Journal of Strategic Security

Volume 13
Number 4 *Vol. 13, No. 4 Climate Change and Global Security*

Article 4

Climate Change and Hybrid Warfare Strategies

Chad M. Briggs
University of Alaska, Anchorage, cbriggs9@jh.edu

pp. 45-57

Recommended Citation
Briggs, Chad M.. "Climate Change and Hybrid Warfare Strategies." *Journal of Strategic Security* 13, no. 4 (2020) : 45-57.
DOI: https://doi.org/10.5038/1944-0472.13.4.1864
Available at: https://digitalcommons.usf.edu/jss/vol13/iss4/4

Climate Change and Hybrid Warfare Strategies

Abstract

Concepts of hybrid warfare and climate security are contested on their own, and are rarely considered as connected in planning for future security risks. Yet climate change presents new hazards for national security, and opportunities for those looking to foment instability and uncertainty in traditional institutions. This article examines the connections between climate change risks and hybrid war strategies, and focuses on concepts of resilience targeting, information warfare, and geoengineering, illustrating that 'full spectrum' analyses of security are necessary in developing future security strategies.

Acknowledgements

My thanks to four anonymous reviewers and the editors for their comments and suggestions, and to Tracy Walstrom Briggs for her editing.

Introduction

National security discussions of climate change and hybrid warfare have barely intersected, despite both being highly visible in discussions of the changing nature of conflict and security. When climate changes are referenced it is typically in the context of how shifting environmental conditions can accelerate certain components of hybrid warfare, such as terrorism, a watered down version of the original conception of climate security as a threat multiplier in security foresight.[1] Yet despite the lack of obvious connections between the concepts, climate security and hybrid warfare are linked in key areas. The difficulty in seeing these links leaves security organizations vulnerable to the associated risks. This article briefly outlines relevant concepts of climate security and hybrid warfare, and discusses connections between climate change and information warfare, attempts to control resources, and geoengineering technologies. In contrast to traditional conceptions of strategic security in terms of military action, climate change highlights the ways in which not only human security is put at risk, but also how actors can take advantage of or force environmental changes in order to undermine adversaries. While Sun Tzu wrote that creating vulnerabilities in one's opponent is too costly, he made an exception with exploitation of environmental factors.[2] In the twenty-first century, we likewise see opportunities for asymmetric action against opponents by opening environmental vulnerabilities.

One of the important contributions that hybrid warfare theorists have made is to widen the concepts of security beyond the standard images of violence and conflict (for example, kinetic warfare), and to argue that increasingly one witnesses coordinated actions across a spectrum of activities, from traditional military actions to cyberattacks, criminal networks, disinformation campaigns, and terrorism. Some analysts argue that hybrid conflicts are not necessarily new, that asymmetric and irregular warfare have existed for ages, while others point out the increased coordination across different spaces, including leveraging cyber technologies and social media.[3] Despite these differences, there is wide agreement that the United States and NATO-centric political concepts of conflict fail to capture the wide range of potential threats and risks inherent in contemporary security.[4] The formal definitions of hybrid

warfare in the US took place at the same time that intelligence analysts called for full spectrum analyses to reflect the complexity of conflict in areas like Iraq and Afghanistan, but also in many ways mirror strategic doctrines developed by the Russian Federation and People's Republic of China (PRC).[5]

Specifically, the Russian Federation has long used concepts of *maskirovka* in operations and strategy, meaning the masking of identity and goal of using proxies when available, and not admitting attribution even in cases where actions are linked to the government.[6] The Russian military occupation of the Crimean peninsula of Ukraine in 2014 was the clearest example of these approaches, but they have continued in its cyber, military, and counter-intelligence operations in the region and abroad.[7] Similarly, though with a slightly different emphasis from Russia's *maskirovka* or Gerimasov Doctrine, is the PRC's concept of unrestricted warfare. Based on insurgency experiences of the Chinese Communist forces in the 1940s and codified more recently in 1999, unrestricted warfare is a strategy of using all possible tools to engage an opponent asymmetrically, from political and legal warfare to traditional kinetic operations.[8] American concepts of wider warfare, such as multi-domain operations (MDO), still tend to focus on military operations and not the broader array of potential actors or actions.

Discussions over climate change as a security risk have encountered similar issues, namely that the concept of climate security often is defined in terms of how much climate-induced environmental changes increase the risks of violent conflict.[9] While the focus on violent conflict in climate security is common in academia, in contrast the applied military definitions of climate security tend to focus more on human security, and try to identify areas in which environmental changes affect operational or strategic goals. In this sense, climate as a cause of conflict is not viewed as a primary factor, but it remains vitally important for understanding a wide variety of logistical and intelligence risks, from future humanitarian assistance and disaster response (HA/DR) operations, to infrastructure risks, force protection (for example, extreme heat events, emerging diseases), search-and-rescue (SAR), and energy supplies.[10] Where extreme environmental changes do threaten social stability, such as a major famine or shifting monsoon rains, the military planning view has been that

https://digitalcommons.usf.edu/jss/vol13/iss4/4
DOI: https://doi.org/10.5038/1944-0472.13.4.1864

responding to complex disasters is a severe drain on resources, and that other agencies heading off such futures is the best course of action, not preparing for additional kinetic scenarios.[11]

While the logistical and humanitarian risks that fall under human security concepts may not appear as salient as violent conflict to some, this is the same criticism made by hybrid warfare analysts. Essentially, focusing primarily on violent conflict and traditional kinetic warfare, and ignoring coordinated actions in the grey zones of activity that fall under the threshold of military response, leaves vulnerable many societies and communities to impacts that fall under the wider concepts of human, energy or cyber security. These vulnerable areas are where security may be most at risk, and yet analysts risk ignoring events that fall outside of traditional definitions of security. Climate-induced environmental changes can pose hazards from massive wildfires to flooding, from crop failure to energy blackouts, from pandemic disease to increased risks of tsunamis.[12] Not only do climatic changes pose risks to security on these more fundamental levels, they are also the areas, which are leveraged as tools for entities employing hybrid warfare strategies. Environmental changes also overlap with strategies that can widen insurgency and conflict potential, from forced migration of refugees, resource capture (including food), destruction of infrastructure (urbicide), and other actions that undermine community well-being and cohesiveness.[13]

Resilience Targeting

In conducting assessments of post-conflict regions and reconstruction, a pattern emerged that suggested many actions taken during a conflict were designed not to target military units, or even civilians directly, but were intended to prevent communities from being able to recover from the conflict. By attacking or blocking access to critical nodes in essential systems, aggressors could exploit key vulnerabilities and actively target those factors that constituted resilience and the ability of systems to recover following a conflict. The specific tactics could vary, from sowing landmines in agricultural areas, destroying environmental or health infrastructure (for example, wastewater treatment facilities), or undercutting livelihoods, this practice of resilience targeting often

occurred in civil wars and was tied to policies of ethnic cleansing.[14]

Similar tactics are observed in hybrid warfare environments. Hybrid warfare strategies are often employed in asymmetric conflicts, where the less powerful actor takes advantage of the adversary's vulnerabilities to create instability and disruption. As resilience is a key component of vulnerability, actively undercutting resilience of critical systems automatically increases associated vulnerabilities, whether the ability to withstand outside attacks, maintain social, political, and economic stability, or to recover following a disaster. In a general sense, any reduction of resilience in a society or its underlying support systems increases that society's vulnerability to emerging hazards linked to climate change. When Ukrainian society, for example, is polarized through social media and disinformation campaigns, energy utilities suffer cyberattacks, financial systems are delegitimized and fail, the country loses its ability to develop climate mitigation policies or respond to hazards such as extreme heat events.

On a more specific level, however, hybrid warfare tools are employed in spaces opened by climate related stresses. One key component that Hoffman and others identified in the application of hybrid warfare has been the criminal element and this may serve as an example of the synergistic effects between climate change and deliberate efforts to destabilize a region or system.[15] To take one example, as drought and desertification affect farmers in central Africa near Lake Chad, criminal and terrorist networks such as Boko Haram can take advantage of the stresses for both recruitment and human trafficking.[16] Human trafficking of refugees not only creates its own crisis, it is used as a weapon to divide societies and destination countries whether in North Africa or southern Europe. This division works best when tied with a coordinated disinformation campaign that frames the existence of refugees as a national, cultural, or existential threat, rather than a humanitarian crisis.[17] Criminal networks can also destabilize regions by focusing on livelihood and environmental resources, from fisheries to illegal trade in wildlife.

The Northern Triangle of Central America (including Guatemala, Honduras, and El Salvador) may be another example where criminal networks have both destabilized a region and taken advantage of unstable

https://digitalcommons.usf.edu/jss/vol13/iss4/4
DOI: https://doi.org/10.5038/1944-0472.13.4.1864

conditions. Research strongly suggests that climate changes have impacts on levels of crime, and that in Central America migration toward the United States is linked to both environmental changes and those taking advantage of resulting disruption.[18] Deforestation and destruction of agricultural land, to take one example, links both larger environmental changes and narco-crime syndicates and local control of land by criminal networks.[19] Coupled with problems of corruption, outside interference by groups (whether nation-states or corporations), and colonial legacies of power structures and economics, it is difficult for countries for develop the capacity and legitimacy to address these non-traditional security dynamics. Note that the criminalization framework can be misused, by framing adaptation strategies following stresses or disasters as threats to national security.[20] The focus should remain on vulnerable populations and systems. For entities looking to destabilize the legitimacy of governing institutions, undercutting basic needs such as food, water, and livelihoods can be an effective component of a wider campaign.[21]

In this sense, climate change is not the cause of conflict, but drives an array of stressors that can be exploited by those looking to profit from uncertainty and instability during or prior to a conflict. An adversary that is deeply divided and unable to cope with disasters may be less formidable an opponent. With natural hazards increasing in scope and intensity in many areas, from extreme heat to flooding and/or drought, undercutting response and perhaps even sparking disasters may be an effective approach for an aggressor who either lacks traditional military capabilities, or wishes to remain hidden and attribute blame elsewhere. Such approaches, however, work best when actors attack resilience not only on a physical basis, but also in the informational space.

Information A2AD

The concept of anti-access and area denial (A2AD) refers to methods by which an adversary denies an opponent the ability to operate in or enter a contested territory. In modern usage, it has often referred to concerns over the Chinese military's efforts to threaten U.S. naval forces in regions like the South China Sea, a region in which the People's Liberation Army (PLA) and People's Liberation Army Navy (PLAN) have used hybrid strategies

(for example, maritime militia) and island construction (more below) to shift the nature of control and security.[22] One could also conceive of information A2AD, however, or ways in which adversaries are able to deny the usual access to and control of informational and cyber spaces. Beyond the traditional denial of service (DoS) attacks on information technology, hybrid warfare can encompass additional attacks that undermine trust in areas like financial services (for example, ransomware and identify theft), navigation (Global Positioning Systems), and medical records. In the climate change realm, attacks can be systematically carried out to question to validity of climate-related scientific data and research, and in so doing even physically deny access to certain regions for military operations.

Campaigns against climate science are not new, and in recent court cases have traced such attacks back to oil companies in the 1970s.[23] Increasingly, attacks on the validity of climate science are carried out by state and non-state actors as part of coordinated efforts to bolster insecurity. Actors employ techniques of uncertainty amplification, cyber aggression against individual scientists, and media campaigns to manufacture conspiracies related to everything from George Soros to chemtrails to weather control at Air Force facilities. Strategic reasons exist for doing so. For state relying heavily on oil and gas exports for government revenue, large-scale policy shifts to invest in renewable technologies and divest from fossil fuel industries, creates an existential threat to the well-being of the state. If, for example, the European Union responds to climate change by investing more in solar and wind technologies, this can directly affect the strength of the Russian state (where the oil and gas sector pay nearly forty percent of government revenues \The more uncertainty that can be inserted into discussions over climate change, the more that scientists are linked to conspiracy theories, the less likely abrupt policy changes will be made that move from dependence on fossil fuel sources.[24]

Intelligence agencies in Russia and petrostates have been linked to climate change disinformation campaigns, and the United States and Canadian governments have not been immune from such actions.[25] Where the goals of such disinformation campaigns is disruption of actions to respond to climate change related risks, and where such actions have implications for disaster or military preparedness, they can constitute components of

https://digitalcommons.usf.edu/jss/vol13/iss4/4
DOI: https://doi.org/10.5038/1944-0472.13.4.1864

hybrid warfare actions. For example, politicization over the existence of climate change in the United States has led the White House to remove all references to climate change from the National Security Strategy, and the recently released Air Force Arctic strategy contained only three mentions of climate change (and all bundled with the term weather).[26] The idea behind referring to A2AD info ops is not that information spaces will be completely off-limits to certain countries, but in the case of climate change and other scientific issues, social media spaces and even academic research have been flooded with strident anti-science voices that can overwhelm discussion, while political pressures have resulted in climate-related data and websites being taken down by government officials.[27]

The potential implications are that the U.S. Navy (whose Task Force Climate Change was shut down in 2019), Air Force, and Coast Guard are constrained in their abilities to discuss key factors in operational and strategic planning for the region.[28] Large-scale loss of sea ice, melting permafrost, changes to Arctic shipping, all require investment in capabilities and/or consideration of lost infrastructure (for example, damage to runways due to permafrost melt), slowing the United States response and leaving open space for Russian and Chinese operations in the region. Denying domain awareness is a long-standing strategy in military operations, and the anti-science campaigns promoted by outside actors accelerate the inability of actors to avoid seeing clearly in rapidly changing regions like the Arctic.

Shifting the Groundwork

One of the more notable tools used in hybrid warfare in recent years has been the construction of new territory by the People's Republic of China inside the South China Sea, and establishment of military bases to assert control over exclusive economic zones. While ruled illegal by both courts in The Hague and by the U.S. State Department, among others, the PRC has skirted traditions of how countries claim control of territory and resources, taking advantage of Law of the Sea (UNCLOS) provisions while at the same time ignoring its prescriptions. This island terraforming is part of a larger strategic approach by the PRC to obtain control of natural resources, including fossil fuels, rare earth minerals, and especially food.

With concerns over food insecurity and availability of water and land, China has not been alone in making concerted efforts to obtain control of land overseas.[29]

Foreign control of land is nothing new. European colonial powers shifted entire agrarian economies to accommodate cash crop exports, and United States companies controlled large parts of Central America through the mid-20th century. Similar patterns now emerge with corporations wresting control of land and crops away from local governments, sometimes with enormous political consequences such as the South Korean company Daewoo's attempts to lease over half of all agricultural land in Madagascar.[30] What may be concerning for the future would be new approaches to control of land, water and resources in response to climate change pressures, elements of which are already evident. It is possible for actors to carry out coordinated campaigns using tools mentioned above, combining resilience targeting, human trafficking, and information warfare, in order to wrest control of territory that they then expand upon as security operations. While governments, corporations, terrorist and criminal networks have taken advantage of disasters in the past, new technologies are emerging that may allow the disasters to be engineered by those same actors.

While geoengineering technologies have long been the work of science fiction, the ability to use technology to affect and control solar radiation management (SRM) of certain parts of the globe are increasingly close to reality. The concept behind SRM is to deploy technologies, such as stratospheric nanoparticles, to reflect the sun's rays away from the earth, or to direct solar radiation onto selected regions to warm it more quickly.[31] While cost, feasibility, and control issues are highly uncertain, from a security perspective three critical issues emerge.

The first hybrid-climate security issue is that geoengineering technologies, if deployed in the future, may not be controlled by traditional space agencies like NASA or the European Space Agency (ESA). Geotech research is often being undertaken by corporations, in part because national governments may be constrained by legal conventions such as ENMOD (Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques), but also because no

https://digitalcommons.usf.edu/jss/vol13/iss4/4
DOI: https://doi.org/10.5038/1944-0472.13.4.1864

governance mechanisms exist to address use of these new technologies.[32] It would be entirely possible, to use a hypothetical example, for Pakistan to contract SpaceX to deploy technologies developed by China, in an attempt to prevent further melt of Himalayan glaciers. The issue is that no clear responsibility may exist, or mechanism for 'downstream' groups affected to protest such actions through formal channels.

The lack of governance leads into the second critical issue, which is that of mis- and disinformation. With geoengineering technologies lacking clear cause and effect, and with conspiracies already circulating concerning such technologies, attribution for environmental events and disasters are open to exploitation. In the above example, even if the deployment of technology had no actual effect on Himalayan glaciers, any subsequent change in the Indian monsoon could be blamed on Pakistan, the United States, or China. Exploiting disasters for political gain is a common tactic, but the point is that technology to address climate change can open space for existing hybrid strategies against countries or societies. The third problem is that there may be some kernel of truth in such geoengineering concerns. It may be possible to employ such technologies in a deliberate attempt to disrupt climate, weather, or ecosystem stability, or even just to give the appearance of doing so. Turning such technologies into a weapon is not beyond the realm of possibility, particularly if the strategic goal is disruption itself.[33]

If the strategic goal of hybrid warfare is to stoke instability in a region or system, to keep it off balance by exploiting available technologies and vulnerabilities, these new approaches to terraforming and geoengineering allow disruptive actors to exploit climate change in ways that are difficult for states and communities to defend against or even anticipate. With climate change (via sea level rise) already shifting land and maritime borders, and natural processes and hazards no longer following historical patterns, these uncertainties will be easy to take advantage of or accelerate.

Conclusion

The disruptions that climate-related environmental changes pose to

military operations and strategy have at many times mirrored those challenges raised by irregular warfare, counter insurgency operations (COIN), and cyber warfare. By not fitting into easily defined categories, emerging risks and threats tended to be redefined so that they did fit traditional security concepts, or they were ignored. Concepts like climate change can be considered either a political issue by military officers or a boutique topic by academics, rather than representing a wide variety of change drivers that could undermine many well-established assumptions about stability, operations, and logistics. So, too, has hybrid warfare been contested as being too broad, too all-inclusive, rather than reflecting coordinated campaigns by aggressive states and non-state actors whose goal is the disruption that many people may hope goes away on its own.

Instead, military strategists should understand that hybrid warfare and climate security are interlinked concepts, both reflecting the ability of aggressors to take advantage of uncertainty and change, and to sow division and accelerate such changes. Both military planners and security studies specialists should focus more attention on climate change not only as a threat multiplier for traditional concepts of security, but incorporate shifts in environmental conditions with advances in understanding hybrid warfare and new technologies for adversaries to take advantage of these changes. With climate security discussions largely focused on either diplomacy or impacts on conventional military operations, greater integration of lessons from hybrid warfare, IW, COIN, and related experiences can allow warning intelligence and planning for new constellations of strategic threats.

Climate change adaptive strategies such as migration can be worsened and turned into a security threat, power plants under stress from heat can be attacked via cyberattacks, and possibly even climate systems themselves can come under threat from more than unintended action. More full-spectrum assessments of these possibilities can assist in anticipating and warning of where and how climate change can be deliberately securitized. The examples discussed in this article, from criminal networks and information warfare to geoengineering, are a subset of tools available within the hybrid warfare spectrum of potential actions. The cases demonstrate that global environmental changes are not external factors affecting the strategic peripheries. The environment is instead the ground

https://digitalcommons.usf.edu/jss/vol13/iss4/4
DOI: https://doi.org/10.5038/1944-0472.13.4.1864

upon and within which we operate, and absent concerted efforts to rethink how climate change affects strategic security, we will be left preparing for the wrong battles.

Endnotes

[1] Elisabeth Braw, "How Climate Change Will Help China And Russia Wage Hybrid War," DefenseOne, October 23, 2019; https://www.defenseone.com/ideas/2019/10/how-climate-change-helps-hybrid-war-practitioners/160810/; John J. McCuen, "Hybrid wars," *Military Review* 88, no. 2 (2008): 107.

[2] Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1971), 141-143.

[3] Christopher Paul, "Confessions of a Hybrid Warfare Skeptic," *Small Wars Journal*, (March 2016); https://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfare-skeptic; Jarno Limnéll, "The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War," *International Journal of Cyber-Security and Digital Forensics* 4, no. 4 (2015): 521-533, http://doi.org/10.17781/P001973.

[4] Robert Johnson, "Hybrid War and its Countermeasures: a Critique of the Literature," *Small Wars & Insurgencies* 29, no. 1 (2018): 141-163, http://doi.org/10.1080/09592318.2018.1404770.

[5] Frank G. Hoffman, "'Hybrid Threats:' Neither Omnipotent Nor Unbeatable," *Orbis* 54, no. 3 (2010): 441-455, https://doi.org/10.1016/j.orbis.2010.04.009; Roger N. McDermott. "Does Russia Have a Gerasimov doctrine?" *Parameters* 46, no. 1 (2016): 97; Alessio Patalano, "When Strategy Is 'Hybrid' and Not 'Grey:' Reviewing Chinese Military and Constabulary Coercion at Sea," *The Pacific Review* 31, no. 6 (2018): 811-839, https://doi.org/10.1080/09512748.2018.1513546; Adrian Wolfberg, "Full-spectrum Analysis: a New Way of Thinking for a New World," *Military Review* 86, no. 4 (2006): 35.

[6] Daniel P. Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (New York: Defense Press 2019).

[7] Mark Galeotti, "Hybrid, Ambiguous, and Non-linear? How New Is Russia's 'New Way of War'?" *Small Wars & Insurgencies* 27, no. 2 (2016): 282-301, https://doi.org/10.1080/09592318.2015.1129170.

[8] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House Arts, 1999); James K. Wither, "Making Sense of Hybrid Warfare," *Connections* 15, no. 2 (2016): 73-87, https://doi.org/10.11610/connections.15.2.06.

[9] Simon Dalby, "Climate Change and Environmental Conflicts," in *Routledge Handbook of Environmental Conflict and Peacebuilding*, eds. Ashok Swain and Joakim Öjendal (New York: Routledge, 2018), 42-53, https://doi.org/10.4324/9781315473772-4; Kendra Sakaguchi, Anil Varughese, and Graeme Auld, "Climate Wars? A Systematic Review of Empirical Analyses on the Links Between Climate Change and Violent Conflict," *International Studies Review* 19, no. 4 (2017): 622-645, https://doi.org/10.1093/isr/vix022; Jürgen Scheffran, Michael Brzoska, Jasmin Kominek, P Michael Link, and Janpeter Schilling, "Climate Change and Violent Conflict," *Science* 336, no. 6083 (2012): 869-871, https://doi.org/10.1126/science.1221339.

[10] Ralph Espach, David Zvijac, and Ronald Filadelfo, "Impact of Climate Change on US Military Operations in the Western Pacific," *Marine Corps University Journal* 7 (2016): 89-113, https://doi.org/10.21140/mcuj.2016si05.

[11] Chad M. Briggs. "Climate Security, Risk Assessment and Military Planning." *International Affairs* 88, no. 5 (2012): 1049-1064, https://doi.org/10.1111/j.1468-

2346.2012.01118.x; Andrew DeWit, "Towards Human Security: Climate Change and the Military Role in Humanitarian Assistance and Disaster Response," in *Human Security and Japan's Triple Disaster*, eds. Paul Bacon and Christopher Hobson (New York: Routledge, 2014), 192-209.

[12] New evidence is emerging that glacier retreat increases the risks of landslide-generated tsunamis in the Arctic. Henry Fountain, "Scientists Warn of Growing Landslide Risk for Alaska," *New York Times*, May15, 2020, A2, https://www.nytimes.com/2020/05/14/climate/alaska-landslide-tsunami.html.

[13] Bruce Stanley, "The City-Logic of Resistance: Subverting Urbicide in the Middle East City," *Journal of Peacebuilding & Development* 12, no. 3 (2017): 10-24, https://doi.org/10.1080/15423166.2017.1348251.

[14] Chad M. Briggs, Moneeza Walji, and Lucy Anderson, "Environmental Health Risks and Vulnerability in Post-conflict Regions," *Medicine Conflict and Survival* 25, no. 2 (2009): 122-133, https://doi.org/10.1080/13623690902943362.

[15] Hoffman, "'Hybrid Threats,' " 29-30.

[16] Simeon Alozieuwa, "Political Economy of War and Violence: the Boko Haram in the Lake Chad Basin," *African Renaissance* 13, no. 1-2 (2016): 165-198.

[17] Stefano Braghiroli and Andrey Makarychev, "Redefining Europe: Russia and the 2015 Refugee Crisis," *Geopolitics* 23, no. 4 (2018): 823-848, https://doi.org/10.1080/14650045.2017.1389721.

[18] Robert Agnew, "Dire Forecast: a Theoretical Model of the Impact of Climate Change on Crime," *Theoretical Criminology* 16, no. 1 (2012): 21-42, https://doi.org/10.1177/1362480611416843; Lauren Markham, "How Climate Change Is Pushing Central American Migrants to the US," The Guardian, 6 April 2019, https://www.theguardian.com/commentisfree/2019/apr/06/us-mexico-immigration-climate-change-migration.

[19] Beth Tellman, Steven E. Sesnie, Nicholas R. Magliocca, Erik A. Nielsen, Jennifer A. Devine, Kendra McSweeney, Meha Jain, David J. Wrathall, Anayasi Dávila, Karina Benessaiah, and Bernardo Aguilar-Gonzalez, "Illicit Drivers of Land Use Change: Narcotrafficking and Forest Loss in Central America," *Global Environmental Change* 63 (2020): 102092, https://doi.org/10.1016/j.gloenvcha.2020.102092.

[20] Jonathan S. Simon, "Wake of the Flood: Crime, Disaster, and the American Risk Imaginary after Katrina," *Issues in Legal Scholarship* 6, no. 3 (2007), https://doi.org/10.2202/1539-8323.1094.

[21] Timothy E. Hill, *Reducing an Insurgency's Foothold: Using Army Sustainability Concepts as a Tool of Security Cooperation for AFRICOM* (Carlisle Barracks PA: Army War College, 2008), https://apps.dtic.mil/sti/citations/ADA493738.

[22] Justin L. Reddick, *Under the Dragon's Wing: A Strategic Approach to China's Militarization Efforts of its Artificial Islands in the South China Sea* (Fort Leavenworth, KS: US Army Command and General Staff College, 2017), https://apps.dtic.mil/sti/citations/AD1038848.

[23] Stephan Lewandowsky, Naomi Oreskes, James S. Risbey, Ben R. Newell, and Michael Smithson, "Seepage: Climate Change Denial and its Effect on the Scientific Community," *Global Environmental Change* 33 (2015): 1-13, https://doi.org/10.1016/j.gloenvcha.2015.02.013.

[24] Sander van der Linden, "The Conspiracy-effect: Exposure to Conspiracy Theories (About Global Warming) Decreases Pro-social Behavior and Science Acceptance," *Personality and Individual Differences* 87 (2015): 171-173, https://doi.org/10.1016/j.paid.2015.07.045.

[25] Indigo J. Strudwicke and Will J. Grant, "#Junkscience: Investigating Pseudoscience Disinformation in the Russian Internet Research Agency Tweets." *Public Understanding of Science* 29, vol. 5 (2020): 459-472, https://doi.org/10.1177/0963662520935071.

[26] Jean Chemnick, "Trump Drops Climate Threats from National Security Strategy,"

https://digitalcommons.usf.edu/jss/vol13/iss4/4
DOI: https://doi.org/10.5038/1944-0472.13.4.1864

Scientific American, December 19, 2017, https://www.scientificamerican.com/article/trump-drops-climate-threats-from-national-security-strategy/; U.S. Department of the Air Force, *Arctic Strategy: Ensuring a Stable Arctic Through Vigilance, Power Projection, Cooperation, and Preparation* (Arlington, VA: U.S. Department of Defense, 2020), https://www.af.mil/Portals/1/documents/2020SAF/July/ArcticStrategy.pdf.

[27] Victoria Hermann, "I Am an Arctic Researcher. Donald Trump Is Deleting My Citations," *The Guardian*, March 28, 2017, https://www.theguardian.com/commentisfree/2017/mar/28/arctic-researcher-donald-trump-deleting-my-citations.

[28] JD Simkins, "Navy Quietly Ends Climate Change Task Force, Reversing Obama Initiative," *Navy Times*, August 26, 2019, https://www.navytimes.com/off-duty/military-culture/2019/08/26/navy-quietly-ends-climate-change-task-force-reversing-obama-initiative/.

[29] Gerald Chan, "China and Small States in Food Security Governance," *African and Asian Studies* 13, no. 1-2 (2014): 59-79, https://doi.org/10.1163/15692108-12341285.

[30] Venusia Vinciguerra, "How the Daewoo Attempted Land Acquisition Contributed to Madagascar's Political Crisis in 2009," in *Contest for Land in Madagascar*, eds. Michael Lambek, Gwyn Campbell and Sandra Evers (Leiden: Brill, 2013), 221-246, https://doi.org/10.1163/9789004256231_011.

[31] Andrew Lockley, "Security of Solar Radiation Management Geoengineering," *Frontiers of Engineering Management* 6, no. 1 (2019): 102-116, https://doi.org/10.1007/s42524-019-0008-5.

[32] Janos Pasztor, "The Need for Governance of Climate Geoengineering," *Ethics & International Affairs* 31, no. 4 (2017): 419, https://doi.org/10.1017/s0892679417000405.

[33] Paul Nightingale and Rose Cairns. "The Security Implications of Geoengineering: Blame, Imposed Agreement and the Security of Critical Infrastructure" (Working Paper, University of Sussex, 2014), http://sro.sussex.ac.uk/id/eprint/52905/.