BUSINESS EXECUTIVES FOR NATIONAL SECURITY
SECURING AMERICA'S FUTURE

A Public-Private Partnership Approach to a Federal Cyber-Insurance Backstop

When Congress ultimately considers the prospect of establishing a federal insurance backstop for catastrophic cyber-attacks, it should create a public-private partnership modeled on the UK's Pool Re program that relies primarily on the private insurance market and is cost-neutral to the U.S. taxpayer. Given the serious risks of a major cyber-attack to the U.S. economy and to critical infrastructure that lives depend on, Congress should take action to create a federal backstop now, rather than taking a far costlier approach to keeping the economy whole after a catastrophic incident occurs. We also believe the U.S. government should consider consolidating existing and new catastrophic federal backstop programs (TRIA, NFIP, etc.) into a single pool to more efficiently and effectively address national catastrophes of all types.

The risk of a major cyber-attack that causes complex and catastrophic damage to U.S. critical infrastructure and the U.S. economy is real and growing.

- In February, U.S. and allied intelligence agencies warned that Chinese government-sponsored cyber actors have compromised critical infrastructure across the United States with the intention of causing destructive cyber-attacks in the event of a major crisis or conflict. Such a scenario would jeopardize American lives and the U.S. economy, as critical infrastructure industries, may be subject to cyber-enabled physical damages or have their operations disrupted for an extended period of time.
- The complexity of the cyber-threat landscape has also been a challenge for the insurance industry, which many companies rely on to protect against cyber-based disruptions. The intentionally opaque nexus between malicious cyber actors and hostile governments such as Russia, China, and Iran complicate the application of "war exclusion" clauses that are standard in insurance coverage.

Key stakeholders overwhelmingly support the notion of a federal backstop for catastrophic cyber-attacks.

- In 2022 the Government Accountability Office (GAO) recommended that the Federal Insurance Office (FIO) and the Cybersecurity and Infrastructure Security Agency (CISA) jointly assess the need for a federal insurance response to such attacks.
- Both agencies are currently considering the issue and issued a request for comment in September 2022 in which the overwhelming majority of industry respondents, including major insurance and cybersecurity firms, supported the general idea of a federal backstop to address scenarios that might overwhelm the insurance market. However, there were also a variety of ideas for how such a backstop could and should be structured.

A public-private partnership approach to a federal backstop would reflect the intention for the private insurance market to take up the majority, and ultimately the entirety of risk, while backed by the federal government.

- While there are several potential models for a federal cyber-insurance backstop, all of the models involving a federal government fund or guarantee, including Pool Re, have been structured with

the intention to reduce the federal government's exposure over time as the private market adapts and assumes more of the risk.

- A cyber-insurance backstop should therefore begin with the intention of enabling the private markets to fill in the exposure gaps that are well known in current cyber-insurance policies, reducing the federal burden over time.
- The objective of such a reinsurance pool should be to cover existing national security exclusions in insurance policies. In particular, the pool would cover scenarios falling under traditional war exclusions applied to cyber-attacks, while allowing insurers to conduct the underwriting of risk themselves. We would expect the pool to backstop business interruption losses to prevent such losses from disrupting the broader U.S. economy.
- A benefit of relying principally on insurers to issue payments rather than a federal program is that payment channels have already been established by the insurance industry and their customers.
- Treasury's Terrorism Risk Insurance Program (TRIP) was intended to be a temporary program until the market adjusted to account for the prospect of catastrophic terrorism. While Congress has reauthorized TRIP four times (most recently extending its expiry from 2020 to 2027), the program's reauthorizations have come with increasing limitations on the federal government's exposure, including through raising the minimum industry-insured loss required before federal payments would be triggered.
- The Federal Emergency Management Agency (FEMA) also found that working with the private sector to share risks through the purchase of reinsurance helped to shore up the National Flood Insurance Program and better address the insurance coverage gap.

The U.S. government should adopt a cost-neutral model so that the recovery burden is ultimately taken on by the companies that are insured and their insurers, over time, rather than the taxpayer.

- The FIO should work with major U.S. insurers and re-insurers to develop a structure modeled on Pool Re for a reinsurance pool funded by insurance industry reserves and backed by a federal government guarantee.
- The FIO, in coordination with these insurance firms, should then work with the relevant congressional committees (including the Senate Banking and House Financial Services Committees) to draft and adopt legislation establishing that reinsurance pool and providing a U.S. Treasury-backed guarantee that would be triggered for the most damaging catastrophic cyber-attacks. This legislation would identify the types of events that the reinsurance pool would cover and the damage thresholds for the source of payouts if a triggering event occurs.
- Because insurance activities are largely governed at the state level, the FIO should also work with National Association of Insurance Commissioners to ensure buy-in and cooperation from state insurance offices on how the reinsurance pool is managed and payouts made.
- We recommend that the declaration of a covered event follows the established TRIP model. The FIO would not need to share information on the provenance of the attack, it only needs to establish that an attack occurred of sufficient scale to trigger the reinsurance program.
- The reinsurance pool is funded by private insurers and backstopped by the U.S. Department of Treasury. Funds paid by U.S. Treasury will be fully reimbursed by the private sector over an achievable and reasonable time horizon.

The backstop should be structured in a way that causes reinsurers to factor greater cyber hygiene into their models, using existing protocols such as NIST 2.0. Achieving this will result in risk mitigation measures being taken by the insured.

- In February, the National Institute for Standards and Technology (NIST) released a new cybersecurity framework, CSF 2.0, providing guidance on reducing cyber risk to organizations of all types, rather than just critical infrastructure. The guidance does not prescribe specific actions but informs how to develop effective cybersecurity practices tailored to a given organization. A recent health industry study found that organizations that use the NIST cybersecurity framework faced lower cybersecurity premiums than those that did not.
- Promoting cyber hygiene through a federally backed insurance program should encourage responsible behavior and motivate organizations to uphold robust cybersecurity practices. While leveraging the NIST CSF as a foundation for establishing a baseline standard to access the proposed backstop, it is crucial to view this as a minimum requirement. Primary insurers are likely to demand even higher standards for issuing cyber-insurance policies, surpassing the baseline.

The reinsurance backstop should adopt a portfolio treaty model that puts more onus on the private market to assume risk, while allowing more flexibility for insurers to underwrite and price that risk.

- In April 2024, Pool Re began a shift from a facultative per risk model in which Pool Re determines rules for underwriting terrorism risk, to a portfolio treaty model that allowed greater flexibility for insurers to conduct risk-adjusted pricing, encouraging more of the risk to be born by the insurance market while reducing exposure for UK taxpayers. This was a natural evolution for Pool Re's intention to increasingly rely on the private insurance market to address terrorism claims and the United States should use this evolution as starting point for addressing cyber-insurance.
- Such a model also helps incentivize cyber hygiene because underwriting is expected to be more closely tied to an organization's risk, which organizations reduce through effective cybersecurity practices.

The FIO and Congress should establish a goal that, over time, all federally backed insurance programs, including TRIP and the National Flood Insurance Program, are folded into a single pool covering all national-level risks, from cyber-attacks to terrorism to natural disasters. The added diversity of risk and flexibility of the model achieves greater efficiency and resiliency.

- The more diversity of risk in an insurance portfolio, the greater the viability of the insurance entity, as funds can be shifted from the variety of risks covered to address the specific incident that occurs.

Authored by BENS Members Andrew Hersh and Matthew Flug with contributions from BENS members Bruce de'Medici, Damon Jackman, Alan Silberstein, and Ben Trowbridge, and BENS Senior Director Peter Crail. The authors are also grateful for the expertise shared by contributing members of the insurance sector, state insurance commissioners, among others with whom the authors consulted in the drafting of this paper.

Appendix: Key Terms and Definitions

Pool Re

Pool Re, or Pool Reinsurance, is the UK's leading terrorism reinsurer with the stated goal of providing financial protection from the impact of terrorism. Their coverage extends to material damage, business interruptions, construction and engineering costs, and chemical, biological, radiological, nuclear (CBRN) attacks. Pool Re started the International Forum of Terrorism Risk (Re)Insurance Pools (IFTRIP), which is aimed at fostering closer international collaboration between sovereign-backed terrorism reinsurance pools. In addition to reinsurance, Pool Re also focuses on risk management and threat analysis.

War Exclusion (in insurance policies)

In the context of insurance policies, a war exclusion is a provision found in nearly all insurance policies that excludes loss arising out of war or warlike actions. This can include invasions, insurrections, revolutions, military coups, and terrorism. The modern form of the war exclusion clause is necessary due to the inability of insurance companies to gauge premiums to cover the associated risk as well as the need to remain solvent in the event of catastrophic damages from war. In the wake of new, nontraditional warlike events, war exclusion policies have broadened their scope, notably with terrorism coverage after the September 11th attacks. Cyber-attacks conducted on behalf of hostile countries represent a legal gray area for insurance policies. While insurers have sought to apply the war exclusion to their cyber-insurance policies, a May 2023 appellate court ruling determined that a war exclusion "requires the involvement of military action," meaning the war exclusion did not apply to the 2017 Russian-backed NotPetya attack against companies working with Ukraine. Since that ruling, insurers have been increasingly limiting their cyber-insurance policies.

The Terrorism Risk Insurance Program (TRIP)

TRIP was created by the Terrorism Risk Insurance Act (TRIA) after the September 11th attacks, which cost the insurance industry an estimated $47 billion. Before TRIA, terrorism acts were not included in war exclusion insurance policies. TRIP provides for a system of shared public and private compensation for insured losses resulting from certified acts of terrorism and requires insurers to make terrorism coverage available to commercial policyholders. TRIP is run by the Secretary of the Treasury and Federal Insurance Office and has been renewed four times, currently expiring in 2027.

The National Flood Insurance Program (NFIP)

The NFIP, administered by the Federal Emergency Management Agency (FEMA), provides federally backed flood insurance to affected communities with the goal of fast-tracking rebuilding efforts in the event of flood damages. The NFIP is a public-private partnership between the federal government, the property and casualty insurance industry, states, local officials, lending institutions, and property owners.