



Insights

Climate Change and Evolving Malicious Risks



Foreword

On 18 November 2022, the United Nations Climate Change Conference, or Conference of the Parties of the UNFCCC (COP27), came to a close in Sharm El Sheikh, Egypt. The annual summit was notable because of the historic deal agreed by almost 200 countries to launch a fund to support states worst affected by climate change. This initiative follows others in recent years where states have agreed to cooperate on this issue. The most high-profile of these is the Paris Agreement, ratified in November 2016, which aims to curb global temperature rises this century to 1.5°C (2.7°F).

Individual states are also taking steps to meet these targets. In 2021, the UK released its 'Climate Change Strategy', with the central aim of achieving net-zero emissions by 2050.¹ The same goal was outlined in an Executive Order by United States President Joe Biden in May 2021. This seeks to ensure the US takes an active role in supporting the financial sector as well as companies, local governments and at-risk communities to understand and address the growing risks.² Moreover, the recently signed US Inflation Reduction Act³ additionally pledges almost \$370 billion over the next 10 years to tackle climate change.

While these developments demonstrate intent, the impacts of climate change in other areas have garnered far less attention. In particular, the nexus between climate change and political violence is an underexplored dynamic. Recent studies by several institutions suggest climate-related malicious action will increase in the future; including research by the US body The National Consortium for the Study of Terrorism and Responses to Terrorism (START) based at

the University of Maryland. Crucially, studies such as this emphasise that the full implications – such as more threat actors, increased levels of violence, a wider range of vulnerabilities, and the sheer increase in insurable infrastructure – have yet to be considered in sufficient detail in policymaking circles.

In May 2022, START produced a report for the United Kingdom's state-backed terrorism reinsurer Pool Re, entitled 'A Climate of Terror? Approaches to the Study of Climate Change and Terrorism'. The paper was presented at the online conference of the the International Forum for Terrorism Reinsurance Pools (IFTRIP), and its key findings are summarised in the 'Climate change will increasingly drive terrorism' section of this report. Indeed, the implications of increasing climate-related malicious activity will be of particular relevance to state-backed insurers, such as Pool Re in the UK and the Federal Insurance Office (FIO) in the US, where more assets will require cover against both climate change and environmentally motivated violence.



Introduction

This report aims to outline the potential consequences of climate change on the field of malicious risk beyond terrorism, encompassing the whole spectrum of political violence from civil commotion at the grassroots up to strategic competition at the international level. The disruptive potential of technology is also considered within this dynamic.

While the detection of potential threats and future opportunities remains a valuable and necessary exercise, climate change is already having demonstrable impacts on the nature of political violence today. Geopolitical tensions are rising between states competing for finite resources and rare earth minerals used in batteries, solar panels, wind turbines, and electric vehicle motors. Climate change is increasingly becoming a source of tensions within countries as well. For example, attitudes towards environmental policy were a key fault-line in the October 2022 election in Brazil, and political violence was widely reported in the run-up to the event. Concurrently, certain terrorist movements are co-opting climate change for their own ideological ends, linking it to undesirable migration that must be curbed with violence.



Think about your risks differently

The risks from climate change can be neatly conceptualised using a framework developed by the Network for Greening the Financial System (NGFS)⁴, a group of 114 central banks and financial institutions that aims to accelerate the scaling up of ‘green’ finance and develop recommendations for central banks’ role in mitigating climate change.

The NGFS identified two broad groups of risks that are contingent on the level of resources and degree of success that carbon reduction initiatives deliver:

- **Transition Risks** develop if significant investment is undertaken to minimise the global temperature rise. Much of this investment will manifest in a significant increase in new infrastructure, such as low carbon power generation and electricity storage. While less to do with climate change grievances, construction of these assets will increase the ‘attack surface’ (the total number of potential targets for attack by malicious actors).
- **Physical Risks** occur if there is insufficient investment in carbon reduction, and the higher modelled temperature rises result in significant climate effects. These broadly concern the loss of biodiversity, water scarcity, and extreme weather. These factors are likely to drive or aggravate political violence, terrorism and other malicious risks (processes already being observed).

Transition and physical risk are not mutually exclusive. It is credible that both could have significant simultaneous impacts, where physical risks drive terrorism and political violence, while the building of ‘green

infrastructure’ is considered a potential target for malicious actors.

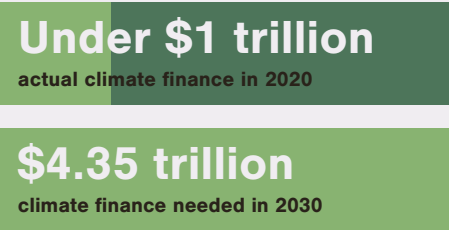
It is estimated that global expenditure on net-zero measures will need to reach \$4.35 trillion by 2030.⁵ Sectors for investment include renewable energy infrastructure, carbon-neutral transportation and other infrastructure such as water management and carbon-capture.

Within the NGFS framework, this report deals more with physical risks, as these are more clearly connected to malicious action. Under this heading, we have identified three broad themes relevant to the relationship between climate change and political violence:

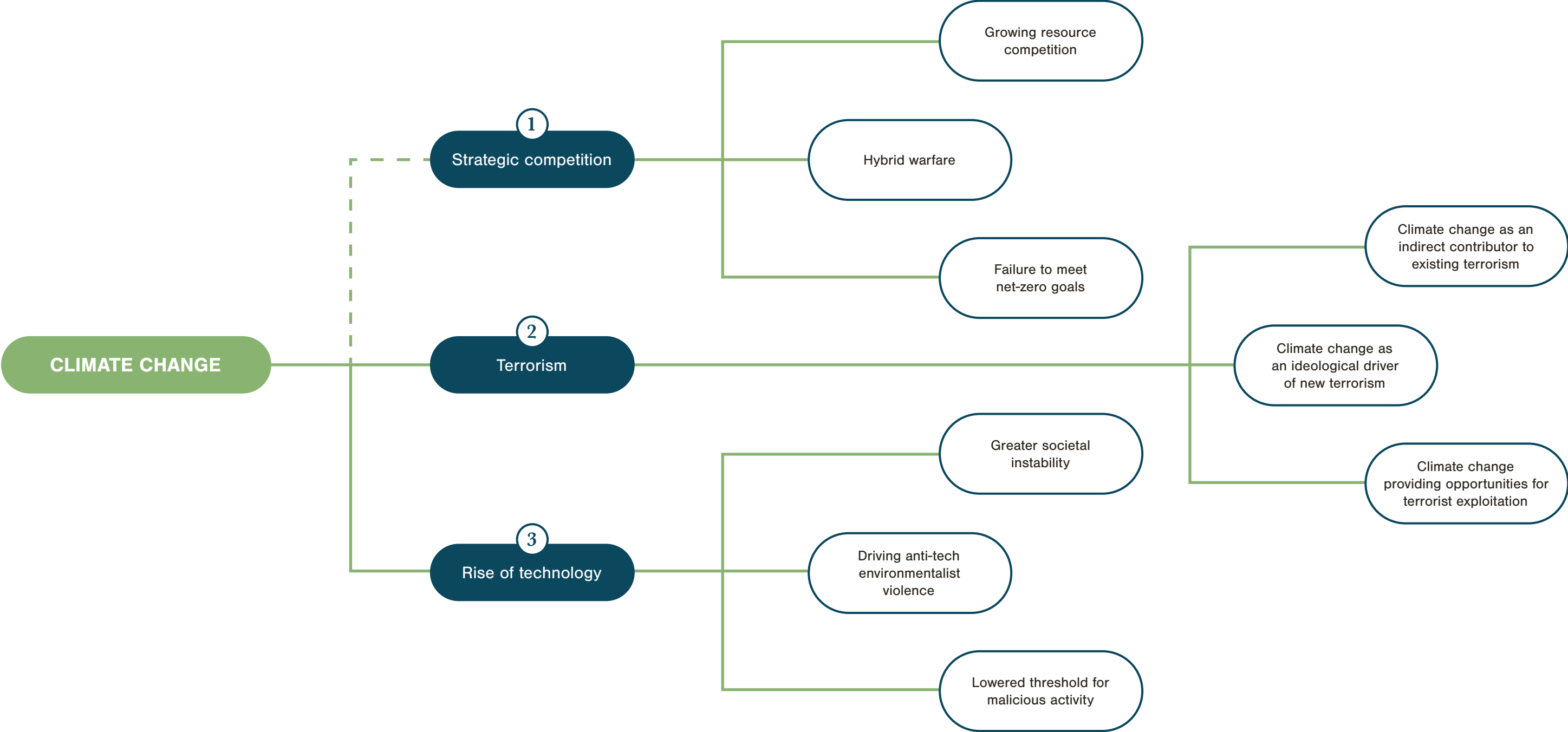
1. Strategic competition
2. Terrorism
3. The rise of technology

Climate finance

The estimated annual climate investment needed to maintain 1.5°C pathway.



 The malicious risk environment



LEGEND

- Underlying driver of change
- Key themes
- Second-order effects

Strategic competition will intensify

We need only consider the current conflict in Ukraine, or the tensions between the People’s Republic of China (referred to hereafter as China) and Republic of China (Taiwan), to recognise that many nations are increasingly willing to exert influence through the projection of power. This is commonly referred to as ‘strategic competition’ and can be defined as the contest for geopolitical dominance of the international order.

It is characterised by the synchronised use of all instruments of power that fall below the level of a conventional or nuclear war. This competition can include cyber activity, as well as efforts to shape security structures, norms and regulations, trade, and technological infrastructure. The potential difficulty in attributing responsibility to an actor following this kind of activity has led to the term ‘hybrid’ or ‘grey’ warfare being adopted in relation to strategic competition.

Aspects of hybrid warfare are intended to sow disorder in target countries, and generally include multi-layered information and disinformation programmes, the sponsorship of political violence, and targeted assassinations. The aggressor often acts through private contractors and other non-state entities, shielding involvement and providing plausible deniability. A mix of government, criminal, terrorist and other non-state actors could all play significant roles in hybrid warfare, and this very situation has unfolded in the ongoing Russian-Ukrainian conflict.

The impacts of climate change, such as rising temperatures and sea levels, have a direct impact on the national security strategies of various countries, and can also render certain territories the subject

of competition. An example of this could be growing competition for influence in the Arctic between Western states and Russia. As sea ice continues to melt, new sea lanes may open, and rising sea temperatures may afford Russian vessels greater manoeuvrability, and possibly even more warm-water ports that remain usable year-round. Moreover, melting polar ice may also spark greater competition for resources – such as fish, oil, and gas – in newly accessible maritime areas.

Competition for resources, particularly rare earth metals, is a pertinent issue. As states attempt to pursue sustainable energy alternatives more concertedly (solar panels, wind turbines, electric cars), competition between nations for finite and increasingly valuable resources is likely to heighten. Rivalry to establish dominant positions within these markets will also intensify.

Growing competition will likely draw other states into this strategic contest, some of which are developing nations that have significant ore deposits. In addition, the provision of either financial, material, or political support to third parties, whether governments or sub-state organisations, by external powers seeking to acquire access to resources is likely. In a situation in which states are vying

Strategic competition will intensify

Pro-chinese government cyber network

It was reported in June 2022 that a pro-Chinese government cyber network, identified as Dragonbridge, had impersonated environmental campaigners on social media to undermine rare earth metals producers across North America⁸. China is dominant in rare earth processing globally, and its use of the Dragonbridge group is likely part of a wider effort to preserve Western dependence on China.



Dragonbridge controlled accounts on Twitter and Facebook pose as concerned residents and promote narratives highlighting pollution and health risks of Lynas’ rare earths production

for the same material in a resource-rich location, proxy war (where combatants act on behalf of powers that are not directly involved) could occur.

Strategic competition could also decrease the likelihood of net-zero goals being achieved. A situation in which tensions between

major powers (and therefore major carbon emitters) ratchet up does not lend itself to states cooperating towards a common goal. Instead of mutually beneficial sacrifice, seeking near-term competitive advantage over rival states is more likely, and medium-term commitments to combating climate change could fall by the wayside.



Climate change will increasingly drive terrorism

Climate change is likely to have significant and varied indirect effects on the nature of terrorism. As climate change becomes an increasingly central aspect of political discourse and its effects impact the lives of growing numbers of people, the actions and ideologies of terrorists will adapt in response. Climate change is likely to drive new terrorism, but also act as force multiplier for existing terror threats.

START’s ‘Climate of Terror’ report neatly outlines that climate change could impact the terrorism landscape in three ways:

Contribute to existing terror threats

Climate change will contribute to, and exacerbate, existing terrorism and political violence campaigns in locations affected by increasingly extreme weather conditions. As more populations suffer the consequences of climate change, radicalisation and extremist violence will become more likely. Such motivators will include increasing water and food scarcity, sea level rises, extreme weather events, large-scale migration, and a wide range of financial losses. Additionally, as climate change grows in importance in mainstream discourse and policy, it will increasingly provide useful narratives for extremists with ideologies that are otherwise unpalatable to the majority of the population.

Instigate and drive new terror threats

Environmental extremism is by no means a novel phenomenon. For decades, groups such as Greenpeace, Earth Liberation Front (ELF), Earth First!, and more recently Extinction Rebellion (XR) have sporadically employed disruptive direct-action to further their causes. Growing political polarisation creates the context for more widespread, forceful

environmental action to occur. A wide array of malicious acts has already been recorded in recent years: from disruptive behaviour in public spaces or targeting organisations, to death threats against politicians, to the assassination of company executives.

On the less extreme end, the targets subjected to direct action by environmentalist groups have in recent years diversified in the West, to include conferences, major roads, and even art galleries. However, lethal attacks linked to eco-fascism have also already been conducted, including:

- Anders Breivik’s mass-casualty attack in Norway.
- Christchurch, New Zealand shooting.
- Attack in Buffalo, New York, in which the attacker published a racist ‘manifesto’ linking population growth and mass migration to the degradation of the natural environment as a justification for murder.

Increase vulnerabilities to be exploited

The consequences of climate change, such as hotter and dryer seasons, will be exploited by malicious actors. There have, for some time, been examples of deliberate setting of wildfires.



Climate change will increasingly drive terrorism

The rise of Arson terror attacks in the united states

Arson attacks using incendiary devices are the single most frequent form of terrorist attack in the United States since the 1990s, according to START’s Global Terrorism Database (GTD).



But increased vulnerability to both ignition and spread of fire, particularly in areas with a greater population and property density, is a growing concern. START has already recorded terrorist groups calling for this kind of violence, indicating that it may become more common as global temperatures rise. Furthermore, arson attacks using incendiary devices are already the single most frequent form of terrorist attack in the United States since the 1990s, according to START’s Global Terrorism Database (GTD).

Other potential threats might include increased

attacks on critical infrastructure that manages and controls scarce resources, such as water for agriculture. In more extreme cases, malicious actors could strategically take control of resources made increasingly scarce by changing weather patterns. Extremists could also exploit the real or perceived weakening of a government’s capacity to respond to climate change as a way of promoting radicalisation and recruitment. A narrative that government inertia and incompetence has led to the abandonment of a population could be an effective way to undermine state legitimacy.



Technology will continue to proliferate

Broadly, technology could intersect with climate change to create greater societal instability. Technological advancements will likely allow for greater efficiency and sustainability in many sectors, and ultimately the replacement of human workers with autonomous machinery. For example, it is assessed that many thousands of jobs could be lost as a result of the shift towards electric vehicles alone.⁷

Likewise, governments under pressure to implement a bold environmental policy agenda may invest in technological solutions to issues such as sustainable energy. A result of this innovation may be the loss of work for individuals or communities engaged in sectors linked to the carbon economy, such as coal mining. In circumstances where livelihoods are adversely affected (without well-laid plans for retraining and re-employment), a generation of more intense socioeconomic grievances is likely. Possibly leading to further strikes, riots, and civil commotion (SRCC) and potentially contributing to the radicalisation of individuals.

The 'Climate of Terror' paper published by START noted that there is some synergy between terrorism and anti-technology movements. The Unabomber, Ted Kaczynski, is the most well-known proponent of this kind of ideology – which includes ideas of primitivism and aversion to modern technology and

industrialisation. Certain corners of the radical environmentalist movement are subsets of the anti-technology movement. A currently active 'eco-nihilist' movement called Individualistas Tendiendo a lo Salvaje (Individualists Tending Towards the Wild; ITS) has committed violence against people and assets in the past decade, including explosives attacks on universities and churches. It is explicitly anti-technological, anti-industrial, and anti-civilisation. ITS cells have been active in Central America, South America and Europe, demonstrating the transnational appeal of its ideology.

Perhaps of equal concern is a second-order consequence, wherein technology enables the capability threshold for malicious actors to be lowered – increasing the number of potential malicious actors. A stark example of this is the rise of manufactured firearms.⁸ A growing decentralised movement of designers and advocates freely socialise plans online.



Key conclusions

Climate change exacerbates an increasingly complex malicious risks landscape

Growing strategic competition, the continuing spread of dual-use technology (having both civilian and military applications), and the societal and financial fallout of the global pandemic have all contributed to a particularly challenging risk environment. States conducting covert offensive cyber-attacks, non-state actors operating on behalf of states as proxy forces, and technologies allowing individuals to access weapons that have until now been unavailable have blurred the lines between various types of political violence. The increasingly noticeable effects of climate change are only serving to complicate matters further.

'Physical risks' of carbon inaction are significant

Even the most optimistic temperature projections suggest that there will be a range of climatic changes that will have first, second and third order consequences globally. It is likely that, to some degree, climate change will contribute to existing terror threats, instigate and drive new terror threats, and/or increase vulnerabilities that can be exploited. Developing a deep understanding of terrorism, political violence and other malicious risks is essential for mitigation strategies to be conceived and implemented.

'Transition risks' relating to new infrastructure projects are considerable

If governments and companies continue to move down the net-zero pathway, significant new infrastructure will be built and operated in the next few decades. Much of this investment will be in energy generation, storage and transmission⁹. The Infrastructure Investment and Jobs Act¹⁰ announced in the US in 2021 outlines hundreds of billions of dollars of investment, with Princeton University suggesting that the total required investment will be \$2.5 trillion¹¹. Not only will the infrastructure require cover for terrorism and other acts of political violence, but the sheer scale of built assets will increase the 'attack surface' available to malicious actors.

What organisations can do to mitigate these risks

Organisations, regardless of sector, should be proactive in scoping and quantifying the risks they are likely to face as a result of this changing risk environment. Decisionmakers should consider if their organisations sit along any of the fault-lines outlined in this report. They should also assess the likelihood of being the target of SRCC, terrorism, or state-backed hybrid warfare as a result of their associations or the nature of their work. There is also value in contemplating how disruptive technologies could impact their operations. In short, organisations should consider undertaking enterprise risk management and business continuity management reviews as a priority in order to mitigate the potential impact of changing risks.



About the Authors

Samphire Risk is a subsidiary of CHC Global, an independent firm of strategic malicious risk advisors. CHC’s Advisory Team offers advice to clients helping them understand and manage malicious risks. The team is staffed by an outstanding group of advisors, each with a specialist portfolio, and in addition to working in partnership with their own clients, offer expert insight and intelligence to the broader CHC business.



Jerry Smith OBE
Senior Partner & Head of Advisory



Alex Theodosiou
Senior Associate

References

1. [assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1019141/UKEF_Climate_Change_Strategy_2021.pdf](#)
2. [www.whitehouse.gov/briefing-room/presidential-actions/2021/05/20/executive-order-on-climate-related-financial-risk](#)
3. [www.democrats.senate.gov/imo/media/doc/inflation_reduction_act_one_page_summary.pdf](#)
4. [www.ngfs.net/en](#)
5. [www.climatepolicyinitiative.org/wp-content/uploads/2021/10/Full-report-Global-Landscape-of-Climate-Finance-2021.pdf](#)
6. [www.ft.com/content/57d5c3fd-35ec-4146-aa6d-9e3fc87fbcfb](#)
7. [www.ft.com/content/319966d4-89ce-4e6c-b0c4-a6f8e500e46a](#)
8. [www.jstor.org/stable/pdf/resrep10742.10.pdf](#)
9. [cmi.princeton.edu/annual-meetings/annual-reports/year-2018/building-a-carbon-net-zero-infrastructure-for-the-u-s-by-2050/](#)
10. [www.whitehouse.gov/briefing-room/statements-releases/2021/08/02/updated-fact-sheet-bipartisan-infrastructure-investment-and-jobs-act](#)
11. [netzeroamerica.princeton.edu](#)

About Samphire Risk

Samphire Risk was formed in 2021 and is a world-leading independent Managing General Agent (MGA) focused on insuring people and companies against hostile and malicious risks. Through an expert team and exceptional technology, Samphire aims to create world-class products that insure against extortive crime, hostage-taking and kidnap; terrorism in all its guises; travel into, and within, insecure countries and locations.

To find out more about Samphire please visit our website www.samphirerisk.com or follow us on LinkedIn.

Samphire and Samphire Risk are trading names of Samphire Services Limited which is an appointed representative of Davies MGA Services Limited, a company authorised and regulated by the Financial Conduct Authority under firm reference number 597301 to carry on insurance distribution activities. Samphire Services Limited is registered in England and Wales number 13421262. Registered Office: 1-3 Leadenhall Market, London, EC3V 1LR.



11/04/23