The Security Implications of Geoengineering: Blame, Imposed Agreement and the Security of Critical Infrastructure

Paul Nightingale & Rose Cairns

Climate Geoengineering Governance Working Paper Series: 018.

Originally published online 12 November 2014

This edition with minor revisions 13 February 2015

Climate Geoengineering Governance (CCG)

Climate Geoengineering Governance (http://geoengineering-governance-research.org) is a research project which aims to provide a timely basis for the governance of geoengineering through robust research on the ethical, legal, social and political implications of a range of geoengineering approaches. It is funded by the Economic and Social Research Council (ESRC) and the Arts and Humanities Research Council (AHRC) - grant ES/J007730/1

CGG Working Papers

The CGG Working Paper series is designed to give a first public airing to a wide range of papers broadly related to the project's themes. Papers published in this series may be, but are not necessarily, early outputs from the project team; equally they may be from other authors, and reflect different perspectives and different issues from those directly pursued by the project itself. The aim is to promote vigorous and informed debate, in a spirit of pluralism.

What the working papers have in common is that they will all be at an early stage of development, prior to full publication. Comment and response, at any level of detail, is therefore doubly welcome. Please send all responses in the first instance to the authors themselves - each paper contains a correspondence address. We will be looking for opportunities to use the website or other project activities to give a wider airing to any dialogues and debates that develop around a paper or issue.

About the Authors

Paul Nightingale (P.Nightingale@sussex.ac.uk) is Deputy Director of SPRU, at the University of Sussex, and a visiting Professor in the Strategy Group at Cass Business School. His research interests relate to the regulation of technology, change in large technical systems and biosecurity (dual use). Paul is a researcher on the Climate Geoengineering Project and works on the governance of geoengineering technologies, and the influence of governance practices on innovation and the application of geoengineering technology.

Rose Cairns (R.Cairns@sussex.ac.uk) is a research fellow at SPRU – Science and Technology Policy Research, at the University of Sussex. Her primary research interests are in environmental politics and governance, participatory research methods and discourse analysis, and the theory and practice of interdisciplinary research for sustainability. Rose completed her PhD on conservation politics on the Galápagos Islands from Leeds University in 2012. She also holds an MSc in Conservation and Biodiversity from Exeter University, and a BA in Social Anthropology from Cambridge University. Prior to her recent roles in academia Rose worked for a number of years in environmental campaigning and the voluntary sector.

The Security Implications of Geoengineering: Blame, Imposed Agreement and the Security of Critical Infrastructure

Paul Nightingale & Rose Cairns

Science and Technology Policy Research (SPRU),
University of Sussex

Abstract

The prospect of geoengineering in response to climate change raises a number of security concerns that have traditionally been understood within a standard geo-political framing of security. This relates to their direct application in inter-State warfare or to a securitisation of climate change. While direct military applications are unrealistic, indirect security implications are potentially significant. Current capability, security threats and international law loopholes suggest the military, rather than scientists would undertake SRM. SRM activity would be covered by Critical National Infrastructure policies, which would necessitate a significant level of secondary security infrastructure to protect them. Concerns about termination effects, the need to impose international policy agreement (given the ability of 'Rogue States' to disrupt SRM and existing difficulties in producing global agreement on climate policy), and a world of extreme weather events, where weather is engineered and hence blameworthy rather than natural, suggest these cost may well be large. Evidence on how blame is attributed suggest blame for extreme weather events may be directed towards more technologically advanced nations, (such as the USA) even if they are not engaged in geoengineering. From a security perspective SRM may well end up being very costly, and difficult to govern. These secondary security concerns are of a sufficient magnitude to suggest that questions can be raised about the viability of geoengineering (SRM) as a policy option.

1. Introduction

In recent years, as concern over climate change has increased, geoengineering has emerged as a policy option that is increasingly taken seriously (IPCC, 2013; Crutzen, 2006). While a range of technologies are captured by the category of geoengineering, only solar radiation management, and specifically stratospheric aerosol injection is generally accepted to be a technically feasible means of impacting on global temperatures in a relatively short time period, and hence is our focus here. Increased interest in geoengineering has been partly driven by perceptions that it offers a way of addressing climate change at a significantly lower cost than alternatives. However, these estimates of future costs have been criticized for their lack of realism as they only focus on direct costs (MacKerron, 2014). High fixed-cost, capital-intensive technologies like geoengineering are characterised by both significant uncertainties and cognitive biases that tend to under-estimate their future costs (ibid).

Major technical systems typically require extended secondary supporting technologies, systems, and governance structures which will only become apparent as technologies progress from imagined ideas to implemented real-world technologies. At present geoengineering remains an imaginary idea, not yet at the proof of concept stage, with an inherent danger that assumptions about its social impact will be biased. At early stages of technology development, expectations of costs are typically based on extrapolating from existing systems. This is subject to survivor bias, as most early-stage technologies fail, making the successes atypical and biasing perceptions of economic and social costs downwards.

Early stage evaluation of the social distribution of costs and benefits (risks and rewards) is therefore subject to very large uncertainties. Given the speculative nature of impacts, the approach of this paper is to highlight some previously overlooked indirect security concerns, and evaluate their magnitudes based on assumptions about the stability of security policy over the next 40 or so years. Doing so suggests the indirect economic and social costs of the security infrastructure that is likely to be needed to enable SRM will be considerable. This is based on four assumptions:

1. Rather than scientists being in charge of geoengineering, as is often implicitly assumed, the military are likely to play a significant role given current capability, the securitisation of climate change, perceived termination risks and loop-holes that exist in international legal frameworks that will constrain non-military developments. Given current

US security policy and doctrine it is unlikely that the US Congress would allow non-US control over geoengineering activity.

2. SRM activity would be likely to be classified as Critical National Infrastructure and subject to a range of security requirements that would potentially be very costly.

3. The costs of this security infrastructure would depend on its temporal scope, geographic scope, and level of intensity. The temporal scope could potentially be many hundreds of years. The geographic scope could be global given the limited political ability of governments to agree on climate change policy and the ability of 'rogue' States to easily counteract any geoengineering efforts. The intensity could be very high because of perceptions of risks from the termination effect, and if geoengineering is imposed and subject to resistance, particularly if that resistance takes a violent form and is directed towards soft targets.

4. The intensity of global security provision is likely to be further increased given the inevitable extreme weather events that will occur around the world during its operation. Once SRM is in operation these will often be seen as engineered outcomes rather than random events, and hence subject to a moral calculus of blame. Individuals and groups may take revenge against the citizens and interests of the States perceived to be involved.

Together these four assumptions suggest that the magnitude of the social and economic costs of security for geoengineering may well be very high, and arguably significantly higher than the direct costs. The political costs may also be very high given the combination of security concerns and in a worst case scenario could imply a dystopian future. A worst case scenario is unlikely, and could easily be avoided, but its existence suggests a broader analysis of the costs of SRM would be useful to inform policy making.

2. Direct and Indirect Security Concerns

In discussing security implications of geoengineering it is important to clarify some key distinctions and terminology in order to avoid conflating the distinction between hostile and peaceful activities with the distinction between military and civilian activity. War is organised violence

threatened or under-taken for political purposes. War reflects a relationship between belligerents, who are not necessarily states with organised military forces (Gray, 2010: 37). Warfare is the conduct of organised violence in war, and typically carried out by militaries, but also by non-State actors (Kaldor, 2000). Military activity however also includes a wide range of activities that are not hostile (for example, transportation, medical care and logistics). Security is a state of being free of danger or its threat, and hence has dimensions related to who is free of the threat - traditionally States, but increasingly individuals - and what those threats are - traditionally military hostility but increasingly non-military threats such as climate change.

Military capability can address threats both directly and indirectly (for example through deterrence) and can be applied to protect different kinds of actors from a variety of threats. Technologies that underpin these military capabilities can in some instances be dual use. In the arms control arena, dual use refers to the features of technologies that enable them to be applied to both hostile and peaceful ends with few or no modifications (Molas-Gallart and Robinson, 1997) while in the economic sphere it applies to technologies that can be applied in both military and civilian settings.

Given these distinctions it should be clear that the security implications of geoengineering go beyond direct application of dual use geoengineering technologies for hostile activity within a war setting. If geoengineering technologies worked, they could potentially be used by the military for non-hostile activity, for example in humanitarian interventions. Moreover, the security implications of geoengineering also address how it might mitigate or enhance wider threats. Indirect security concerns cover both the security infrastructure that would be needed to protect geoengineering projects from external threats, and the security concerns that this security infrastructure might itself endanger. In the next two sub-sections we contrast direct and indirect security concerns.

2.1 Direct Military Use

Interest in the direct military use of geoengineering and other weather modification technologies has a long history (Fleming, 2006; 2010), going back to Francis Bacon's prediction that one day science would allow control of the weather (1606). Langmuir's discovery in the 1940s that

silver iodide could be used to seed clouds generated a range of military projects, which expanded considerably in the 1950s with military backing. In 1958 the NSF became the lead agency for research into weather modification.

The 1950s were characterised by a shift in the scale at which military planners and weapons developers thought, generating suggestions for approaches to military engagement with global impacts. Of these nuclear weapons remained the most viable, particularly mass air-burst weapons with the potential to generate firestorms that would have a global impact. However, there was interest in using cloud seeding techniques to address natural threats, such as hurricanes. This, for example, was addressed in project Cirrus which ran from 1947 to 1952 (Havens, 1952).

While there was considerable interest in the military application of weather modification, the technology was plagued by uncertainty about its impact. The inherently unpredictable nature of the weather made it impossible to predict counter-factual outcomes of what the weather would have been like without an intervention. Hence it is impossible to robustly assess the impact, or lack of impact, of weather modification measures. For example project Stormfury, funded by the US Navy and US department of Commerce ran from 1962 to 1983, and attempted to modify hurricanes using cloud seeding techniques. The impacts were inconclusive because of the difficulties of determining the effects caused by the treatment in the absence of a solid understanding of outcomes under the counter factual untreated scenario (Cairns, 2014; Willoughby et al. 1982, p.411).

Nonetheless, the US military applied such techniques during the Vietnam War and operated a secret cloud seeding program, codenamed Popeye, over North and South Vietnam, Laos and Cambodia from 1967 to 1972. The aim was to extend the rainy season and disrupt the flows of logistics along the Ho Chi Minh trail by flying over 2,600 cloud seeding sorties using 47,000 silver iodide flares. Trials of Popeye began in Laos in 1966 and were extended in the 'Motorpool' operational phase in 1967 (McLeish, 2014). The operation was exposed by Jack Anderson in his Washington Post column in 1971, followed by an article in Science in June and then in 1972 an extended article by Hersh (1972) in the New York Times.

The exposure led to a Senate investigation, the unilateral decision by the US to renounce the military application of climate modification techniques in 1972 and the passing of a resolution urging President Nixon to begin international negotiations to ban the practice. This eventually led to the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD), negotiated in parallel with the SALT negotiations. Bilateral discussions started in 1974; identical texts were issued in 1975, which were finalised on the 10th December 1975. ENMOD entered into force on 5 October 1978 and prohibits the hostile use of environmental modification techniques that have widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party.

The legal ban on the use of weather modification techniques for hostile (but not peaceful purposes) in the Treaty, as well as the limited effectiveness and significant uncertainty about whether such techniques have any meaningful impact, have lessened military interest in weather modification. Funding fell to $500,000 by the 1990s, but in 2003 the NRC (2003) called for increased research, and in 2008 the Department for Homeland Security convened a workshop on weather modification to address national security threats (i.e. hurricanes).

While weather modification programmes remain extensive in China (Xueliang, 2009; Edney, & Symons, 2013), in the West there is limited practical military interest given the uncertainties involved and the existence of cheaper, more effective solutions to all the potential applications of weather modification techniques in a military setting. In the 1960s unguided munitions were extremely inaccurate and muddying up the Ho Chi Minh trail with additional rain may have seemed a viable option. Today with guided munitions, battlefield surveillance and improved vehicles, the application of weather modification seems a quaint historical dead end.

Despite this lack of interest, increased attention to geoengineering in the scientific community has seen an increase in the attention given to the military use of weather modification techniques on a greater than local scale (Foreign Affairs, 2012). Such applications are banned by an international convention, have limited military use (Briggs, 2013) given the inherent unpredictability of weather systems, (caused by the laws of physics and hence not amenable to change by technology), and compete

against cheaper, more effective alternative means of achieving the same military ends. [1]

3. Indirect Security Implications

While the direct relevance of solar geoengineering to security settings is probably minimal (despite significant funding) the indirect security implications may well be considerable. A first point to highlight is that the widespread assumption that geoengineering will be undertaken by scientists is questionable. Instead there are a number of reasons for thinking that the military rather than scientists will run solar geoengineering projects.

The first reason relates to capability, and the experience the military has of running large complex technical projects. Existing weather modification programmes in China for example exploit artillery and rockets, both technologies with military applications that are under the PLA's control.

A second reason relates to the increasing securisation of climate change policy, where geoengineering is seen as a solution to a wider climate change problem which is itself framed as a security problem. For example the UK MOD, the UN (2007; 2011), the RUSI and the US (CNA, 2007) see climate change as a security threat (see also Campbell, et al 2007; Clapper, 2014). The underlying assumption is that climate change can destabilize weakened and failing governments, leading to conflicts, mass migrations, ethnic tension and extremism (see Homer-Dixon, 1991, and in a more apocalyptic tone Kaplan 1994). However, the supposed direct links between scarcity and insecurity are more complex and context dependent than this literature suggests (Eastin, et al 2011) making the link to geoengineering unclear. A related body of research frames the security threat of climate change in terms of human security rather than traditional inter-state security, arguing that geoengineering may be a responsible approach to address the security threats to individuals posed by major changes in climate. In each instance a security framing directs policy implementation towards military settings.

A third reason relates to exemptions and sovereign immunity clauses based on national security concerns in international law. These provide

[1] For a related argument see

ways of avoiding legal constraints on geoengineering activity that would apply to non-military activity.

A fourth reason relates to current US security policy and doctrine, whereby it is extremely unlikely that Congress would approve the development of geoengineering systems under United Nations or other international organisations control. Moreover, given the perceived risks of a potential termination effect, it is also unlikely that Congress would accept another State, such as China, or group of States, such as the EU, producing technological systems whose failure could pose a catastrophic risk to the US.

Since the 1950s US foreign policy has been characterised by a set of norms that sees the US as taking a leadership role in security matters, with a unique responsibility for deciding and enforcing those norms (Bacevich, 2010). These norms are enforced through a mix of soft and hard power, with the US negotiating from a position of strength based on a level of distributed military resources, structured for interventionist global power projection, far in excess of all other nations combined. US military policy divides the world up into unified commands Pacific, Central, European, Africa, Southern, Northern, Space and Strategic - structured for intervention and acting to prevent the emergence of competing powers in any region. A key part of this, involves acting to prevent the development of military capabilities that might threaten US interests, by States unaligned with US norms.

In the security domain, perceptions of threats, which can be highly uncertain and unlikely, play important roles in policy. The perceptions that geoengineering would create a potential doomsday device, which if stopped would rapidly lead to a catastrophic 'termination effect', could easily be perceived to present a threat to US security. Under such circumstances it would be reasonable to assume that there would be considerable US security interest and a desire to have it under US security control or at least subject to considerable oversight. The notion that North Korea, Iran, Russia, China or even the EU could develop a geoengineering capability without generating concern in Washington is unrealistic.

Lastly, given the perceived (or constructed) risks of termination, geoengineering is likely to be geographically distributed to spread risks. This again suggests military involvement, particularly given the geographic scope of US military assets and the ability of military

organisations to ease deployment because of their exemptions to legal restrictions on international action.

3.0.1 Critical national infrastructure

Even if the military are not directly involved in stratospheric aerosol injection related geoengineering activity, they are likely to take a security interest in it. Geoengineering, if carried out, we be classified as Critical Infrastructure, defined as "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, across any Federal, State, regional, territorial, or local jurisdiction" (NIPP, 2013, see also Critical Infrastructures Protection Act, 2001).

Currently policy to secure infrastructure was set up in the Homeland Security Act of 2002, Critical Infrastructure Security and Resilience and is outlined in NIPP 2013: and upgraded in Presidential Policy Directive 21 (PPD-21), Partnering for Critical Infrastructure Security and Resilience. It involves managing risks in a partnership between "owners and operators; Federal, State, local, tribal, and territorial governments; regional entities; non-profit organizations; and academia" using an integrated approach to "Identify, deter, detect, disrupt, and prepare for threats and hazards", reduce vulnerabilities, and mitigate consequences (NIPP 2013, page 1).

The main focus on threats relates to terrorism, pandemics, cyber attacks, extreme weather and accidents or technical failures. These are understood using a traditional "threat, vulnerability, consequences" framework. Within this framework threats relate to "natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property" (NIPP, 2013 pg. 17). These are then prioritized in relation to how vulnerable infrastructure systems are to them, and what the consequences might be if those vulnerabilities were exploited.

Consequently, assessing the security requirements for geoengineering infrastructure requires assessing vulnerabilities and consequences. In relation to consequences these are large as the termination effect presents a major threat. Once geoengineering was in place for decades, stopping the activity could lead to a rapid increase in global temperatures,

which in turn could lead to significant environmental impacts that would threaten not just US economic interests, but the survival of its society (Jones et al 2013). On a consequences ranking, geoengineering would score highly, and would require comprehensive risk management that mapped out and explored vulnerabilities in the elements of the wider technological systems it was embedded in. Moreover, given the systems would have to operate for many hundreds of years, a larger set of environmental and systemic uncertainties and 'unknown unknowns' would likely be explored.

Moving to vulnerabilities, it may be the case that direct vulnerabilities would be no more than those faced by a traditional military facility and could be managed in the same way. Resilience to catastrophic failure could be built in through redundancy, replication, backup facilities etc. It is hard to see how any direct threats could not be managed by organisations that are capable of dealing with the protection of nuclear weapons.

However, geoengineering activity is very vulnerable to counter-measures. For example, if a country disagreed with either geoengineering or the end-points that the climate was being geo-engineered to it could easily disrupt existing programmes. For example, Russia may disagree with India about what temperature rise should be aimed at and both might disagree with the USA. Russia might then disrupt geoengineering efforts by venting methane into the atmosphere from oil and gas deposits, or by releasing greenhouse gases, which could be done in ways that would be potentially difficult to detect. The scope of surveillance to deter, detect and prevent this activity could therefore potentially be extremely large and costly as it would have to cover not just existing political actors but also political actors that may emerge in the future.

The costs of security would rise with the extent to which geoengineering measures were imposed because of failure to agree globally. We have already mentioned the potential for regional tensions about end points, and the need to constrain countermeasures, but the implementation of geoengineering would require either a degree of international agreement or unilateral implementation and imposition. Given the very limited ability of the global community to agree on climate policy, it is not clear that a consensus will emerge. The impacts of geoengineering activity on local weather is extremely poorly understood (Trenberth and Dai, 2007) including on local precipitation patterns (Hegerl and Solomon, 2008;

Ferraro, et al 2014). States' activity under conditions of uncertainty will be subject to moral hazard and reaching agreement will be potentially costly. It is unfortunate that a plan to deal with a failure to achieve a global climate policy consensus, itself requires a global climate policy consensus that will be arguably more difficult to achieve.

If global consensus on end points and governance cannot be achieved, questions arise about the extent to which countries can veto activity that will directly influence their climate. Would countries be ignored? Particularly given their ability to use countermeasures. Would geoengineering be imposed on parts of the world without their agreement or in direct opposition to their clearly expressed preferences? If so, the security threats to geoengineering activity would be higher and the scope and intensity of security infrastructure would increase. Implementing geoengineering under such conditions will increase the social and political commitment required, which, in turn, has the potential to generate lock-in to costly governance structures and security infrastructure (Rayner et al 2013).

3.0.2 The geography of blame

A key influence on potential threats relates to the number of people, organisations and States that wish to disrupt geoengineering and the intensity of those aims. A key issue that has been often overlooked in geoengineering debates is how geoengineering might itself change people's feelings towards it. Extreme weather events can be very disruptive, but are currently seen as naturally occurring and therefore outside the moral calculus of blame. However, if the climate is being engineered, then weather may cease to be seen as natural, and instead be seen as the result of deliberate interventions. If this is the case, it becomes blameworthy.

Given it is likely that extreme weather events will continue and possibly increase with climate change, this opens up the risk that any extreme weather event will be seen as a consequence of intentional action by States that engage in geoengineering. This will be the case even if the consequences are unintended. Since the same uncertainty about weather patterns that makes the effectiveness of weather modification techniques very difficult to establish will apply to the calculus of blame, there is no clear baseline for establishing the counter factual outcomes that would

have occurred had geoengineering not taken place and indeed that make it impossible to attribute any given extreme weather event to anthropogenic climate change (c.f. Pielke Jr. 2010, chap.7). This raises the potential scenario where every extreme weather event and its consequences are blamed on the States involved in geoengineering activity.

Aggrieved parties that seek revenge on the States involved will find it very difficult to disrupt geoengineering activities directly, as noted earlier, and may therefore vent their anger indirectly. For example, anger could be vented at the citizens or economic assets of the countries involved. The additional costs of protection on a global scale could therefore be very large, very quickly. If climate change ends up generating large impacts on peoples' livelihoods, it is not inconceivable that over the next few hundred years a politics of climate might emerge, that in turn may have violent fringes.

There is an additional concern about the geography of blame, relating to its mismatch with action. When people assign blame they do so within socialized normative frameworks, with blaming activity providing a public display and reaffirmation of those frameworks. Such frameworks rarely match the complexity of the underlying causes. For example, rather than recognize the complexity of systemic technical failures, society seeks scapegoats and blames individuals. Blaming affirms a hidden moral reality behind the appearance of social life and as a result links to trust, normative frameworks, social structures and specific local, temporal concerns. In practice this can link back in a chain to more fundamental causes. For example, a disaster can be attributed to the actions of a local group, but their actions in turn can be attributed to a more powerful and sinister set of forces. This does not necessarily match the underlying causality at work. For example, currently in the Middle East blame is attributed to other groups, who in turn are seen as agents of other powers such as Israel and the USA, rather than other nations that are much more directly involved.

Under such conditions the security consequences of engaging in geoengineering, in a world subject to extreme weather events, for States would be extremely high. Moreover, for some States such as the United States, which are seen to have superior technological capabilities and global influence, that blame may be applied and acted upon, even if the USA does not engage in geoengineering. Put crudely, if the USA decides

not to engage in geoengineering and the EU does, the US may well get the blame if things go wrong. Moreover, it may be blamed for the consequences of extreme weather events around the world it had no influence over.

Even if no-one engages in geoengineering there is a significant proportion of the population who will believe it is ongoing anyway (Cairns, 2014b), who often blame the US government, and the sinister hidden organisations they believe are controlling its actions. While these individuals are not part of the current mainstream geoengineering debate, they should not be dismissed. Currently, some 14% of the population by some polls expresses a degree of agreement with the idea that the climate is being covertly manipulated for nefarious ends. It may be unrealistic to assume that these suspicions will not increase if solar geoengineering is introduced.

4. Conclusion: Avoiding Dystopian Futures

Given the very early stages of SRM research, and hence the lack of clarity about its development it is important to highlight the uncertainties involved in any analysis of future impacts. Caveats should be highlighted, and it is logically possible that none of these security concerns will arise. It may be the case that the world will agree on a framework for geoengineering activity and no country, group or individual will dissent. Similarly, the US Congress may accept the deployment of a climate modification system under the control of international organisations and subject to UN control even though they pose a potentially catastrophic threat to the US. Political authorities may decide geoengineering systems are not Critical National Infrastructure, or do not require extensive security oversight. Moreover, there may be global agreement with these actions such that security concerns are minimized. Social science research on blame may be wrong and rising education levels may make the allocation of blame more 'rational'. Under such circumstances scientists can get on with engineering the climate and not worry about the costs of indirect security.

However, given the failures of States to agree on climate policy, the concerns raised about having US military dog training teams under UN control, the stability of existing security frameworks and policy, and the existing concerns about the social distribution of risks and rewards of

geoengineering activity, it may be wise to be cautious. In a worst case scenario, where geoengineering is unilaterally deployed without agreement and therefore imposed on an unwilling world that is increasingly paranoid about extreme weather, the security infrastructure required would be substantial. At the extreme it may require a global system of surveillance and extensive interventions to protect soft targets around the world in a political climate where the impact of every hail storm and flood was being blamed on the States perceived to be undertaking geoengineering. The costs of such an infrastructure would not just be measured in percentages of GDP, but also in political terms as they would require substantial changes in political structures and engagements both internationally and at home. In a worst case scenario, global threat suppression would have to be undertaken for centuries, would be likely to be subject to secretive, bureaucratic decision-making under conditions of uncertainty, and could take place in a world subject to paranoia, blame and confrontation over climate outcomes. Such an outcome is clearly not inevitable, but would be very dystopian.

Given these concerns, the widespread assumption that SRM would be undertaken by scientists and its indirect security impacts will be inconsequential is questionable. Similarly, the implicit assumption that achieving agreement over global governance would be easy is questionable, as achieving stable, global agreements about security issues is notoriously difficult. Current experience suggests it may well be impossible, and the deployment of geoengineering would have to be imposed, possibly without the consent of all nations, and almost certainly over the objections of political groups. While the direct security impacts of geoengineering, through its use in military contexts or for the protection of facilities are likely to be slight, the indirect security impacts may well be much larger. Based on a series of assumptions that security policy changes slowly, that agreement on climate outcomes will continue to be difficult, and that geoengineering will make weather events blameworthy, the potential security costs may be large. Any security threats could in theory be suppressed on a global scale, but the political and economic costs of doing this over centuries would be significant.

The currently widespread assumption that solar geoengineering will be undertaken by agreement, by the scientific community, that it will be easily governable and subject to effective democratic oversight on a global scale, and then not have any adverse security consequence, may

turn out to be unrealistic. Instead, while it is hard to predict the future, it is hard to avoid the conclusion solar geoengineering is likely to be difficult to implement, raises questions about effective governance (and may well be ungovernable as suggested by Hulme, 2014), and has the potential to have very costly social and economic consequences. These social consequences may well be of such a magnitude as to make SRM untenable as a low cost solution to climate change. In worst case scenarios, they may turn out to be so high as to make SRM it untenable as a policy option."to make it untenable as a policy option.

References

[1] Briggs, C. M. (2013). *Is Geoengineering a National Security Risk?* Geo-engineering Our Climate Blog Available at: http://wp.me/p2zsRk- 8U

[2] Cairns R (2014) *Will solar radiation management enhance global security in a changing climate?,* CGG Working Paper 16.

[3] Cairns, R (2014b) *Climates of Suspicion*, CGG Working Paper 9.

[4] Campbell, et al (2007); Campbell, B.K.M. et al., (2007). *The Age of Consequences : The Foreign Policy and National Security Implications of Global Climate Change.*

[5] Clapper, (2014). Worldwide Threat Assessment of the US Intelligence Community, Washington

[6] CNA (2007). National Security and the Threat of Climate Change, Available at: securityandclimate.cna.org.

[7] CNI (2013)

[8] Eastin, J., Grundmann, R. & Prakash, A., (2011). The two limits debates: _`Limits to Growth'_ and climate change. *Futures*, 43, pp.16_26.

[9] Edney, K., & Symons, J. (2013). China and the blunt temptations of geo-engineering: the role of solar radiation management in China's strategic response to climate change. *The Pacific Review*, (February 2014), 1_26. doi:10.1080/09512748.2013.807865

[10] Ferraro, A.J., Highwood, E.J. & Charlton-Perez, A.J., 2014.

Weakened tropical circulation and reduced precipitation in response to geoengineering. *Environmental Research Letters,* 9(1), p.014001. Available at:

http://stacks.iop.org/1748-

9326/9/i=1/a=014001?key=crossref.878d5812d41285f5514acaa5402e63c3 [Accessed January 10, 2014].

[11] Fleming, J., (2010). *Fixing the Sky*, New York: Columbia University Press.

[12] Fleming, J., (2006). The pathological history of weather and climate modification : Three cycles of promise and hype. *Historical Studies in the Physical and Biological Sciences,* 37(1), pp.3_25.

[13] Gray C S (2005), *Another Bloody Century*, Phoenix Books.

[14] Havens, B.S., (1952). *History of Project Cirrus* (Report No. RL 758), New York: General Electric Research Laboratory.

[15] Hegerl, G.C. & Solomon, S., (2009). Risks of Climate Engineering. *Science*, 325, pp.955-956.

[16] Homer-Dixon, T., 1991. On the Threshold: Environmental Changes as Causes of Acute Conflict. *International Security*, 16(2), pp.76-116.

[17] Hulme, M. (2014). *Can Science Fix Climate Change?: A Case Against Climate Engineering*. Oxford, UK: Polity Press

[18] Jones, A., et al. (2013). The impact of abrupt suspension of solar radiation management (termination effect) in experiment G2 of the Geoengineering Model Intercomparison Project (GeoMIP). *Journal of Geophysical Research: Atmospheres, 118* (17), 9743-9752

[19] Kaldor, M 1999, New and Old Wars. Organized Violence in a Global Era. Stanford

[20] MacKerron, G (2014) Costs and economics of geoengineering, CGG Working Paper 13.

[21] Molas-Gallart and Robinson, 1997

[22] NIPP 2013, *National Infrastructure Protection Plan*, Department

for Homeland Security, Washington. Available at: http://www.dhs.gov/national-infrastructure-protection-plan

[23] NRC, 2003. *Critical Issues in Weather Modification Research*, Washington D.C.

[24] Pielke, R.A., 2010. *The climate fix: what scientists and politicians won't tell you about global warming*, Basic Books.

[25] Rayner, S. et al., 2013. The Oxford Principles. *Climatic Change*. Available at: http://link.springer.com/10.1007/s10584-012-0675-2 [Accessed March 7, 2013].

[26] Trenberth, K.E. & Dai, A., 2007. Effects of Mount Pinatubo vol-canic eruption on the hydrological cycle as an analog of geoengi-neering. *Geophysical Research Letters*, 34(15), p.L15702. Available at: http://doi.wiley.com/10.1029/2007GL030524 [Accessed January 23, 2014].

[27] UN 2007 UN Council, Letter date 5 April 2007 from the Permanent Representative of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council;

[28] UN, 2011. UN Security Council 6587th Meeting, New York.

[29] United States Department of Defense, 2014. *Quadrennial Defense Review 2014*, Washington D.C.

[30] US Department of Homeland Security, 2008. *Hurricane Modification Workshop Report,* Boulder Colorado.

[31] Willoughby, H.E., Clos, J.A. & Shoreibah, G., 1982. Concentric eye walls, secondary wind maxima, and the evolution of the hurricane vortex. *Journal of the Atmospheric Sciences*, 39, pp.395 _ 411.

[32] Xueliang, G. U. O. (2009). Advances in Weather Modification from 1997 to 2007 in China. *Advances in Atmospheric Sciences*, 26(2), 240_252.