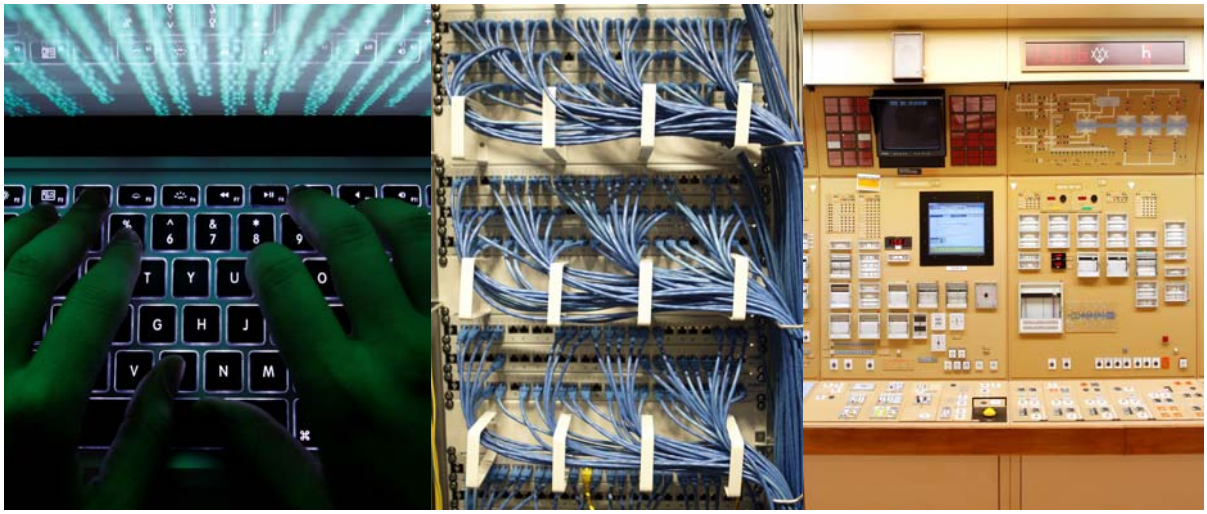
COUNCIL *on* FOREIGN RELATIONS

*Center for Preventive Action*



*CONTINGENCY PLANNING MEMORANDUM NO. 24*

# Strategic Risks of Ambiguity in Cyberspace

Benjamin Brake

May 2015

# Author Bio

**Benjamin Brake** is an international affairs fellow at the Council on Foreign Relations and a foreign affairs analyst in the Bureau of Intelligence and Research at the U.S. Department of State. The views expressed in this paper are those of the author and do not necessarily represent those of the Department of State or the U.S. Government.

## *INTRODUCTION*

As major powers increasingly rely on digital networks for critical services, the number of plausible network attacks, accidents, or failures that could trigger or exacerbate an international crisis will increase. The likelihood and severity of such a destabilizing event will also grow as long as norms of appropriate behavior in cyberspace are underdeveloped, timely and convincing attribution of attacks remains difficult, and the number of cyber-capable actors increases. Preparing for or responding to such a crisis is complicated by ambiguity in cyberspace, primarily regarding responsibility and intent. Ambiguity about who is responsible for a cyberattack exacerbates the risk that countries amid a geopolitical crisis will misattribute an attack, unduly retaliate or expand a crisis, or be unable to attribute an attack at all, thereby preventing or delaying a response and weakening their deterrence and credibility. Ambiguity of what is intended complicates a country's ability to distinguish between espionage operations and activity conducted in preparation for a cyberattack. The United States has strategic interests in preventing and mitigating these risks, given its commitment to global security and overwhelming dependence on networked systems for national security missions, commerce, health care, and critical infrastructure. The longer it takes to implement preventive and mitigating steps, the greater the likelihood of unnecessary military conflict in and outside of the cyber domain.

## *THE CONTINGENCIES*

Cyberattacks are increasing in frequency, scale, sophistication, and severity of impact, including their capacity for physical destruction. China, Iran, North Korea, and Russia have demonstrated an ability to conduct destabilizing cyber activity. Such actions—whether for destructive purposes, intelligence collection, or economic espionage—are designed to evade network defenses and can involve various means of deception to thwart attribution. Recent incidents have shown that U.S. adversaries can no longer assume they will be able to conceal their identities in cyberspace, but cybersecurity experts still lack agreed-upon standards for attribution; evidence for a credible and convincing attribution can take a long time to compile; and malicious actors continue to develop new means of obscuring responsibility. Moreover, unlike many cyber operations designed to exfiltrate large amounts of data, destructive cyberattacks can be made to operate with limited communication between the malware and controller, offering fewer forensic details to establish responsibility. Even when an attacker can be identified, public attribution will remain as much a political challenge as a technical one, given that competing allegations of responsibility will likely follow any public accusation. Without corroborating signals or human intelligence—which, if it exists, officials may be reluctant or slow to disclose—computer forensic data may be incomplete or too ambiguous to convince a skeptical public. Should a major cyberattack occur over the next twelve to eighteen months, or even beyond that period if sufficient preventive and mitigating steps are not taken, public pressure to respond could outpace the time needed to credibly attribute responsibility and, if desired, build an effective coalition to support a response. Over the same time period, ambiguity regarding the intent of cyber operations will also remain a challenge, leaving policymakers uncertain about whether malware discovered on a sensitive system is designed for espionage or as a beachhead for a future attack.

The United States could face several plausible crises over the next twelve to eighteen months that would be complicated by the risks of ambiguity in cyberspace. These include destructive insider

threats, remote cyber operations that threaten trust in financial institutions, and cyberattacks by foreign nations or nonstate groups against critical infrastructure systems that cause widespread panic and loss of life, or similar attacks against a U.S. ally. National Security Agency (NSA) Director Admiral Michael Rogers warned in late 2014 that he expects U.S. critical infrastructure—assets essential to the function of a society and economy, such as water supply systems, electric grids, and transportation systems—to be attacked, noting that multiple foreign nations and groups already possess the ability to shut down a U.S. power grid and several others are investing in the capability. Attacks like the publicly unattributed January 2015 cyberattack that severely damaged a German steel mill suggest the ability to bring about physical destruction through cyber means may be proliferating quickly. Of particular concern would be the proliferation of these capabilities among terrorist groups, which currently possess limited technical skills but destructive intent. As the number of cyber-capable adversaries grows, so too does the number of critical targets, especially as industrial control systems move to web-based interfaces and more common operating systems and networking protocols.

The implications of any crisis will depend on the current geopolitical context; the type of networks that fail; and the extent of economic damage, physical destruction, or human costs that result directly from network failure or its cascading effects on public health, communication and financial networks, and the economy. A successful cyberattack against one or more critical infrastructure systems could endanger thousands of lives, halt essential services, and cripple the U.S. economy for years. Two plausible factors that could exacerbate such a crisis are intentional and inadvertent ambiguity.

**Intentional Ambiguity**

Over the past two years, Iran and North Korea have appeared most willing to conduct destructive and disruptive cyberattacks against U.S. and foreign targets while attempting to conceal responsibility. Tactics have included data wipes, destruction of computer hardware, and denial-of-service attacks. Russia and China have exhibited some of the most advanced capabilities, and actors in both countries have been linked to disruptive attacks during regional tensions. Actors in South Asia and the Middle East have also conducted operations in regional conflicts that could quickly entangle U.S. interests. During a crisis involving the United States or an ally, any one of these countries could conduct cyber operations that risk further destabilization. As the rate of operations grows, so too could the challenge of attribution, with each incident exposing tools and techniques that can be repurposed.

Cyber activities that could not be promptly attributed have already appeared in several conflicts. Though most have rarely elevated beyond nuisance, others have caused significant damage or threatened escalation. In 2008, Russia-based actors launched a wave of attacks against Georgian targets, and similar malware appeared in operations against Ukraine in 2014. Japanese networks are frequently targeted, including during heightened Sino-Japanese territorial tensions and sensitive anniversaries, with origins reportedly traced to China. North Korean cyber actors are suspected of having conducted destructive operations that compromised South Korea's national identification system—damage that may cost more than $1 billion and over a decade to repair. In 2014, U.S. officials blamed North Korea for destructive attacks against Sony Pictures Entertainment, an American subsidiary of the Japanese company Sony. North Korean officials deny the country's role in these attacks and will likely seek to similarly obscure their hand in attacks during future crises to deter or delay a potential American or South Korean response.

U.S. officials suspect Iran's involvement in a 2012 cyberattack against two energy firms, one in Saudi Arabia and another in Qatar, that destroyed data and crippled thirty thousand computers, possibly in retaliation for alleged U.S. cyber operations, and to demonstrate an ability to conduct similar attacks against U.S. targets. U.S. financial firms subsequently suffered tens of millions of dollars in losses resulting from Iranian denial-of-service attacks launched in retaliation for economic sanctions. In 2014, Iran became the first country to carry out a destructive cyberattack on U.S. soil when it damaged the network of Las Vegas Sands after its chairman advocated a nuclear strike against the country.

### Inadvertent Ambiguity

Due to the difficulty of determining whether certain activity is intended for espionage or preparation for an attack, cyber operations run the risk of triggering unintended escalation. Espionage malware that could be reprogrammed to gain control of networks, such as BlackEnergy, which has been discovered on critical infrastructure networks, may be viewed by victims as one update away from becoming an attack tool capable of crippling energy supplies, water-distribution and -filtration systems, or financial transactions. Security scans of networks intensified amid heightened geopolitical tensions could reveal such malware and prompt fears of an imminent attack, even if the malware was implanted for espionage purposes long before the crisis began. The difficulty of predicting a cyber operation's effects and the interdependency of networked systems increase the risks that an operation will inadvertently spill over onto sensitive systems or cause unintended effects.

One example of ambiguity and the risk of misperception is the 2010 discovery on Nasdaq servers of malware similar to a cyber tool reportedly developed by Russia's Federal Security Service. Initial assessments maintained that the malware was capable of wiping out the entire stock exchange. Only later was it shown to be less destructive, according to media accounts. Such ambiguities during periods of heightened geopolitical tensions pose significant escalatory risks. Information security experts have raised similar concerns about other Russia-linked activity and questioned whether aspects of the activity are intended to insert offensive capabilities into critical infrastructure systems for future use.

Ambiguity also arises in the case of "worms"—self-replicating malware that seeks out other computers to infect. Worms can spread so pervasively that their origin and intent can be difficult to infer from known victims. One worm, Conficker, spread to millions of computers and disrupted military communications in several European countries. Its creator and purpose remain unknown.

## *WARNING INDICATORS*

Indicators of activity with the potential to create or exacerbate an international political crisis include leadership statements of an intent to conduct or permit computer network operations against foreign networks; evidence of that intent, including research and development, budgetary allocations, or organizational changes, such as the creation of offensive cyber forces; the express or tacit acceptance of parastatal hackers; and a demonstrated capability to conduct computer network operations, including cyber-espionage and cyber operations against domestic targets.

Tactical warning indicators resemble traditional conflicts, such as changes in the alert status of military units and an increase in crisis-related rhetoric. Indicators unique to cyber operations include increased efforts to probe foreign networks and an uptick of activity in online hacker forums discussing foreign targets and tools, techniques, and procedures appropriate for operations against them.

## *IMPLICATIONS FOR U.S. INTERESTS*

First, cyberattacks will eventually be part of every nation's military strategy. The United States depends on information communications technologies for critical military and civilian services far more than its strategic rivals or potential adversaries. U.S. officials have noted an increase in computer network operations targeting state, local, and privately operated critical infrastructure, some of which have the potential to cause considerable harm to operations, assets, and personnel.

Second, ambiguity in cyberspace elevates the risk that a significant cyber event amid a geopolitical crisis will be misattributed or misperceived, prompting a disproportionate response or unnecessary expansion of the conflict. Such an escalation would impair the United States' prominent role and interest in global security and its commitment to international law.

Third, U.S. officials' ability to respond swiftly and effectively to cyberattacks is complicated by the difficulty of timely public attribution and ambiguity over what type of cyberattack would trigger a right to self-defense or security commitments to strategic partners. A failure to confidently attribute an attack or determine whether such activity constituted an attack could limit U.S. response options. Such confusion, uncertainty, and delay could weaken deterrence and the credibility of U.S. assurances, trigger a misperception of U.S. commitment, and undermine a U.S.-led coalition.

## *PREVENTIVE OPTIONS*

Unilateral and bilateral steps offer the most immediate path for preventing and mitigating risks of ambiguity. Diverse interests and challenges that inhibit verification limit the likelihood and effectiveness of a comprehensive international agreement in the near term. The United States has two broad sets of policy options.

*The United States could enhance deterrence by strengthening defenses, building and supporting more resilient networks, and bolstering the capacity and credibility of U.S. retaliatory threats.*

- *Improve cyber defenses, elevate the role of the private sector, and support research.* Government agencies and the private sector, which owns and operates the majority of critical networks on which the United States relies, should be encouraged to build and operate better defenses. Congress has considered several competing pieces of legislation to establish a legal framework that would encourage sharing of best practices and vulnerabilities between the public and private sectors. The disclosure of significant cybersecurity failures would expand awareness of threats and successful defenses, reduce duplicative efforts, improve the quality of cybersecurity products, and support market mechanisms to develop network security, such as the cybersecurity insurance market.
- *Intensify testing of national cyber defenses.* The Department of Homeland Security, the intelligence community, and relevant state, local, and private actors could expand national training exercises to clarify responsibilities and demonstrate capabilities, such as the CyberStorm series. Cyber exercises can showcase resiliency and improve incident response, and should include disaster-response operators to simulate health and safety issues that could accompany a major attack.
- *Improve real and perceived attribution.* A credible retaliatory threat will depend on perceptions of U.S. attribution capabilities. To showcase this capability, U.S. officials could expand intelligence collection against potential adversary cyber programs and increase public or government-to-

government disclosures of intrusions. Intelligence, defense, and law enforcement officials could develop standards of attribution confidence that can be used to recommend levers of national power, including judicial, economic, diplomatic, intelligence, and military tools, as well as network actions, such as slowing or blocking Internet traffic to and from U.S. and allied networks. Modeled on legal burdens of proof, these standards could shorten the time it takes for U.S. agencies to recommend response options. U.S. officials could also support efforts to reduce anonymity on the Internet, including adjustments to the design, distribution, and authentication of Internet protocol (IP) addresses, but such reforms would come at too great a cost to free expression.

- *Clearly define and enhance the role of the Cyber Threat Intelligence Integration Center (CTIIC) to ensure effective planning, coordination, and assignment of cyber operations.* Congress can enhance U.S. cyber posture by codifying CTIIC's role in integrating intelligence for the director of national intelligence and serving as an interagency forum to coordinate roles and responsibilities. The special assistant to the president and cybersecurity coordinator essentially serves as an interagency coordinator, but his or her portfolio is expansive and staff is small. An enhanced CTIIC, on the other hand, could ensure united efforts and report operational issues directly to the White House; these measures could improve operational awareness and guard against inadvertent escalation.
- *Promote greater public clarity on U.S. cyber strategy and doctrine.* Uncertainty over what amounts to a use of force in cyberspace can weaken deterrence if potential adversaries misperceive thresholds for retaliation. National security officials can reduce risks of miscalculation by more clearly defining how the United States perceives "use of force," "armed attacks," "aggression," and activity below those thresholds. Some uncertainty is unavoidable to ensure flexibility in the context of an attack, but more clarity would promote stability by shaping expectations of behavior.
- *Make good on (and use of) retaliatory threats.* U.S. deterrence rests on credible assurances that the United States will retaliate strongly against perpetrators—both in and outside of cyberspace. When responsibility can be established, the White House could inflict costs on the offender that also have a deterrent effect on other potential adversaries. This could include an expanded offensive cyber capacity that provides policymakers with a wider range of options, but because operations in cyberspace may be noticed only by adversary network operators, they will likely have greater effect as part of a broader campaign that includes responses outside of the cyber domain, including use of the recently announced sanctioning authority targeting malicious cyber actors.

*The United States could establish responsible cyber precedents and norms.*

- *Intensify ongoing diplomatic efforts to promote the development of shared norms and expectations.* Consensus on controversial issues relating to how international law applies to state behavior in cyberspace is unlikely in the near term. The diversity of national interests and verification challenges makes efforts to build cyber norms through formal treaties especially challenging. Given the risk of inaccurate attribution in cyberspace, however, countries should recognize a high threshold for what merits a forceful retaliation and remain mindful that the benefits of international communications technology come with vulnerabilities and defensive burdens. U.S. efforts to build such a shared understanding could include operational restraint; continued diplomatic work in the UN Group of Governmental Experts on international information security; confidence-building measures, such as joint cyber exercises that standardize bilateral attribution, mitigation, and data-sharing procedures; and the expansion of bilateral consultative mechanisms.

- *Further clarify roles and responsibilities in the cyber domain.* Congress could take several steps to elevate the role of diplomacy in U.S. cyber policy, better integrate cyber capabilities into military strategy and doctrine, ensure effective oversight, and signal the important distinction between cyber espionage and other types of cyber operations. These steps include establishing an assistant secretary of state for Internet and cyberspace affairs and ending the current policy that places a single official in charge of both the NSA and U.S. Cyber Command. A reallocation of responsibilities would further distinguish Title 10 (national defense) and Title 50 (covert) operations and help generate precedents of responsible state practice for each.
- *Enhance support for foreign efforts to combat cybercrime.* International cooperation is essential to combat illicit cyber activity from nonstate actors, such as terrorist networks, criminal groups, and patriotic hackers. Greater resources for international programs of the Department of Justice (DOJ) and streamlining how foreign officials receive DOJ assistance in cyber investigations would reinforce the norm of mutual assistance and pressure foreign governments to do likewise.

## *MITIGATING OPTIONS*

- *Establish or use a crisis-management group with allies and countries hosting affected networks.* The same elements of ambiguity that can trigger a crisis can also exacerbate one. Because defensive cyber operations, which may be appropriate during an ongoing attack, can involve activity on information networks located in other countries and appear offensive in nature, the public or private messaging of a U.S. response will be vital to prevent crisis escalation or expansion. Such crisis-management groups should include top national security and diplomatic officials, and cyber officials from other countries' computer emergency response teams, to build a foundation of familiarity and trust among relevant actors that would be called on in the wake of a major attack.
- *Work with potential adversaries to prevent misperception of U.S. cyber activity*. Given varying structures of cyber forces within the security agencies of potential adversaries, a U.S. signal sent by cyber means during a crisis may not reach national leaders. U.S. national security officials could establish or expand bilateral crisis-communication channels with foreign counterparts to issue warnings, request assistance, or open a dialogue about state involvement in a perceived attack.
- *Pressure states unwilling to stop or support investigations of cyberattacks.* In cases where the United States cannot attribute a cyberattack, it has levers short of force both in and outside of the cyber domain. Countries whose networks are used in a multistage attack could be given notice that a failure to stop it or to support an investigation is a breach of state responsibility that could result in adjustments to network traffic, diplomatic condemnation, or other sanctions. Such threats increase incentives to conduct cooperative forensics, develop mitigation measures, and make their information infrastructure a less attractive path for hostile computer network operations.

## *RECOMMENDATIONS*

Prospects for a comprehensive international solution to the risks posed by ambiguity in cyberspace are limited at this time, and some technical fixes that would aid attribution by limiting anonymity online would come with too great a social cost. Instead, a strategy that focuses on fortifying U.S. networks, building a more credible deterrent, and demonstrating responsible state practice offers the best path forward.

*The United States should improve the security and resilience of its networks and fortify the credibility of retaliatory capacity.*

- Congress should pass legislation that facilitates real-time information sharing within and between the private and public sectors. Implementation of this information-sharing program is expected to cost $20 million over five years, according to the Congressional Budget Office.
- Congress should build on the February 2015 executive order designed to promote information sharing among private actors by offering tax incentives or grants to companies that join and support the work of information-sharing and analysis organizations—sector- or region-specific hubs that facilitate the exchange of cyber-threat data and cybersecurity best practices.
- Congress should help reduce critical vulnerabilities by expanding support for the new National Cybersecurity Federally Funded Research and Development Center (FFRDC); creating or incentivizing bug bounty programs for critical systems; adjusting criminal and civil laws, such as the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act, to enable and encourage responsible security research; and mandating robust cybersecurity requirements as a condition for federal-procurement eligibility to drive the commercial market for secure products.
- The Department of Defense (DOD) should expand efforts to improve cyber defense capabilities, information-assurance responsibilities, and research and development. DOD officials estimate this to cost $5.5 billion annually. Joint training exercises in the combatant commands ($456 million requested by DOD for 2016) should include cyber threats that could impede global access and operations to improve DOD mission resilience, support the development of best practices to share with critical infrastructure operators, and generate data to help avoid costly adjustments to hardware, firmware, and other fixes in later development stages.
- The Office of the Director of National Intelligence (ODNI) should expand signals and human intelligence collection against potential adversary cyber programs, as well as accelerate the intelligence community's production and release of actionable cybersecurity information to vital information network and critical infrastructure operators. U.S. intelligence officials should also identify, in advance, types of classified data that could be shared publicly in the event of an incident to avoid a lengthy interagency declassification process that would delay a timely public attribution.
- When possible and appropriate, DOD officials should highlight U.S. involvement in offensive cyber operations against states, terrorist groups, and other illicit actors to fortify the credibility of U.S. retaliatory capacity among potential adversaries. Greater transparency into offensive cyber operations, as well as the doctrine underlying them, would also reinforce emerging norms in cyberspace by demonstrating responsible state practice and supporting U.S. efforts to overcome the skepticism of its commitments to shared interests and values in cyberspace that emerged in the wake of unauthorized disclosures of U.S. cyber activity.

*The United States should elevate diplomacy, clarify doctrine, and ensure clarity between intelligence and military cyber operations.*

- Congress should create a Department of State (DOS) Bureau of Internet and Cyberspace Affairs to demonstrate that the United States gives as much attention to diplomatic policy options as it does military ones. The bureau should retain a direct reporting line to the secretary for threats, operations, and related strategic considerations. Congress should also make the NSA director a

Senate-confirmed position eligible for civilians. Missions other than intelligence should be shifted to other appropriate entities, including U.S. Cyber Command and the combatant commands.

- ODNI should more frequently review intelligence priorities, operations, and targets to prevent unintended escalatory cyber events. The reviews should also clarify the chain of command and congressional oversight of Title 10 and Title 50 cyber operations. The director of CTIIC should facilitate reviews and broaden operational awareness among national security officials.
- DOD should further clarify doctrine related to cyber-effects operations to provide greater transparency into U.S. operations, reduce risks of miscalculation, and clarify response options.

*The United States should intensify diplomacy in concert with like-minded nations to promote the development of shared norms and expectations of appropriate behavior in cyberspace.*

- DOS should expand formal dialogues with partners and potential adversaries to share views on appropriate behavior in cyberspace, including prohibitions against operations that damage critical infrastructure or computer emergency-response agencies, as well as affirmative norms, such as mutual assistance in investigations or efforts to counter ongoing attacks.
- The White House should publicly outline for less cooperative states the possible range of political-economic levers, including adjustments to network traffic, criminal sanctions, diplomatic condemnation, and U.S. Treasury actions that the United States could use to hold countries accountable for failing to stop harmful activity conducted from or through their networks.

*The United States should improve responsiveness to foreign requests for assistance in cyber investigations.*

- Congress should increase support for the DOJ's Computer Crime and Intellectual Property Section, National Security Division, Office of International Assistance, and Federal Bureau of Investigation to bolster prosecutorial efforts and keep pace with the growing number of foreign requests for support. DOJ estimates this to cost $722 million.
- Congress should support DOJ efforts to provide prompt support to cyber investigations including creating an online system to process requests. DOJ estimates this to cost $24.1 million.

## CONCLUSION

Attacks against the diverse and growing number of vulnerabilities on critical U.S. networks will pose a significant risk of triggering or aggravating a crisis for years to come. Though the cyber threat cannot be eliminated, implementing the recommendations above would put the United States on a course to better manage its risks and promote stability. The United States should act now to enhance its cyber defense and deterrence, support the growth of shared norms, and improve the processes through which attacks are mitigated and investigated. The longer the United States delays taking these steps, the harder it will be to prevent and mitigate a crisis. Deterrence failures and misperceptions occur routinely in international relations, but a renewed focus now would significantly reduce the risk of an unnecessary crisis or escalation.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries.

**The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All statements of fact and expressions of opinion contained in its publications are the sole responsibility of the author or authors.**

The Center for Preventive Action (CPA) seeks to help prevent, defuse, or resolve deadly conflicts around the world and to expand the body of knowledge on conflict prevention. The CPA Contingency Roundtable and Memoranda series seek to organize focused discussions on plausible short- to medium-term contingencies that could seriously threaten U.S. interests. Contingency meeting topics range from specific states or regions of concern to more thematic issues and draw on the expertise of government and nongovernment experts.

*The Council on Foreign Relations acknowledges the Rockefeller Brothers Fund for its generous support of the Contingency Planning Roundtables and Memoranda.*

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.