboundary effect is likely to be far more controversial. Two are seen broadly as plausible: Marine Cloud Brightening (MCB), which would be delivered from a flotilla of small ships; and Stratospheric Aerosol Injection (SAI – replicating the cooling following volcanic eruptions), which is delivered from one or more tethered balloons, or from a number of free-flying aircraft. SRM does not constitute a complete solution to emissions. First, it is temporary— excepting far-fetched technologies, such as space mirrors. Secondly,

Received October 15, 2018; accepted December 5, 2018

Andrew LOCKLEY (✉)
School of Construction and Project Management, University College London Bartlett, London WC1E 6BT, UK
E-mail: andrew.lockley@gmail.com

SAI also is imperfect in its climatic corrections. SAI would, for example, lead to a global climate drier than a pre-industrial climate with the same global average temperature. Plausible methods of SRM are comparatively inexpensive: It is climate and ecosystem risks, and political controversy, that underpins the reluctance to deploy. N.B. SAI is the most widely-discussed form of SRM, and comments within this paper relate principally to SAI.

Large-scale geoengineering deployments have not yet occurred, save for various afforestation (tree-planting) programmes, and suchlike. However, various anthropogenic processes (e.g. particulate air pollution) have inadvertent effects on climate – although lack the relevant intent to qualify as geoengineering. In addition, many necessary technologies exist only in theory – but deployment is not generally regarded as posing insurmountable challenges (although some high-tech implementations are potentially problematic, e.g. space mirrors).

Geoengineering, therefore, exerts an increasing influence on climate discourse and policy. More formally, CDR is becoming deeply embedded in international agreements. The recent Paris agreement relies on large-scale CDR in the second half of the 21st century (Lewis, 2016). SRM, by contrast, is not widely accepted as a policy instrument and is not given prominence in the recent IPCC 1.5°C report (Intergovernmental Panel on Climate Change, 2018).

SRM geoengineering can be regarded as having an ongoing annual cost. This is due principally to its impermanence – and to dominance in the cost calculations of chemicals, labor, and short-life or leasable equipment (McClellan et al., 2012). McClellan et al. (2012) estimate total SRM costs for global climate management at as little as $2 billion per year. To give an idea of scale, this potentially involves as few as 14 aircraft or as few as 4 bases (trade-offs exist). Notably, cost estimates and cooling assumed may differ widely between different studies. However, in all deployment scenarios, the costs remain trivial when compared to the size of the fossil-fuel economy. Notably McClellan's costings do not consider potential savings from drone deliveries— an obvious possibility, considering widespread current deployment of military drones. As GHG levels in the atmosphere rise, more aggressive interventions may be needed. Nevertheless, SRM's total direct costs remain a negligible proportion of global GDP.

Future deployment of geoengineering technologies may be by commercial firms (Lockley, 2016a), or by states. Likewise, two models for the future commercial purchase of geoengineering exist— depending on whether states or private actors, are the customers.

The rapid cooling effect of SRM geoengineering is reversible. Therefore, SRM by aerosol manipulation risks 'termination shock' if deployment suddenly ceases (McCusker et al., 2014) – due to the relatively short lifetime of SRM aerosols (Irvine, 2015). The more sudden the termination of SRM, the greater the risks – as rapid climate change is a direct risk factor for the biosphere (MacMartin et al., 2014). Such a situation is potentially far more damaging than would be the case if geoengineering had not been commenced. Any security threats to SRM operations may therefore risk dangerous termination shock. The effects of termination shock differ over land and ocean, due to mass transfer in the mixed layer of the surface ocean.

Discussion of SRM in the literature primarily focuses on two scenarios: state provision or regulation (Ricke et al., 2013); and the rogue philanthropist (Victor, 2008) (aka 'Greenfinger'). Some limited discussion of alternative funding models can be found (Lockley, 2016b) (including the use of SRM for the creation of Voluntary Carbon Offsets (VCOs) (Lockley, 2016a). Our discussions below are applicable broadly – although we make specific comment on different potential providers, where relevant.

A considerable literature exists, concerning the role of climate change in conflict. This sub-discipline already benefits from broad-reaching systematic reviews (Hsiang et al., 2013), quantitative historical studies (Zhang et al., 2007), and analyses which drill down into individual risks (e.g. terrorism) (The CNA Corporation, 2007). The canon encompasses retrospective analysis of conflicts (e.g. Darfur (United Nations Environment Programme, 2007), Syria (Gleick, 2014; Selby et al., 2017), Nigeria (Sayne, 2011), Somalia (Maystadt and Ecker, 2014)), and discussion of potential future flashpoints – including consideration of nuclear war (Scheffran et al., 2016; Mian, 2016). However, much of the literature is focused on the role of a changing climate on the frequency, likelihood or preconditions for conflict (Scheffran and Cannaday, 2013; Scheffran, 2015; Christiansen, 2016;). Conversely, there has been comparatively little attention given to the risk of direct action (kinetic or otherwise) against climate-relevant infrastructure (save some research on the occasional direct-action civil society protests) (Schlembach, 2011). Paradoxically, conflict over fossil fuels (Caselli et al., 2015) is, of course, debated *ad nauseum*.

The study of geoengineering is a relatively nascent discipline, and formal reviews have identified significant weaknesses in the scope of extant analysis of the international relations aspects (Horton and Reynolds, 2016). Nevertheless, links between geoengineering and geopolitics (Yusoff, 2013; Dalby, 2015), and between geoengineering and conflict (Fleming, 2012; Maas and Scheffran, 2012; Link et al., 2013), have received attention (notably, this again includes a claimed potential role in triggering nuclear war) (Robock, 2015). Nevertheless, the specific risk of action (kinetic or otherwise) against geoengineering control systems and institutions; infrastructure; and hardware appears to have been given little, if any, academic attention. That potential flashpoint is the subject of this paper.

2 Discussion

Below, we extensively discuss hostile actors, threat types and defensive strategies, as relevant to SRM security.

We generally consider only aircraft-delivered SRM operations, while noting that other SRM technologies (Shepherd et al., 2009) and injections methods (McClellan et al., 2012) are available. However, we make brief mention of some other technologies, where these are particularly relevant. Furthermore, we consider only direct threats to operations – while noting that SRM may trigger wider hostilities, or even counter-geoengineering (the deliberate release of GHGs, in response to an SRM program) (Nightingale and Cairns, 2014). Issues of wider international relations are beyond the scope of our paper.

To constrain discussions, we consider only security issues relevant specifically to geoengineering. All normal organisations and operations face a range of non-specific threats (petty theft, fraud, hacking, etc.). Airports and airbases additionally have a well-understood range of security issues. Where these are not related to SRM operations, we do not discuss them in depth. Because of the highly heterogeneous combinations of deployment loci, actor identities and geopolitical backgrounds, we eschew formal analysis tools (threat matrices, etc.) which would be cumbersome to generalize so extensively. Instead, we take a discursive approach to the subject.

2.1 Threat actors and objectives

We consider a range of actors, with a potential interest in disruption of operations: Civil society protests (including social instability); terrorist groups; and states.

2.1.1 Civil society protests and social instability

Civil society protests are to be expected at the inception of an SRM program – due to the controversial nature of the technology. The extent and nature of these protests are entirely undetermined, with a wide envelope of potential scale and scope. Violence may occur, causing damage with high economic impact (Lancaster and Mulaudzai, 2016). Geoengineering activities have already attracted significant, often site-specific protests – which may have been a causal factor in shutting some down (e.g. SPICE (Stratospheric Particle Injection for Climate Engineering, 2018)) (Geoengineering Monitor, 2017). Bases are a natural location to concentrate protests (Kidron, 2013), but civil society groups often rely on numbers for effective protest. Isolated airbases may be not only difficult to reach, but may also be in locations incapable of practically supporting a sustained protest population: e.g. deserts, etc. Generally, consideration must be given to the political and social stability of countries of operation. A history of successfully managing any locally-common forms of civil protest, without resorting to brittle authoritarianism, is a desirable indicator for location selection.

A threat comparable to direct protest is social instability – considered here as a general disruption to law and order, continuously-functioning government, and the wider economy. This threat is distinct, in that it does not need to be directed at SRM operations to have an effect.

The local political environment is, therefore, a key consideration, in managing both types of threat. Japan, Switzerland, and Canada offer ready examples of major countries with high political stability (The World Bank, 2015). Nevertheless, none are located well for geophysical purposes (Australia is an obvious alternative, here). Many stable states are better located, but these are typically much smaller geographically and economically, and thus more vulnerable to external influence: Tonga, Mauritius, Kiribati, Macao, etc. Additionally, many are geographically-isolated, which may increase operational costs. The World Bank Index is not a solid proxy for suitability – with e.g. Israel scoring low, despite having an intuitively-capable situation and institutions for enduring strategic operations. The Marsh Country Risk Index (Marsh LLC, 2018) is another useful measure, which offers French Guiana (technically part of France – although in S. America, and notably home to a major spaceport), Chile and Malaysia as countries which combine relatively good location, with relatively low risk. A useful heuristic is to search for countries which (when adjusted for their economy and population) rarely make the global news – a bias to the boring. Notably, political stability indices are likely protective against both capricious governments and restive populations – each of which offers its own profile of threat to SRM operations.

Specific to SRM, it is not unrealistic to expect that protesters may direct their attentions to more accessible targets – such as the political hierarchy, or potentially to supply chain elements (BBC, 2008). Protests should, therefore, be expected at a variety of locations. However, these are much less likely to become an insurmountable major security issue than they are to remain a political risk. Serious disorder from environmentalists is rare, and organized terrorist violence is virtually unheard of. Nevertheless, the cost of security operations can be high (Highways England, 1998).

Cyberattacks may be expected as a part of a modern and sustained civil society protest (Raza, 2016) – although these are likely to lack sophistication. Doxing attacks (i.e. publishing confidential information on personnel, to compromise their privacy or security) (Quodling, 2015), Distributed Denial of Service (DDoS) (Kiruthika Devi and Subbulakshmi, 2016), etc. are likely to be the ‘weapon of choice’ – rather than the committed and sophisticated sabotage attempts necessary to materially directly disrupt operations (such as that seen in the Stuxnet attack on Iran) (Singer, 2015).

2.1.2 Terrorist groups

Terrorism (and, by association, counter-terrorism (Ugorji, 2017)) lacks precise, agreed definition (Greene, 2017) – but may include actions by both groups and lone actors (Pantucci et al., 2015). Terrorists certainly have the means to attack SRM operations. However, it is uncertain whether they possess the will. With exceptions (e.g. animal rights extremists (ADL, 2016)), modern terrorist groups often seek to act 'on behalf' of a race, religious group, or other populace. As a likely prerequisite for such terrorism, SRM would have to be seen (perhaps incorrectly) (CGG, 2016) as imposing a specific cost on a specific population that is sufficient to prompt such an attack. Of course, a terrorist group seeking to harm a country carrying out SRM operations for reasons unrelated to SRM could elect to attack its geoengineering facilities – but there is no obvious reason why this would be the chosen approach, particularly bearing in mind that the risk of termination shock is borne globally. Furthermore, other targets are far easier to hit – notably concentrations of people in urban landmarks and using public transport infrastructure. As time goes on (and the risk of termination shock thus increases) the likelihood of SRM being selected as a target of opportunity further diminishes – as there becomes an increasing likelihood that whichever group the terrorists claim to 'represent' will be harmed in equal measure to the population of the country operating or sponsoring the SRM operations.

However, should SRM be applied in such a way that a particular group could be identified (rightly or wrongly) as significant losers, attack risk may be elevated. Terrorists may be emboldened by the perceived injustice, and perhaps supported (or not actively opposed) by a wider group than may otherwise be the case. One might postulate, for example, a scenario in which North African Arab countries are perceived to be disadvantaged by a US SRM program. This resentment could inflame existing perceived discrimination, leading to disgruntled Arab sympathisers or established terrorist groups selecting SRM infrastructure or operations as a focus for attacks – perhaps as one facet of a wider campaign of hostilities.

Two inevitable facts serve to increase the likelihood of such attacks. First, while there may be a net global benefit from SRM, there will be relative winners and losers – both perceived and real. Secondly, these losses (real or imagined) will not exist in a political vacuum, and thus have the potential to inflame existing tensions (Nightingale and Cairns, 2014). Accordingly, a comprehensive defense against terrorism may include diplomatic efforts to ensure an equitable global settlement for SRM – including compensating relative or absolute losers.

Finally, it merits note that an extortionist or lone-wolf terrorist may launch or threaten a 'Dr. Evil' (New Line Cinema, 1997–2002) style attack on SRM operations – i.e. one conducted with no rational regard to the global negative consequences. Nevertheless, we regard such a scenario as inherently unlikely – the necessary combination of single-point vulnerability and concentrated personal power is almost certain not to exist. However, the above is not true for balloon-and-hose systems, which are particularly vulnerable.

2.1.3 States

In common with terrorist groups, states represent nations and peoples – albeit with acknowledged legitimacy, in most cases (Thomas, 1999). Accordingly, the same forces that may motivate terrorists to act to redress perceived inequities may also motivate states. However, states differ from terrorists in three obvious ways: They are more identifiable as coherent organisations; ordinarily more accountable to their peoples; and they are generally both more technologically sophisticated and economically capable. States are thus generally more able to muster the means for an effective attack; and yet they are generally more constrained in their practical ability to launch one (militarily, diplomatically, and politically) – as a result of their ability to suffer consequences in a backlash (sanctions, retaliatory strikes, etc.). This leads to a bifurcation into two potential types of state threat. First, an overtly-attacking state must be in a position of great strength (or great desperation). Secondly, even a weak state may be capable of mounting a covert operation, disguised as terrorism. Indeed, there is generally a fairly blurred line between state action and terrorism – with recent examples including Iran's Hezbollah (US Department of State, 2016) proxy and Russian 'volunteers' or 'little green men' (Shevchenko, 2014) in Ukraine. Multiple branches of a state may be capable of engaging in such actions (Kibbe, 2007), which may be carried out in contravention of the aggressor's domestic law prohibiting such actions (Kibbe, 2012).

2.2 Threat timings

The nature of an SRM program is such that, once incepted, it is difficult and disruptive to unwind quickly. This is largely due to the real risk of termination shock, but also because of the increasing operational and organisational robustness that comes from full establishment. Additionally, ongoing acquiescence to any given program tends to ultimately morph into tacit permission – which constitutes one form of social licensing process (as opposed to e.g. an explicit treaty). These issues make the start point of the program an obvious time for a threat to manifest itself. After a decade or so, the risk of termination shock is likely to outweigh any benefit to an opponent – even a disadvantaged one. However, it is not sufficient to assume rational behavior in this regard – and ongoing vigilance would be required. If the perception took hold (falsely or

otherwise) that SRM was not a public good (Morrow, 2014), then it may be seen simply as a high-profile and relatively soft target. In such circumstances, an opportunistic attack could result in significant environmental and economic damage, and a major public victory for the attackers (albeit perhaps a Pyric one). If, for example, a full-scale SRM program was deployed by balloon (Robock et al., 2009), its total destruction could be relatively easily achieved (by any moderately competent attacker able to gain access to the tether ground point). N.B. Security is one strong counter-argument against balloon-and-hose systems, unless they are built with significant overcapacity and redundancy.

Weather events blamed on SRM, or unrelated geopolitical matters, may similarly serve to trigger tensions to erupt. One later-stage attack scenario would involve geoengineering as a flashpoint to an existing geopolitical crisis. The idea that SRM is 'being done to us' could offer a lightning rod to existing concerns – as it may well be perceived as a violation of sovereignty, particularly to a state perceiving itself as a 'loser' (correctly or otherwise) (Whyte, 2012).

Furthermore, there is always a residual long-term risk of an isolated individual launching a cyberattack or terrorist operation – despite the risk of termination shock, and a lack of support from a wider community. Anders Breivik (Biography.com Editors, 2014) and the Unabomber (Biography.com Editors, 2017) are examples of such threats, which came largely as a surprise. Due to the potential irrationality or deliberate destructiveness of such attacks, there is no time horizon after which the threat from such individuals can be entirely discounted.

2.3 Threat loci

SRM has, by its nature, an extended supply chain. Unless carried out in an end-to-end secure environment (e.g. by the military), unsophisticated attacks are possible at a range of locations in the supply chain. Such attacks potentially include vulnerable, unconventional and highly-personal targets (Ward and Morris, 2006) – including worker's families. While militarisation of SRM has been discussed (Nightingale and Cairns, 2014), civilian models for operation have also been considered (Lockley, 2016). It should be noted that modern state functions are frequently outsourced to private firms, which may be far less secure than equivalent military-led counterpart operations. Pilots and staff (or their families); ground facilities and airstrips; aircraft; and logistics for fuel, spares, and the chemicals supply chain are all possible targets.

Airports and airbases tend to be reasonably secure locations, but the extended nature of the supply chain means that security is often difficult outside of the base. Personnel can, in extremis, be housed in secure accommodation – leading to a quasi-military environment. Supply chains are difficult to secure generally, unless logistics are exclusively by air, sea, or by protected road convoys. The cost of securing supply chains can be disproportionate to the cost of launching attacks. For example, occasional small arms fire can be enough to mandate permanent use of armoured vehicles and armed escorts. Even unarmed protestors can easily damage or obstruct vehicles, leading to severe disruption (Smith, 2015). Likewise, most suppliers will not have the preparations to enable any serious defense against targeted physical or cyber threats, and particularly those directed against staff. In extremis, a long-term pattern of attacks could mandate the construction of a secure supply chain – raising costs enormously.

Non-military aircraft in flight are, in principle, vulnerable. However, the range of threats is limited. Aircraft are generally reasonably well-protected against cyber attack (although successful attacks are not unknown (Norman, 2011)), and the range of possible actors capable of launching a kinetic attack on airborne aircraft is limited by the technological sophistication required (even man-portable guided air-defense systems are not commonly available to non-state actors). Furthermore, this technological sophistication makes tracing the hostile actor inherently easier than tracing a ground attack – thus tending to force any attack 'into the open'. This makes missile attacks on flying aircraft an option open only to desperate or powerful states. Nevertheless, even a one-off attack of this nature would be a clear act of escalation, which may serve an important political signaling purpose. Such a scenario could perhaps be most easily be envisaged were a less powerful state (e.g. Bangladesh) to attempt to geoengineer in defiance of a superpower.

There is, nevertheless, a potential threat to airborne aircraft from readily-available (and hence untraceable) simple weapons – but only when fired from close to the airbase. Commonly-available man-portable weapons, such as machine guns and RPGs, are only effective at very short range. Accordingly, keeping a significant secure zone beyond the runway is helpful in ensuring such attacks cannot be mounted. More sophisticated weapon systems, such as the SA-18 Igla, are much less widely available – and run a high risk of being traced to an attacking state.

2.4 Threat types

We consider a range of threat types: Kinetic attack; cyber attack; and civil protest. We consider (where appropriate) effectiveness, cost, likelihood, actors, and other criteria. The degree to which these threats are likely, or effective, will change according to the precise nature of the program's engineering choices – e.g. aerostats vs. planes, or MCB boats vs. SAI. Therefore, our analysis should not be seen as binding or definitive.

Before discussing individual threat types in detail, it is

worth considering the purpose of any attack. This may range from a simple protest – without serious attempts at disruption. Examples could include firing warning shots, or the symbolic destruction of non-critical assets (e.g. flagpoles). The next escalation would be an attack designed to cause temporary or symbolic loss of capability, so as to fully demonstrate destructive power – e.g. downing a single aircraft. Finally, an attack may involve the complete destruction of capacity, necessitating a comprehensive rebuild. This could include a simultaneous cyber-hijack of all aircraft (forcing them to crash), or simultaneous intensive bombing of all airbases and factories.

In all likelihood, any tactical attack would likely be backed up by a diplomatic strategy. Save for a willingness to engage in either repeated military action or an enduring military occupation, it would be unlikely that any determined geoengineering program could be permanently halted by hostile action. A country facing annihilation from rising seas would potentially be very determined in its efforts – and would likely garner considerable external support against an aggressor. Any attack is therefore likely to have the threefold aims of temporary interruption; an increase to cost and risk for the geoengineering country; and an attempt to force negotiations (either directly, or via a 'good cop' proxy nation).

2.4.1 Kinetic attack

The most obvious form of attack is kinetic – from bullets, bombs, missiles, etc. In principle, this threat type is serious – but a swift analysis of the likely behavior of potential hostile actors suggests that it is perhaps less probably than may be intuitively expected. Nevertheless, it is worth exploring the range of options open to a potential attacker. Airbases can potentially be directly attacked. However, they are likely to be located in friendly territory – typically beyond the range of naval guns. Accordingly, airstrikes (from planes or cruise missiles), or a clandestine/special forces attack are likely to be the only options. An airstrike would be such a provocative act that it would be likely only as an option for the most powerful actors (e.g. a superpower), or a desperate state facing a perceived existential threat.

A clandestine attack could be used against an airbase, and indeed terrorist/special forces (Winterman, 2011) attacks are typically considered a significant risk to airbases – which have long perimeters, low occupancy levels, and distributed assets within. However, there are other options for such an attack, which incur far less risk to the attacker – albeit lacking the spectacular nature of an airbase attack. The supply chain is the most obvious place to launch a kinetic attack – with road transport and civilian suppliers being particularly vulnerable.

Airborne aircraft are in principle vulnerable– particularly considering that practical flight plans will likely cross national borders or international waters, as injection patterns must straddle the equator (Kravitz et al., 2017), or be close to it (Kleinschmitt et al., 2018). It is unlikely that the tanker-type aircraft needed would be able to conduct any credible defense against kinetic attack, save for anti-missile systems (Staff, 2015). However, any attack may have to be carried out relatively close to the airbase – as the planes would be extremely high-flying (McClellan et al., 2012) (albeit perhaps for only part of their flight). Only the most capable ground-to-air or air-to-air systems would be capable of hitting them at operational altitude. Nevertheless, the regular flight locations and plans make airbase locations relatively vulnerable to shoulder-launched missiles (Millar, 2003). However, as discussed before capable missiles are likely to be traceable, as they are not widely available (Crile, 2007) – although attack attribution may not be without some degree of wriggle-room (Miller, 2016). The potentially limited geographic range needed for distribution means that air operations could be carried out entirely within 'friendly' territory – thus making a kinetic operation against aircraft essentially limited to an overt and risky military attack. The only exception to this near-invulnerability within friendly territory is a potential low-tech attack on or near the ground (which is predicated on close access, and therefore on poor base security).

2.4.2 Cyberattack

Cyberwarfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke, 2010). However, alternative definitions exist – which may be broader in scope (Arquilla, 1999). A range of different potential cyberattacks may be conducted. Examples include hijacking industrial controls, to execute the physical destruction of a system (Kelley, 2013); or less direct forms of attack, such as deletion of data or leaking of sensitive information. Personnel can also be attacked by means of doxing, if identification poses a risk to them.

Cyberattacks are a threat type available to a wide range of actors. Potentially all parties have access to cyberattack capabilities – from a lone-wolf activist or blackmailer, right up to a nation state (BBC News, 2007). The advantages of a cyberattack are myriad. Often inexpensive, they can be assembled and conducted in a clandestine fashion. The identity of the actors may be unknown – even after the event (Kelley, 2013). Furthermore, cyberwarfare even offers the opportunity to disguise the fact of the attack. For example, a plane can potentially be forced to crash (AFB, 2015) – but with the cause of the crash potentially disguised to look like an unrelated problem. This gives an attacker a substantial advantage when it comes to prolonging their capability to launch attacks.

2.4.3 Civil protest

Civil protest is multifaceted. It can manifest itself as lawful political and media campaigning; through disruptive but lawful public protests; up to significant or violent civil unrest (Schock, 2013; BBC News, 2000). The extent of this spectrum, and the range of possible actors and targets, are at the core of the difficulty of tackling this challenge. While it is not within the scope of this paper to address the 'threat' from political campaigning, we seek to address other aspects. Physical methods typical of civil protest include pickets, blockades, and (in some cases) rioting. This can raise security costs (Serck, 2016), disrupt operations, trigger the withdrawal of suppliers, and severely intimidate personnel. One possible solution to the risks of civil protest is to move facilities to remote locations, but that may simply divert the threat further up the supply chain. As with other physical threats, the road transport supply lines to airbases are a key vulnerability (Wilson, 2010). Unlike with kinetic threats, civil protests are likely to be concentrated at the gate – this being a prominent focus for pickets, protests and demonstrations. Civil protest typically aims to be as open and confrontational as possible, and the gate (or headquarters) provides the most obvious focus for this. The boundaries between civil environmental protest and criminality/terrorism are sometimes blurred (Maas et al., 2013). Additionally, the most capable civil protest groups are potentially able to launch sophisticated cyberattacks on operations, and others can deploy more basic cyberattacks on personnel (Quodling, 2015). Such supplementary attacks can be expected to be both synchronous and asynchronous with protests.

2.5 State *vs* private contractors

The use of private contractors is common as a way of discharging the responsibilities of a modern state. In such a situation, applied to SRM, it is to be expected that a contractor (if overtly employed) would have the full blessing and protection of the commissioning state. Indeed, a full operational and legal model exists from the military: Contractors on Deployed Operations (CONDO) (Moore and Antill, 2011). However, an alternative model exists – where private firms are fully responsible for the SRM process, and the state is uninvolved. The result of the latter relationship may be that the state's protection is supplied reluctantly, or not at all. For example, the responses of states to the threat of piracy on the high seas differ markedly – with the US offering an entirely uncompromising approach (Sheikh and Guled, 2009), as distinct from that of other flags. The degree to which a private SRM operator can expect security protection from the state depends on a range of factors, such as legality, personal connections to power brokers, physical location, etc. A detailed case-by-case evaluation would be needed, before conclusions could be drawn.

2.6 Legal protection

As a novel activity, it is possible that SRM may be subject to a range of legal challenges and uncertainties. While not a security threat as such, any doubts regarding the lawfulness of SRM offers an opportunity for cover for attacks – whether legitimate or otherwise. Similar doubts about the lawfulness of operations have been used by opponents of conventional (O'Shaughnessy, 1996) and nuclear weapons (Schlosser, 2015) to mount kinetic attacks on these systems. Furthermore, legal uncertainty may result in dithering by the state– under whose protection the SRM operation supposedly lies.

2.7 Ocean operation

One option for SRM operations is to host them at sea. Indeed, there is a precedent for controversial processes being conducted in international waters (Organisation for the Prohibition of Chemical Weapons, 2016). This approach renders the operation far more secure against civil protest or terrorism than would a land-based operation. However, unless conducted from a fully-protected military aircraft carrier (at great expense), the ability of states to move military assets freely into the theater of operations means that providing military security potentially becomes much more difficult – with submarine threats particularly difficult to anticipate, prevent or react to. Furthermore, the range of aircraft available for carrier-borne operations are greatly restricted – and special aircraft types may need to be developed to support this approach. A compromise strategy may be the conduct of operations from isolated island airbases (which are akin to large, moored aircraft carriers) – such as Diego Garcia or Ascension Island. The former offers a convenient, near-equatorial location (7 degrees south) – allowing access to both Northern and Southern hemispheres. An additional benefit of islands is that they have exclusive littoral rights – as distinct from carriers, which lack such a legal perimeter. They are also generally invulnerable to deniable submarine attacks; any submarine-launched cruise missiles are likely to leave identifiable fragments. Overall, ocean islands are therefore very attractive places to locate SRM operations.

One advantage of ocean operations is that location can be precisely controlled – set purely by scientific means, rather than working around the political and logistical considerations necessary when locating airbases. This has the potential to reduce flight times, and potentially chemical usage – thus controlling operating costs and (by reducing aircraft numbers) also capital costs. Accordingly, this offers a trade-off with the increased costs associated with ocean operations.

A brief mention is merited here of Marine Cloud Brightening (MCB) – although this is not generally the subject of this paper, it is taken seriously as an SRM technique. This may be carried out by autonomous drone

ships, which can operate using renewable energy for extended periods of time (Shepherd, 2009). This approach gives a range of inherent security advantages. The use of a large fleet of small ships means that a very comprehensive operation would be needed to destroy or disable them using kinetic operation, once they were deployed. Even finding and accessing them in a large ocean theater of operations would be very challenging. This strategy therefore, appears to offer inherent security advantages. However, there are also inherent disadvantages. The ships themselves are highly vulnerable to kinetic attack – unless designed with armour, a suite of sensors, and perhaps defensive weaponry that would dramatically increase their cost. Additionally, the use of a fully-autonomous system leaves a degree of vulnerability to cyberattack inherent– unless the ships were not subject to any direct remote control, or other remote systems access (an unlikely scenario). A variety of strategies are available to a potential cyber-attacker. Vessels could be programmed to ram each other; reverse their bilge pumps, causing them to sink; maneuver into storms or ice floes; shut down; falsely report activity and position; etc. One downside of marine cloud brightening is that termination shock would onset in a matter of days, should the system be interrupted – although this would be buffered by the ocean's heat capacity and mixing.

2.8 Defensive strategies

We consider the following defensive strategies: Redundancy; heterogeneity; overcapacity; inventory depth; logistics hardening; operation shrinkage; covert operations; cyber security; (counter) intelligence; physical security; and multilateralism.

2.8.1 Redundancy

Redundancy through replication is key to ensuring resilience – removing single points of failure. Balloon-and-hose systems are particularly vulnerable, in this regard – inherently being singular or few in number, and being of a highly-specialized type (i.e. one with replicated vulnerabilities). Even the provision of multiple entrance gates to an airbase is an important strategy to improve resistance to a variety of attacks (ambush; civil protest; sniping; etc.). The location of airbases in a globally distributed manner is likely to make good sense from an operational point of view, regardless of any security risk. Floods, storms, and civil disruption are a potential issue regardless of location – and a more distributed strategy engenders resilience (a doctrine known as 'Force Dispersal' (Dunnigan, 2003)). When added to this mix, security concerns add an additional reason to remove any single points of failure. Moreover, the benefit of having distributed airbases adds more security value than might perhaps be assumed – as air assets can potentially be redistributed at short notice.

2.8.2 Heterogeneity

An aspect of redundancy that can be regarded as a separate defensive strategy is heterogeneity. A distribution system that relies on any one technology, item of equipment, etc. has an inherent vulnerability. Security threats affecting one necessarily affect all – and this extends to more mundane issues, such as safety recalls.

2.8.3 Overcapacity

Beyond the strategy of reducing the presence of single points of failure, there is an additional need for a generalized overcapacity and/or redundancy (Liu et al., 2013) at most or all points in the system. Each system stage should ideally be operating at well below capacity. This helps to guarantee operational integrity in the face of a wide variety of issues – including security threats. There is both a direct and indirect (deterrent) effect in this regard. Any single points of failure are inherently vulnerable to an attack – risking the whole program. Furthermore, the presence of obvious redundant overcapacity makes hostile operations much less appealing – as even a successful attack may have little or no operational impact. For optimal results, a redundancy strategy should consider a variety of macroscopic geo-political threats. For example, locating airbases in countries with a range of political affiliations and economic situations may be helpful. For example, it is unlikely that South Korea, Cuba and Saudi Arabia will all experience closely-aligned economic, social and political shocks at the same time. Nevertheless, the selection of unstable countries is unlikely to be beneficial.

2.8.4 Inventory depth and resilience

The attractiveness of any attack tends to be influenced by the ability of such an attack to cause disruption and disablement of operations. Conducting an attack, especially on a long and poorly-defended supply chain, is likely to be relatively easy. However, sustaining any such an attack is likely to be difficult – as defenders can readily adapt to repetitious attacks. Accordingly, inventory depth (Lyons, 2014) and site resilience are key to sustaining operations. Strategies for achieving this are relatively simple. The most basic is keeping adequate supplies of fuel, spares and chemicals on deployment sites to 'ride out' an extended period of supply disruption – possibly of the order of years, for less readily-available inventory. Likewise, utility resources can be made resilient by the use of renewable site power, water boreholes, etc. Furthermore, the ability to house pilots and other essential personnel on site for extended periods of time not only adds resilience generally but also particularly reduces vulnerability to unsophisticated attacks. In addition, further resilience can be added in more imaginative ways: Simplifying inven-

tories, to reduce the range of items needing to be held; and having the capacity to improvise repairs using a machine shop or 3D printer, rather than waiting for deliveries. A tension exists between the benefits of reduced inventory complexity and the need to avoid homogeneity of equipment (for both type-approval and security reasons).

2.8.5 Logistics hardening

Extended or convoluted supply lines are vulnerable to a wide range of attacks from diverse actors (Bichou et al., 2013; Bichou et al., 2014). Additionally, they may experience an associated multitude of non-adversarial threats – resistance to which may be classed as resilience (Lam and Dai, 2015), as opposed to security. Accordingly, minimising the use of road transport offers both a strategic and tactical advantage. The main bulk supplies to an airbase, other than utilities, are fuel and chemicals. Major airports already benefit from pipelined fuel supplies, and similar facilities can be developed for importing chemicals (although sulfur needs to be melted for pipeline transport, or transported as a powder or compound). Buried pipelines are hard to trace and attack, and multiple filling points give redundancy. In extremis, supplies can be airlifted in. Notably, MCB does not rely on continual supplies of materials or (potentially) even fuel.

2.8.6 Operational shrinkage

Smaller operations give a smaller attack surface (Manadhata and Wing, 2004). For example, the use of drones will remove risks posed to and by aircrew. (Paradoxically, however, the freedom to attack without casualties may greatly reduce the political, legal and ethical hurdle for an attacker.) Likewise, the use of pre-programmed or artificial-intelligence-controlled flight routes will reduce the risks posed by communications jamming or hacking. Development of technologies that require lower chemical fluxes, fewer flights, etc. all give opportunities to further reduce the attack surface.

2.8.7 Covert or confidential operations

Covert operations (Daugherty, 2010; Downes and Lilley, 2010) are an established tool of warfare. There is no need for SRM operations to be overt. Aircraft used can be mingled with conventional traffic, and can use markings and flightpaths that do not serve to distinguish them. Furthermore, supply chains can be mixed up with a range of unrelated logistics flows – especially for non-bulk inventory, such as parts. This makes it not only more difficult to launch an attack, but also less fruitful. For example, destruction of a mixed load of road cargo would only result in a small amount of damage to an SRM operation. Any lack of dedication in operations greatly raises the risks of collateral damage – potentially alienating otherwise supportive or neutral factions, in the event of an attack. Consider, for example, the (flawed) suggestion of attaching SRM equipment to airliners (Laakso et al., 2012) (not in itself covert). Such a policy would greatly raise the stakes for any attacker – as can be seen from the tremendous difficulties that accidental 'shoot downs' cause for even the greatest powers (Kuypers et al., 1994).

One approach to making operations covert is to adapt the military principle of 'shoot and scoot' (US Army, 2014). In principle, an SRM aircraft can land at any ordinary airport. It can quickly be resupplied and relaunched, with a new crew if needed. In such a model, there is no 'base' of operations to attack. This style of operations may have a range of operational advantages, as well as reducing vulnerabilities to certain types of attack. For example, the ability to adapt flight plans to use inexpensive landing slots; and the potential cost savings available from avoiding the need for a permanent base. However, civilian airports are unlikely to accept any significantly increased security threat – which SRM operations may bring.

It is notable that covert operations can feed mistrust and conspiracy theories – as is abundantly evident from the persistent "chemtrails" conspiracy theory (Bakalaki, 2016; Cairns, 2016). There remains a significant difference between a program which is fully secret in nature, and one that is simply restricted in terms of operational detail. The latter is good practice, the former is unlikely to be sustainable in the long run. Governments are not good at keeping large-scale operations secret for long periods (Fenster, 2014).

2.8.8 Cybersecurity

Inevitably, providing a proper program of cybersecurity management (Kohnke et al., 2016) a necessary, but not sufficient, security response. Most cybersecurity comes down to simple good practice: ensuring mission-critical systems (e.g. avionics, process control (Macaulay and Singer, 2011; Instrumentation.co.za, 2007)) are kept separate from peripheral IT assets (e.g. website hosting); ensuring software is patched properly; firewall and anti-virus implementation; training staff on good security discipline; and (in extremis) air-gapping (Zetter, 2014) (completely disconnecting mission-critical IT from the wider internet). Nevertheless, it must be recognized that cybersecurity does not exist in isolation from other threats. A cyberattack (e.g. a leak of personnel files) may be the precursor to another attack type (e.g. kinetic attack, such as an assassination). In the case of more sophisticated cyberattacks (e.g. those with state sponsorship, or similar resourcing), a more sophisticated response is potentially required (e.g. a counterattack). Such interventions are outside the scope of this paper. Again, it must be recognized that the supply chain must be considered as carefully as the core operation.

2.8.9 Intelligence and counter intelligence

The major classes of intelligence (Keegan, 2003) are HUMINT (human sources – e.g. spies), IMINT (imaging intelligence – e.g. photography) and SIGINT (signals – e.g. phone taps). These are supplemented by other sources, such as OSINT (open source intelligence – e.g. websites), MASINT (measurement and signature intelligence – e.g. passive infrared detectors) and TECHINT (technical intelligence, e.g. weapon ranges). As should be obvious from the above, intelligence is a broad field – and generally beyond the scope of this paper. Nevertheless, briefly listing a few techniques is helpful in guiding further consideration of the subject.

Counter-intelligence (Prunckun, 2012) measures are an important way to deny an enemy the opportunity to mount an attack. Examples include:

a. Hide-from-view screens (IMINT). Simply obscuring bases from direct view helps prevent enemy imaging. This can, for example, prevent identification of personnel and targeting of weapons. The use of camouflage and decoys is a related technique.

b. Pseudo-random timetables (various). Regular operations allow predictability for an attacker. Preventing this prediction using randomness can help disrupt attack plans.

c. Concealing countermeasures (TECHINT, others as applicable). For example, keeping secret the existence of anti-missile Electronic Countermeasures (ECM) systems on aircraft.

d. Screening (HUMINT). Carefully screening operational personnel to ensure they do not pose a risk, either to operations (Sawer, 2015) or to security (Evans, 2015) is critical. Elimination of unnecessary job roles may be a superior approach to improved screening. Even designing-out the need for support staff (caterers, cleaners, etc.) can improve security, by reducing the attack surface.

e. Non-disclosure (OSINT). Placing unnecessary information into the public domain may result in an increased risk of attack. For example, listing staff names, building addresses, etc. leaves a trail of evidence that can be used to inform an attack.

Active intelligence operations may be incorporated into all SRM operations, as an essential part of security. In the case of civil protest, intelligence examples (provided for illustration, not as recommendation) include:

a. Infiltration of protest groups (HUMINT). This can be as simple as turning up to public meetings, or befriending/bribing sources.

b. Monitoring base perimeter (MASINT). For example, tracking the presence of mobile phones outside the base; using passive infrared detectors to detect intrusion attempts.

c. Photographing demonstrators (IMINT).

d. Perimeter-setting (TECHINT). Setting base perimeters to ensure that aircraft are clear of locally-available weapons.

e. Monitoring protestor communications (SIGINT/OSINT).

f. Monitoring protest group websites and general press activity (OSINT).

It should be borne in mind that, while passive counter-intelligence is routine, the same cannot be said for active intelligence gathering. Intelligence gathering on civil society is especially controversial – and the more invasive types are especially seen as being problematic. For example, CCTV on a base perimeter would widely be seen as reasonable – whereas trailing or bugging demonstrators is likely to be seen as far more controversial. General recommendations on intelligence gathering cannot realistically be made in the absence of an understanding of the particular threat landscape faced by an operator. As a final note, there is also the issue of public relations. If overt or suspected intelligence and counter-intelligence activities are seen as being a sign of imperiousness, then they may galvanise protest. Comparably, the arguable militarisation of policing is not without controversy and detraction (Hall and Coyne, 2013).

2.8.10 Physical defense

Physical defense must match the threat type. The less sophisticated the threat, the simpler the defenses capable of providing resistance. The simplest passive defenses (fences, walls etc.) are among the most effective, offering good protection against a range of intelligence and kinetic threats. While operations may be conducted from civil airports (which have their own security literature and processes (Sweet, 2009)), the use of military airfields or dedicated geoengineering airbases offer a general step up in security (at least in peacetime, in the case of military airfields). It is sensible to locate bases in areas that are both military secure (e.g. out of the range of naval guns), and sufficiently remote to be able to be easily screened from disruptive civil protest. As discussed earlier, the lower-sophistication attacks are the larger risk, and therefore a basic but robust defensive strategy is sensible. In general, the larger the area controlled around the airbase's operational core, the harder it is to effectively attack. A larger area means concentric fences can be used to increase security. Additionally, targeting basic weapons becomes far more difficult at increasing range. The need for physical defense may extend up the supply chain – which can be vastly more complex and expensive than securing a single site.

Depending on the degree of threat, and the degree of militarisation deemed acceptable, a range of active defenses may be used. These could conceivably include both ECM systems (e.g. communication jammers) and kinetic systems. Surface kinetic defenses may include anti-missile missile systems, such as Iron Dome; and gun systems, such as Goalkeeper and Phalanx (guns ordinarily cannot be deployed near civilians, due to the risk of

collateral damage). Operation from existing military bases makes such defenses available, without additional expense or policy concerns. Aircraft themselves can potentially carry jammers and flares, to confound inbound missiles. It is even conceivable that aircraft could be armed with air-to-air missiles, but this would serve to militarise the program. Any ship-borne operations may additionally have to monitor and defend against the threat from submarines – the existence of which would make operating within a military battle group essential.

2.8.11 A comment on multilateralism

Multilateralism's central principle is the "opposition [of] bilateral discriminatory arrangements that were believed to enhance the leverage of the powerful over the weak and to increase international conflict" (Kahler, 1992). Perhaps the most effective defense to a range of threats is a consensual, multilateral process. The more individuals, countries and groups feel that they are represented within the decision-making process (analogous both to procedural justice (Hough et al., 2013) and representative government (Barker, 2013)), the more that they are likely to feel they are best served by working with the decision-making system, rather than against it – they will tend to see provision of SRM as a public good, even if benefits are not homogeneous or even universal (as opposed to disruption of rogue SRM itself being seen as a public good). The distribution of operations, and of decision-making, across a range of actor countries may be the best way to demonstrate that communities around the world feel that they are 'part of the process' – be that through political or economic involvement. This bears comparison to a 'coalition of the willing' (Baum, M A, 2013; Johns and Davies, 2014). This may not be the least-cost option; and may increase the theoretical attack surface, albeit while generally improving redundancy. Nevertheless, the effect in defusing opposition may yield disproportionate benefits. Furthermore, the broader the coalition, the more powerful their collective military forces. Nevertheless, this approach is not without potential pitfalls, and a power bloc may emerge that can impose its will on others (Ricke et al., 2010). Appropriate institutional architectures for controlling the issues arising from this 'free driver' problem have been considered by other authors (Weitzman, 2015). While noting the importance of effective governance mechanisms, we note the broad scope of such investigation, and its active investigation by other authors. Accordingly, it falls generally outside the scope of this work.

3 Conclusions

We discuss a range of threat types, actors and vulnerabilities. While it is impossible to predict with certainty the security threats to SRM operations, we nevertheless make the following broad-brush observations:

We consider the threat type risks as follows:

a. Civil protest is almost inevitable – but is unlikely to pose any lasting material threat to SRM operations. It may, however, greatly increase operational difficulties and costs – especially around logistics. Furthermore, it opens operations to additional political pressure. Societal unrest is an overlapping, but indirect threat – which invites simultaneous scrutiny.

b. Overt military attacks on airbases or aircraft are possible, although unlikely. While the airbases and aircraft themselves may be vulnerable in principle, they are protected by the envelope of security offered by the state. The doctrine on non-aggression offers significant protection – and even powerful states are generally unwilling to carry out overt military attacks, especially on other capable states. Even private companies conducting SRM would reasonably expect to operate within the general envelope of a state's military security. The only likely attack scenario is a superpower aiming to 'teach a lesson' to a far less powerful state, which is permitting or conducting operations in ongoing defiance of the more powerful state's wishes.

c. Cyber attacks are highly likely, to the point of being inevitable. The key uncertainty is the degree of sophistication. While DDoS attacks, website hacking, etc. are to be expected, they are largely inconsequential. By contrast, process attacks (causing aircraft to crash, chemicals to leak, etc.) are far more serious. A lone wolf hacker, or protest group, may be capable of mounting such an attack. However, it is far more likely that such a sophisticated attack will come covertly from a state – or a party with similar resources. A robust program of cyber defense is therefore necessary throughout the supply chain.

d. Covert kinetic attacks – whether from quasi-terrorist groups, or from states – are a serious risk. The less sophisticated the attack, the better the cover offered by a wide range of potential culprits – making simpler attacks far more likely. Accordingly, physical and intelligence defenses should be concentrated on the simplest threats: small arms fire, arson, etc.

We consider the threat locus risks as follows:

a. Aircraft in flight have the least risk, in totality. They are, however, highly vulnerable to a determined military attack – should one occur. Good base security, and a large perimeter area will help prevent unsophisticated attacks on aircraft that are on or near the ground.

b. Bases and ground operations are somewhat vulnerable to kinetic attack; but are far more likely to experience low-grade attacks from civil protestors, such as blockades. Military bases have existing general defenses.

c. By far the greatest weakness is the supply chain, which necessarily includes chemicals, fuel, personnel and spares. This chain can be hit at any point by civil protestors, clandestine kinetic attackers, or cyberattacks.

While supply chain attacks may not cause a lasting service outage, they are nevertheless likely to cause very large cost increases and operational disruption. However, such attacks may lack the aesthetics and newsworthy nature of a direct attack on SRM-specific bases, aircraft, etc.

We analyze threat timings, concluding that the vulnerability is greatly elevated in the early stages of operation. Accordingly, an uneventful launch bodes well for a future free of attacks.

Nevertheless, we recommend the following defensive measures for SRM operations generally:

a. Basic physical security – ensuring bases and overt supply chain elements are given at least a minimum level of physical security. Relative remoteness (e.g. in deserts or on islands) and a politically-stable environment of operation offer significant advantages. An alternative strategy is to distribute operations widely throughout existing civilian infrastructure – diluting the value of any one target (this relies on the acquiescence of civil airport operators).

b. Redundant operations – replicating capacity in a number of locations, and with excess resources. This redundancy should be designed to ensure that similar threats do not tend to impact multiple assets at the same time. For this reason, we caution against the use of balloon-and-hose systems, particularly those with limited redundancy.

c. Heterogeneous operations – a heterogeneous supply chain should be used, ensuring that destruction or unavailability of materials, spares, etc. (or non-hostile safety and manufacturing issues) impact only a portion of operations. Combined with redundancy, this will prevent even a catastrophic loss of capability in one division, firm or system from reducing total capacity below a threshold level.

d. Resilient operations – for example: ensuring operations are sited in low-risk countries; that airbases are well stocked and capable of operating with disrupted logistics or access for extended periods of time; using well-proven equipment; selecting easily-defensible bases.

e. Cybersecurity – a generally vigilant approach to cybersecurity; in particular, ensuring that operational systems are appropriately separated (air-gapped) from publicly-accessible or peripheral systems.

f. Attack surface reduction – minimising the complexity of the operational program, to reduce the extent of the attack surface (e.g. using fewer flights) and the potential range of attacks that can be mounted (e.g. by switching pilots for drones).

g. Confidential, flexible operations – limiting the dissemination or predictability of information concerning operation greatly reduces the attack surface. Releasing flight times, supply schedules and personnel information (or allowing them to be observed or predicted) will greatly aid potential attackers.

Notwithstanding the above, we note that the best defense to all attacks is likely to be an inclusive, just, transparent and fair decision-making process. This reduces or removes incentives to attack.

References

ADL (2016). Ecoterrorism: Extremism in the animal rights and environmentalist movements. https://www.adl.org/education/resources/reports/ecoterrorism, 2016–5–15

AFB (2015). The ever-evolving cyber threat to planes. Security Week, https://www.securityweek.com/ever-evolving-cyber-threat-planes, 2016–2–05

Army U S (2014). Field Manual FM 3–09 Field Artillery Operations and Fire Support. United Sates Government. Washington DC: Department of the Army

Arquilla J (1999). Can information warfare ever be just? Ethics and Information Technology, 1(3): 203–212

Bakalaki A (2016). Chemtrails, crisis, and loss in an interconnected world. Visual Anthropology Review, 32(1): 12–23

Barker D W M (2013). Oligarchy or elite democracy? Aristotle and modern representative government. New Political Science, 4: 547–566

Baum M A (2013). The Iraq coalition of the willing and (politically) able: Party systems, the press, and public influence on foreign policy. American Journal of Political Science, 57(2): 442–458

BBC (2008). On this day- April 1, 1983: Human chain links nuclear sites. http://news.bbc.co.uk/onthisday/hi/dates/stories/april/1/newsid_ 2520000/2520753.stm, 2016–2–05

BBC News (2000). Animal rights, terror tactics. http://news.bbc.co.uk/2/hi/uk_news /902751.stm, 2016–15–05

BBC News (2007). Estonia hit by 'Moscow Cyber War'. http://news.bbc.co.uk/2/hi/europe/6665145.stm, 2016–2–05

Bichou K, Bell M, Evans A (2013). Risk Management in Port Operations, Logistics and Supply Chain Security. New York: CRC Press

Bichou K, Szyliowicz J S, Zamparini L (2014). Maritime Transport Security: Issues, Challenges and National Policies. Cheltenham and Massachusetts: Edward Elgar Publishing

Biography.com Editors (2014). Anders Behring Breivik biography. A&E Television Networks, https://www.biography.com/people/anders-behring-breivik-20617893, 2016–15–05

Biography.com Editors (2017). Ted Kaczynski biography. A&E Television Networks, https://www.biography.com/people/ted-kaczynski-578450, 2016–15–05

Cairns R (2016). Climates of suspicion: 'Chemtrail' conspiracy narratives and the international politics of geoengineering. Geographical Journal, 182(1): 70–84

Caselli F, Morelli M, Rohner D (2015). The geography of interstate resource wars. Quarterly Journal of Economics, 130(1): 267–315

Christiansen S M (2016). Climate Conflicts – A Case of International Environmental and Humanitarian Law. Cham: Springer

Clarke R A (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins

Climate Geoengineering Governance (CGG) (2016). What are the security implications of solar geoengineering? http://www.insis.ox.ac.uk/fileadmin/images/staff/Briefing_note_3.pdf, 2018–9–15

Crile G (2007). Charlie Wilson's War: The Extraordinary Story of the Largest Covert Operation in History. New York: Grove Atlantic

Dalby S (2015). Geoengineering: The next era of geopolitics? Geography Compass, 9(4): 190–201

Daugherty W J (2010). Covert action: Strengths and weaknesses. In: Johnson L K, eds. The Oxford Handbook of National Security Intelligence. Oxford: Oxford University Press

Downes A B, Lilley M L (2010). Overt peace, covert war? Covert intervention and the democratic peace. Security Studies, 19(2): 266–306

Dunnigan J F (2003). How to Make War. New York: HarperCollins

Evans R (2015). Lisa Jones, girlfriend of undercover policeman Mark Kennedy: 'I thought I knew him better than anyone'. The Guardian, https://www.theguardian.com/uk-news/2015/nov/20/lisa-jones-girlfriend-of-undercover-police-office-mark-kennedy-interview, 2016–2–05

Fenster M (2014). The implausibility of secrecy. Hastings Law Journal, 65(2): 309–360

Fleming J R (2012). Will geoengineering bring security and peace? What does history tell us? Sicherheit und Frieden/Security and Peace, 30 (4): 200–204

Geoengineering Monitor (2017). Resistance to geoengineering: A timeline, http://www.geoengineeringmonitor.org/resistance/, 2018–18–09

Gleick P (2014). Water, drought, climate change, and conflict in Syria. Weather, Climate, and Society, 6(3): 331–340

Greene A (2017). Defining terrorism: One size fits all? International and Comparative Law Quarterly, 66(2): 411–440

Hall A R, Coyne C J (2013). The militarization of U.S. domestic policing. The Independent Review, 17(4): 485–504

Highways England (1998). A34 Newbury Bypass Opens. Highways England Press Release, NB 348/98, 2016–15–05

Horton J B, Reynolds J L (2016). The international politics of climate engineering: A review and prospectus for international relations. International Studies Review, 18(3): 438–461

Hough M, Jackson J, Bradford B (2013). Legitimacy, trust and compliance: An empirical test of procedural justice theory using the European social survey. In: Tankebe J, Liebling A, eds. Legitimacy and Criminal Justice: An International Exploration. Oxford: Oxford University Press

Hsiang S M, Burke E, Miguel E (2013). Quantifying the influence of climate on human conflict. Science, 341(6151): 1235367

Instrumentation.co.za (2007). Resist cyber attack: Securing integrated SCADA systems. South African Instrumentation & Control. http://www.instrumentation.co.za/article.aspx?pklarticleid = 4736, 2016–2–05

Intergovernmental Panel on Climate Change (2013). Summary for Policymakers. In: Stocker T F, Qin D, Plattner G K, Tignor M, Allen S K, Boschung J, Nauels A, Xia Y, Bex V, Midgley P M, eds. Climate Change 2013: The Physical Science Basis. Contribution of Working Group I to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge and New York: Cambridge University Press

Intergovernmental Panel on Climate Change (2018). Global Warming of 1.5°C. In: Masson-Delmotte V, Zhai P, Pörtner H O, Roberts D, Skea J, Shukla P R, Pirani A, Moufouma-Okia W, Péan C, Pidcock R, Connors S, Matthews J B R, Chen Y, Zhou X, Gomis M I, Lonnoy E, Maycock T, Tignor M, Waterfield T, eds. An IPCC special report on the impacts of global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty

Irvine P (2015). Initial climate response to a termination shock. EGU General Assembly Conference Abstracts, 17

Johns R, Davies F A M (2014). Coalitions of the willing? International backing and British public support for military action. Journal of Peace Research, 51(6): 767–781

Kahler M (1992). Multilateralism with small and large numbers. International Organization, 46(3): 681

Keegan J (2003). Intelligence in War. New York: Knopf

Kelley M (2013). The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. Business Insider, https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11, 2016–2–05

Kibbe J D (2007). Covert action and the Pentagon. Intelligence and National Security, 22(1): 57–74

Kibbe J D (2012). Conducting shadow wars. Journal of National Security. Law & Policy, 5(2): 373–392

Kidron B (2013). The women of Greenham Common taught a generation how to protest. The Guardian, https://www.theguardian.com/uk-news/2013/sep/02/greenham-common-women-taught-generation-protest, 2016–3–05

Kiruthika Devi B S, Subbulakshmi T (2016). A comparative analysis of security methods for DDoS attacks in the cloud computing environment. Indian Journal of Science and Technology, 9(34)

Kleinschmitt C, Boucher O, Platt U (2018). Sensitivity of the radiative forcing by stratospheric sulfur geoengineering to the amount and strategy of the SO_2 injection studied with the LMDZ-S3A model. Atmospheric Chemistry and Physics, 18(4): 2769–2786

Kohnke A, Shoemaker D, Sigler K E (2016). The Complete Guide to Cybersecurity Risks and Controls. Florida: CRC Press

Kornneef J, Can Breevoort P, Hendricks C, Hoogwijk M, Koops K, Koper M (2011). Potential for biomass and carbon dioxide capture and storage. International Journal of Greenhouse Gas Control, 11 (2012): 117–132

Kravitz B, MacMartin D, Mills M, Richter J, Tilmes S, Lamarque J, Tribbia J, Vitt F (2017). First simulations of designing stratospheric sulfate aerosol geoengineering to meet multiple simultaneous climate objectives. Journal of Geophysical Research, D, Atmospheres, 122 (23): 12616–12634

Kuypers J, Young M, Launer M (1994). Of mighty mice and meek men: Contextual reconstruction of the Iranian airbus shootdown. Southern Journal of Communication, 59(4): 294–306

Laakso A, Partanen A I, Kokkola H, Laaksonen A, Lehtinen K E J, Korhonen H (2012). Stratospheric passenger flights are likely an

inefficient geoengineering strategy. Environmental Research Letters, 7(3): 034021

Lam J S L, Dai J (2015). Developing supply chain security design of logistics service providers: An analytical network process-quality function deployment approach. International Journal of Physical Distribution & Logistics Management, 45(7): 674–690

Lancaster L, Mulaudzi G (2016). You only listen when I'm violent. Institute for Security Studies, https://issafrica.org/iss-today/you-only-listen-when-im-violent, 2018–3–09

Lewis S (2016). The dirty secret of the Paris climate deal. Foreign Policy, https://foreignpolicy.com/2015/12/17/the-dirty-secret-of-the-paris-climate-deal-carbon-capture-negative-emissions-global-warming, 2016–3–13

Link P M, Brzoska M, Maas A, Neuneck G, Scheffran J (2013). Possible implications of climate engineering for peace and security. Bulletin of the American Meteorological Society, 94(2): ES13–ES16

Liu Y, Huang H Z, Wang Z, Li Y, Yang Y (2013). A Joint redundancy and imperfect maintenance strategy optimization for multi-state systems. IEEE Transactions on Reliability, 62(2): 368–378

Lockley A (2016a). Licence to chill: Building a legitimate authorisation process for commercial SRM operations. Environmental Law Review, 18(1): 25–40

Lockley A (2016b). Geoengineering: A war on climate change? Journal of Evolution and Technology / WTA, 26(1): 26–49

Lomax G, Workman M, Lenton T, Shah N (2015). Reframing the Policy Approach to Greenhouse Gas Removal Technologies. Energy Policy, 78: 125–136

Lyons D J (2014). The impact of inventory leanness and slack resources on supply chain resilience: An empirical study. Georgia State University, https://scholarworks.gsu.edu/cgi/viewcontent.cgi?article=1048&context=bus_admin_diss, 2018–9–26

Maas A, Bodó B, Comardicea I, Roffey R (2013). Global Environmental Change: New Drivers for Resistance, Crime and Terrorism? Baden-Baden: Nomos

Maas A, Scheffran J (2012). Climate conflicts 2.0? Climate engineering as a challenge for international peace and security. Sicherheit und Frieden / Security and Peace, 30(4): 193–200

Macaulay T, Singer B L (2011). Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. New York: CRC Press

MacMartin D, Caldeira K, Keith D (2014). Solar geoengineering to limit the rate of temperature change. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 372(2031): 20140134

Manadhata P, Wing J (2004). Measuring a system's attack surface. Carnegie Mellon University, School of Computer Science, https://www.cs.cmu.edu/wing/publications/tr04-102.pdf, 2018–3–09

Marsh L L C (2018). Marsh & McLennan Companies. http://www.marsh.com, 2018–9–18

Maystadt J F, Ecker O (2014). Extreme weather and civil war: Does drought fuel conflict in Somalia through livestock price shocks? American Journal of Agricultural Economics, 96(4): 1157–1182

McClellan J, Keith D W, Apt J (2012). Cost analysis of stratospheric albedo modification delivery systems. Environmental Research Letters, 7(3): 034019

McCusker K E, Armour K C, Bitz C M, Battisti D S (2014). Rapid and extensive warming following cessation of solar radiation management. Environmental Research Letters, 9(2): 024005

Mian Z (2016). Kashmir, climate change, and nuclear war. Bulletin of the Atomic Scientists. http://thebulletin.org/kashmir-climate-change-and-nuclear-war10261, 2017–7–10

Millar S (2003). Heathrow a soft target for missile attack. The Guardian, https://www.theguardian.com/uk/2003/feb/12/terrorism.world1, 2016–2–05

Miller N (2016). Malaysia airlines flight MH17 was shot down from pro-Russian rebel controlled territory, investigation finds. Sydney Morning Herald

Moore D M, Antill P D (2011). The use of contractors on deployed operations (CONDO) in the age of austerity. RUSI Defence Systems, 14: 32–34

Morrow D R (2014). Why geoengineering is a public good, even if it is bad. Climatic Change, 123(2): 95–100

New Line Cinema (1997–2002). Austin Powers franchise

Nightingale P, Cairns R (2014). The security implications of geoengineering: Blame, imposed agreement and the security of critical infrastructure. Climate Geoengineering Governance Working Paper Series: 018, http://www.geoengineering-governance-research.org/perch/resources/workingpaper18nightingalecairnssecurityimplications.pdf

Norman J (2011). Iran shows intact drone, boasts of cyberattack. CBS News, https://www.cbsnews.com/news/iran-shows-intact-drone-boasts-of-cyberattack/, 2016–5–15

O'Shaughnessy H (1996). £1.5M hawk attack women freed. The Independent, http://www.independent.co.uk/news/pounds-15m-hawk-attack-women-freed-1331285.html, 2018–03–09

Organisation for the Prohibition of Chemical Weapons (2016). Destruction of declared Syrian chemical weapons completed. Destruction of Syrian chemical weapons completed, 2016–2–05

Pantucci R, Ellis C, Chaplai L (2015). Countering lone-actor terrorism series no. 1: Lone act literature review. Royal United Services Institute for Defence and Security Studies, https://rusi.org/sites/default/files/201512_clat_literature_review_0.pdf

Prunckun H (2012). Counterintelligence Theory and Practice. Plymouth UK: Rowman & Littlefield

Quodling A (2015). Doxxing, swatting and the new trends in online harassment. The Conversation, http://theconversation.com/doxxing-swatting-and-the-new-trends-in-online-harassment-40234, 2016–2–05

Raza A (2016). 8 most awesome hacks conducted by Anonymous hackers. HackRead, https://www.hackread.com/8-most-awesome-hacks-conducted-by-anonymous-hackers/, 2016–2–05

Ricke K L, Moreno-Cruz J B, Caldeira K (2013). Strategic incentives for climate geoengineering coalitions to exclude broad participation. Environmental Research Letters, 8(1): 014021

Ricke K L, Morgan M G, Allen M R (2010). Regional climate response to solar-radiation management. Nature Geoscience, 3(8): 537–541

Robock A (2015). Cloud control: Climatologist Alan Robock on the effects of geoengineering and nuclear war. Bulletin of the Atomic Scientists, 71(3): 1–7

Robock A, Marquardt A, Kravitz B, Stenchikov G (2009). Benefits, risks, and costs of stratospheric geoengineering. Geophysical Research Letters, 36(19): L19703

Sawer P (2015). Andreas Lubitz: Everything we know about

Germanwings plane crash co-pilot. The Telegraph, https://www.telegraph.co.uk/news/worldnews/europe/france/ 11496066/Andreas-Lubitz-Everything-we-know-about-Germanwings-plane-crash-co-pilot.html, 2016–2–05

Sayne A (2011). Climate change adaptation and conflict in Nigeria. United States Institute of Peace. https://www.usip.org/sites/default/files/Climate_Change_Nigeria.pdf

Scheffran J (2015). Climate change as a risk multiplier in a world of complex crises. Planetary security conference, The Hague, https://www.researchgate.net/publication/284284909_Climate_Change_-as_a_Risk_Multiplier_in_a_World_of_Complex_

Scheffran J, Burroughs J, Leidreiter A, Van Riet R, Ware A (2016). The climate-nuclear nexus: Exploring the linkages between climate change and nuclear threats. World Future Council, https://www.worldfuturecouncil.org/wp-content/uploads/2016/01/WFC_2015_The_Climate-Nuclear_Nexus.pdf, 2018–18–09

Scheffran J, Cannaday T (2013). Resistance to climate change policies: The conflict potential of non-fossil energy paths and climate engineering. In: Maas A, Bodó B, Burnley C, Comardicea I, Roffey, R, eds. Global Environmental Change. Auflage: Nomos, 261–292

Schlembach R (2011). How do radical climate movements negotiate their environmental and their social agendas? A study of debates within the Camp for Climate Action (UK). Critical Social Policy, 31 (2): 194–215

Schlosser E (2015). Nuns and nuclear security. The New Yorker, https://www.newyorker.com/magazine/2015/03/09/break-in-at-y-12, 2016–2–05

Schock K (2013). The practice and study of civil resistance. Journal of Peace Research, 50(3): 277–290

Selby J, Dahi O S, Fröhlich C, Hulme M (2017). Climate change and the Syrian civil war revisited. Political Geography, 60: 232–244

Serck L (2016). Did the Newbury bypass tree-huggers change anything? BBC News, https://www.bbc.com/news/uk-england-berkshire-35132815, 2016–2–05

Sheikh A, Guled A (2009). U.S. Navy rescues captain, kills Somali pirates. Reuters, https://www.reuters.com/article/us-somalia-piracy/u-s-navy-rescues-captain-kills-somali-pirates-idUSTRE53A1LP20090412, 2016–2–05

Shepherd J G (2009). Geoengineering the Climate: Science, Governance and Uncertainty. London: The Royal Society

Shevchenko V (2014). “Little Green Men” or “Russian Invaders”? BBC News, https://www.bbc.com/news/world-europe-26532154, 2016–2–05

Singer P (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. Case Western Reserve Journal of International Law, 47(1): 79–86, http://heinonline.org/HOL/LandingPage?handle = hein.journals/cwrint47&div = 11&id = &page =, 2018–9–15

Smith G (2015). The day the troop trains came to Berkeley (first person). The Berkeley Daily Planet, http://www.berkeleydailyplanet.com/issue/2015-08-07/article/43569, 2016–5–15

Staff T (2015). Eilat-bound jets get anti-missile defense pods. The Times of Israel, https://www.timesofisrael.com/eilat-bound-jets-get-anti-missile-defense-pods/, 2016–2–05

Stern N (2006). Executive summary. In: Stern N, eds. Stern Review: The Economics of Climate Change. Cambridge: Cambridge University Press

Stratospheric Particle Injection for Climate Engineering (2018). The Spice Project, http://www.spice.ac.uk, 2018–9–15

Sweet K M (2009). Aviation and Airport Security: Terrorism and Safety Concerns. New York: CRC Press

The CNA Corporation (2007). National security and the threat of climate change. https://www.cna.org/cna_files/pdf/national%20security%20and%20the%20threat%20of%20 climate%20change.pdf, 2018–9–18

The World Bank (2015). Political stability- country rankings. The Global Economy, https://www.theglobaleconomy.com/rankings/wb_political_stability/, 2018–9–18

Thomas D G (1999). The Recognition of States: Law and Practice in Debate and Evolution. Westport, Connecticut: Praeger

Ugorji B (2017). Combating terrorism: A literature review. International Center for Ethno-Religious Mediation, https://www.icermediation.org/publications/combating-terrorism-a-literature-review/, 2018–9–18

United Nations Environment Programme (2007). Sudan post-conflict environmental assessment. http://postconflict.unep.ch/publications/sudan/00_fwd.pdf, 2018–9–15

United Nations Framework Convention on Climate Change (2014). Report of the conference of the parties on its twentieth session, held in Lima from 1 to 14 December 2014. http://unfccc.int/resource/docs/2014/cop20/eng/10.pdf, 2018–9–15

U.S. Department of State (2016). Chapter 3: State sponsors of terrorism overview. In: Country Reports on Terrorism 2016, https://www.state.gov/j/ct/rls/crt/2016/272235.htm, 2018–9–18

Victor D G (2008). On the regulation of geoengineering. Oxford Review of Economic Policy, 24(2): 322–336

Ward D, Morris S (2006). Jail for animal rights extremists who stole body of elderly woman from her grave. The Guardian, https://www.theguardian.com/uk/2006/may/ 12/animalwelfare.topstories3, 2018–3–09

Weitzman M L (2015). A voting architecture for the governance of free-driver externalities, with application to geoengineering. Scandinavian Journal of Economics, 117(4): 1049–1068

Whyte K P (2012). Now this! Indigenous sovereignty, political obliviousness and governance models for SRM research. Ethics, Policy & Environment, 15(2): 172–187

Wilson L (2010). Fifteen years since live exports divided Brightlingsea. BBC News, http://news.bbc.co.uk/local/essex/hi/people_and_places/history/newsid_8506000/8506735.stm, 2016–5–15

Winterman D (2011). SAS War Diary: the SAS secret hidden since World War II. BBC News, https://www.bbc.com/news/magazine-14952939, 2016–2–05

Yang P, Yao Y, Mi Z, Cao Y, Liao H, Yu B, Liang Q, Coffman D, Wei Y (2018). Social cost of carbon under shared socioeconomic pathways. Global Environmental Change, 53: 225–232

Yusoff K (2013). The geoengine: Geoengineering and the geopolitics of planetary modification. Environment & Planning A, 45(12): 2799–2808

Zetter K (2014). Hacker lexicon: what is an air gap? Wired.com, https://www.wired.com/2014/12/hacker-lexicon-air-gap/, 2018–9–18

Zhang D D, Brecke P, Lee H F, He Y Q, Zhang J (2007). Global climate change, war, and population decline in recent human history. Proceedings of the National Academy of Sciences of the United States of America, 104(49): 19214–19219