Research Report

DANIEL EGEL, GABRIELLE TARINI, RAYMOND KUO, ERIC ROBINSON, ANTHONY VASSALO

Can the United States Deter Threats from Uncertain Origins?

Examining the Cases of Havana Syndrome, SolarWinds, and the Chinese Mafia

For years, a diplomatic mystery spanning multiple countries—involving speculation about foreign adversary attacks and high-tech, undetectable weapons—vexed U.S. officials. The mystery began in late 2016, when diplomats and intelligence officers at the U.S. embassy in Cuba reported hearing strange sounds, followed by headaches, dizziness, blurred vision, and memory loss. Since then, similar incidents—which the U.S. government has termed *anomalous health incidents* but are colloquially known as *Havana Syndrome*—have been reported by U.S. government personnel in 70 different countries, including China and Russia.[1]

Debate has raged within U.S. government agencies over whether such events are merely a medical anomaly or actually the product of a nation-state or nonstate actor attack on U.S. officials around the globe. The Central Intelligence Agency (CIA) and the U.S. Department of State have established numerous panels and analytical teams to investigate the cause of the incidents. No U.S. rival has taken public responsibility. The incidents sent the intelligence and diplomatic communities into a years-long tailspin involving more questions than answers. In March 2023, the U.S. Intelligence Community (IC) judged that it was unlikely or very unlikely that a foreign adversary bore responsibility for Havana

KEY FINDINGS

- The ability of the United States to respond effectively to a threat is limited when the attribution, nature, and method of the threat are ambiguous.
- Maintaining this level of ambiguity likely constrains the scale at which U.S. adversaries can deploy these approaches, but the costs the approaches impose can be large.
- Despite the appeal of other deterrence or punishment strategies, denial-by-defense is likely to be the only approach capable of reducing the efficacy of these threats.

Syndrome, although agencies varied from low confidence to moderate to high confidence in this judgment—leaving some level of ambiguity in the IC's assessment.[2]

Nevertheless, the mystery surrounding Havana Syndrome illustrates the challenges of mustering a response to a national security threat when both the threat and the underlying method and actor behind the threat are not understood with certainty. Traditionally, states will seek to prevent adversary aggression through *deterrence*, or efforts to discourage or restrain a rival from taking unwanted actions. If an adversary's aggression is already underway, states will seek to *compel* their rivals to stop taking such actions or pursue an alternative approach.[3]

But how can states deter an adversary from violence—or compel such violence to end—if the aggressor successfully masks their role in perpetrating the violence and creates uncertainty about whether violence has even occurred?

Beyond the academic debate, this challenge has become an increasingly prominent issue in modern competitive statecraft, particularly in terms of how states and nonstate actors signal and shape the behavior of rivals short of outright, conventional war. The further development of cyberspace and other types of nonlethal, indirect weapons may prompt these sorts of unattributable incidents to occur with greater frequency in the future.[4] This report is a preliminary, exploratory analysis that examines the applicability of existing baseline concepts for deterrence and compellence in the context of three contemporary short case studies, in which attacks against U.S. interests are believed to have occurred through origins that are unknown or uncertain and in which questions remain regarding whether coercive violence was actually deployed. In addition to Havana Syndrome, we also explore the SolarWinds breach, in which hackers believed to be linked to Russian intelligence targeted American companies and U.S. government agencies, and the Chinese Communist Party's connections to organized crime syndicates around the world. We do not explore these cases in significant depth or detail. We focus primarily on examining the unique characteristics of each case that make deterrence and compellence difficult.

Structure of This Report

The report begins with a brief discussion of the deterrence and compellence literature. We develop a simple framework to understand deterrence and compellence approaches in the context of our three case studies. In the subsequent sections, we briefly explore, for each case, how these approaches could be applied to deter, dissuade, or compel an end to violence to U.S. interests from unknown threat actors. The report concludes with a brief discussion of the implications for U.S. government policymakers on how to address such threats going forward.

Understanding Deterrence and Compellence

In the cases of Havana Syndrome, SolarWinds, and Chinese government engagement with organized crime, the U.S. government is seeking to prevent or stop hostile foreign actors from taking actions that are harmful to its people, institutions, and interests. At their core, U.S. strategies to respond to threats from adversaries typically seek to reduce the prospective benefits or increase the prospective costs of an adversary's attack to persuade an adversary to avoid taking or stop taking the unwanted action.[5] In this section, we briefly review the major strategies and methods the United States traditionally uses to prevent unwanted adversary aggression.

The United States, broadly speaking, uses two complementary but theoretically distinct approaches for incentivizing adversaries to behave in a particular way: deterrence and compellence.[6] *Deterrence* involves actions to discourage or restrain an adversary from taking unwanted actions. The related concept of *compellence* involves actions to force an adversary to take desired actions or stop taking unwanted actions if they have already started.[7] Both approaches are examples of interstate *coercion*.

Broadly speaking, the United States has four major methods of coercion: denial by defense, the threat of punishment, entanglement, and normative taboos.[8] Denial by defense and the threat of punishment represent scholars' classical conception of coercion; entanglement and norms are part of a broader conception that play a significant role in the modern

era, given the nature of contemporary threats.[9] We briefly review these strategies below. Table 1 provides a short summary.

Denial by Defense

Denial by defense seeks to prevent an adversary's action by "making it infeasible or unlikely to succeed."[10] This typically includes the hardening of the potential targets of attacks, whether through enhanced security (e.g., cybersecurity) or resilience (e.g., social resilience of a population). In addition, where feasible, denial by defense includes the development of capabilities to actively counter the offensive capabilities of adversaries (e.g., countercyber operations, the development of local proxy forces, control of the information environment).[11] Denial by defense features in compellence strategies as well by making an adversary's ongoing aggression unlikely to succeed. For example, air forces may use airstrikes to compel an adversary to stop fighting by interdicting military supplies and destroying key military infrastructure.[12]

Threat of Punishment

In contrast, the threat of punishment operates by threatening to impose severe penalties on an adversary if they attack.[13] These threats can be public, with the defender making public statements declaring its intent to take a specific response in response to an aggressor's action (e.g., a threat to impose sanctions), or taking actions (e.g., mobilizing troops) that are deliberately costly.[14] Private threats (sometimes referred to as *secret diplomacy*) can also signal a defender's intent to carry out specific punitive actions in response to an adversary's aggression.[15] For deterrent threats to be effective, the potential aggressor must "view the defender's threats as credible and intimidating."[16] Threat of punishment also features compellence strategies. For example, returning to the airpower example, air forces use airstrikes to inflict pain on adversaries, but such strikes also signal a defender's intent to escalate and cause future pain if an aggressor does not stop taking the unwanted action.[17]

Entanglement

Entanglement involves a general set of strategies in which a defender establishes relationships with an attacker such that the attacker "will refrain from launching attacks because they themselves will incur costs too."[18] One mechanism is through structural entanglement, in which a defender's interdependencies with an attacker (e.g., economic or technological interdependence) means that any attack by an adversary runs the risk of directly affecting that adversary as well. A more active and adversary-specific approach to entanglement is *inducement*, in which such benefits as confidence-building measures and capacity-building assistance could be removed if an attack occurs.[19]

TABLE 1
Strategies of Deterrence and Compellence

Type	Definition	Examples
Denial by defense	Actions that reduce the benefit expected from an attack	Development of defenses, development of counteroffensive capabilities, interdiction of military supplies, destruction of military infrastructure
Threat of punishment	Threats that communicate punitive actions will be taken in response to certain adversary actions	Threat of sanctions, the threat of nuclear escalation, other actions that signal an intention to inflict future pain
Entanglement	Structures that ensure an attack will also impose costs on the attacker	Structures that create economic or technological interdependence
Normative taboos	Imposition of reputational costs that damage the soft power of an adversary	Public disclosure of information

Normative Taboos

Finally, normative taboos leverage allies, international organizations, civil society organizations, and other actors to prevent or stop unwanted adversary aggression through reputational effects. These strategies focus on "imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack."[20] A common approach for using international norms against an adversary is through public attribution, which changes the "cost-benefit calculus of the adversary through, for example, delegitimization and shame."[21] The usefulness of norms is strongly affected by the degree of attribution that is possible.[22]

Analytical Approach

In the following three sections, we aim to provide an initial exploration of how the traditional conceptions of deterrence and compellence can be applied to our three cases of interest. Previous research conducted at RAND has identified three factors as the most important determinants of the success or failure of deterrence strategies: the intensity of an aggressor's motivation, clarity from the defender on what exactly is to be defended and on the specific actions the defender will take to defend it, and confidence in the mind of the aggressor that the defender actually has the capability and will to carry out the actions it threatens.[23]

Therefore, any successful strategy to prevent or stop adversary aggression must begin with a clear understanding of the potential aggressor and what it values. However, in all three of the cases we explore in this report, attacks against U.S. interests have occurred though relatively unknown or uncertain origins, and there are questions about whether coercive violence was actually deployed. Thus, in each case, U.S. decisionmakers cannot clearly

- identify the attacker (attribution)
- link the attacker to a state actor (sponsorship)
- identify why the attack was conducted and what objectives the attacker aimed to achieve (motivation).

The three case studies vary in terms of the level of certainty surrounding each of these three factors. For example, U.S. officials suspect that Havana Syndrome was an instance of true confusion on attribution. SolarWinds featured attribution to a state that is fairly evident but still difficult to prove. The Chinese mafia case is an example in which the state sponsor is known and could stop the activity but is choosing not to do so.

The subsequent three sections follow the same structure. After a short overview of the context and basic facts of each case, we briefly explore the threat using this simple, three-part framework (attribution, sponsorship, motivation) to illustrate the difficulties of responding to threats from unknown or uncertain origins. We then discuss how the lack of a clear understanding in attribution, sponsorship, and motivation makes each of the four response options discussed above difficult for U.S. policymakers to execute.

Havana Syndrome

Since 2016, approximately 1,000 U.S. officials deployed overseas have experienced unexplained headaches, dizziness, or memory loss—a series of symptoms that, in some cases, have been reported to cause long-lasting and debilitating injuries.[24] The first public reports of the incidents were from the U.S. embassy in Cuba in 2016, from which the term for the incidents, *Havana Syndrome*, was coined. However, since then, public reporting has emerged on similar incidents at U.S. overseas missions in Austria, China, India, Russia, Serbia, and Vietnam and even on U.S. soil.[25]

The United States is now investigating whether the Havana Syndrome might be the result of the actions, deliberate or otherwise, of a foreign power.[26] In February 2022, an IC scientific panel of experts concluded that the injuries suffered by people in this smaller subset of cases were most likely caused by "pulsed electromagnetic energy, particularly in the radiofrequency range."[27] The findings of this panel expanded on a 2020 report from the National Academies of Sciences, Engineering, and Medicine (NASEM), which also found that pulsed electromagnetic energy was the most plausible explanation for the injuries.[28]

In March 2023, the IC released an updated assessment in which seven intelligence agencies judged that it was unlikely or very unlikely that a foreign adversary bore responsibility for Havana Syndrome. Agencies varied from low confidence to moderate to high confidence in this judgment.[29] The IC has thus not yet reached consensus on the issue, and some ambiguity remains.

Regardless of whether a state actor was responsible, the potency of a threat like Havana Syndrome is primarily in the uncertainty it creates for U.S. government personnel deployed abroad and the bureaucratic time and energy that U.S. diplomatic and intelligence agencies must spend trying to muster a response with little information. Whether or not Havana Syndrome is a global phenomenon, whether it affected only two dozen people, or whether it affected no one at all is, in some ways, not the most important thing. An adversary needs only to create the perception that it has the ability to clandestinely use technology to harm U.S. personnel at U.S. embassies around the world for such a coercive attack to have its desired effect.

Response Options

This subsection discusses the feasibility of options that the United States could incorporate into a tailored response to Havana Syndrome—or attacks in which the actor is unknown and uses low-technological means that are difficult to detect. U.S. options for deterring the possible antagonist in the Havana Syndrome incidents, as with all threats from potential aggressors, are determined by the unique characteristics of the threat:

- **Attribution**: The perpetrator, if there is indeed a foreign actor involved, is unknown because the possible technology causing the symptoms is poorly understood and because similar symptomology is associated with other environmental and medical characteristics.
- **Sponsorship**: The attacks could be state-sponsored, given the sophistication of the incidents and the similarity of the symptomology to injuries experienced at the U.S. embassy in Moscow in the 1960s, but the type of perpetrator (e.g., state, proxy, nonstate) is currently unknown. Attacks have been reported to occur on every continent, including within China, Russia, and the United States, obfuscating the identity of the sponsor. If the incidents were state-sponsored, it would be difficult for any service or entity to operate without the knowledge of the host intelligence service.
- **Motivation**: The incidents may be occurring as an unintended consequence of an espionage effort, a deliberate attempt to harm U.S. officials, or both or for another reason altogether. Individuals with certain profiles (e.g., IC personnel) have purportedly been specifically targeted.

Denial by Defense

A denial by defense response to Havana Syndrome or incidents with similar characteristics would harden the force by developing or implementing the technologies and behaviors to detect and deflect pulsed electromagnetic energy—thought to be the most likely source of the attacks. Detection would enhance the U.S. ability to identify additional information in real time about the cause and source of the attack. Deflection would harden U.S. personnel and facilities to deny the adversary confidence in the expected benefit of an attack.

Enhancing U.S. capabilities to detect Havana Syndrome would deny the adversary the ability to conduct attacks on U.S. personnel in a clandestine manner (a critical component of the nature of the threat), potentially increasing their chances of being discovered. For example, the NASEM report highlights the importance of taking steps to detect a possible attack if and when it occurs. The report notes:

> Tremendous advances are being made in sensor technology that provide the means for stationary, personal, or wearable devices that capture signal or material or both for evaluating the presence of chemical, biological, or physical agents.[30]

DoD has sought to develop a "wearable RF [radio frequency] detector to signal and document exposure to injurious levels of RF energy."[31] "Such

sensors could be randomly and routinely deployed or be available for response under circumstances when there is concern" about possible Havana Syndrome incidents.[32]

In addition to detection, deflecting the attack from U.S. personnel would reduce the expected benefit an adversary gains from the attack. For example, U.S. government buildings and facilities could be hardened against attack. Behavioral adaptions for deployed U.S. personnel, such as "getting off the X"—immediately leaving the area where symptoms are experienced—may also be an effective way to "stop the symptoms and limit their lasting severity," again denying a possible adversary the expected benefits of an attack.[33]

Increasing detection capabilities, hardening U.S. facilities and personnel, and encouraging behavioral adaptation are relatively simple solutions that could be pursued as part of a denial-by-defense approach, although hardening all locations where U.S. personnel are present that an adversary could target would be costly. While such denial measures are unlikely to comprehensively block a determined adversary employing pulsed electromagnetic energy against U.S. deployed personnel, they may provide some measure of protection and have the added benefit of providing psychological benefits for deployed U.S. personnel.

Threat of Punishment

The threat of punishment is extremely difficult without clear attribution. The United States cannot issue clear threats of punishment in response to given actions without being certain of who the actor is. In the case of Havana Syndrome or incidents with similar characteristics, the aggressor's role cannot be clearly identified or proved in a specific event or action. Moreover, because Havana Syndrome incidents have unfolded slowly and steadily over the course of seven years, no one incident has proven to be a "rallying point" for the threat of punishment.[34]

However, as Joseph Nye notes in his analysis of the challenges of cyber attribution, "attribution is a matter of degree . . . the problem of attribution should not be belittled, but imperfect attribution does not prevent some degree of threat of punishment."[35] For example, U.S. officials have long considered Russia a leading suspect in the Havana Syndrome incidents. Analysts have also reasoned that conducting an attack like the Havana Syndrome is consistent with Russia's past attacks—such as the use of traceable radioactive poisons to kill or attempt to kill individuals in foreign countries, including in Europe.[36] Russia has both the means and the motives to carry out such an attack—indeed, the Soviet Union targeted the U.S. embassy in Moscow with microwaves for decades.[37] However, Russia having these capabilities and intentions does not provide sufficient grounds for the United States to issue a threat directed at Moscow publicly.

However, even with imperfect attribution, U.S. officials may use private threats to articulate precisely what they are reacting to and what they will do in response if the suspected behavior does not stop. For example, when CIA Director William Burns traveled to Moscow in December 2021, he raised the issue of the health incidents and said, "if Russia was found responsible, there would be consequences."[38]

Still, there are significant risks to issuing even private threats of punishment without a reasonable measure of certainty about who is responsible for the attack. Particularly with peer adversaries, issuing threats of punishment risks escalation. Going after the wrong adversary in public could also play into the real perpetrator's intent—to generate confusion and make U.S. officials look incompetent. Attribution is a significant factor in deterrence by threat of punishment and, thus, is largely infeasible for Havana Syndrome when U.S. officials remain uncertain about who is conducting the attacks, if anyone.

Entanglement

Entanglement seeks to leverage the interdependencies between attackers and victims to impose costs on the attacker for conducting the attack. Unlike deterrence by threat of punishment, some degree of attribution or a full understanding of an adversary's specific motivation is not entirely necessary for entanglement to work. For example, in the case of Havana Syndrome or incidents with similar characteristics, the ability of all countries to provide services to citizens around the world and conduct diplomacy depends

heavily on the safety and security of diplomats serving in embassies overseas. Keeping diplomats working abroad safe is highly valuable to most nations. All countries benefit from this status quo and its continuation.

One method of entanglement would be, for example, to mobilize the international community to affirm their commitment to keeping diplomats safe and repudiate attacks against diplomatic personnel working in embassies overseas—perhaps through a United Nations General Assembly vote or other public declaration. Nations that did not sign on would be marginalized and perceived to be involved in such behavior. It is possible that nations would sign onto a pact and still perpetrate attacks against deployed U.S. personnel. However, an entanglement strategy would raise the risks of doing so because it would make discovery of a country's involvement all the more damaging.

Normative Taboos

Normative considerations can deter actions by imposing reputational costs on aggressors that outweigh the value gained from an attack. However, like deterrence by threat of punishment, "naming and shaming" is almost impossible without attribution. There are certainly norms against attacking adversary's diplomats and spies. During the Cold War, for example, the United States and the Soviet Union operated under an understanding known as the "Moscow Rules," under which both countries agreed not to target each other's intelligence officers or diplomats with physical attacks.[39] However, for the costs of breaking the taboo to outweigh the benefits gained, an attacker must be able to be publicly identified and subjected to widespread international condemnation.

In the case of Havana Syndrome or incidents with similar characteristics, the IC does not have information connecting the incidents to a perpetrator it feels sufficiently confident in to release publicly. The government may also be reluctant to release too much information to the public because doing so could reveal techniques for detecting and countering the attacks. If the government suspected an adversary in the attacks but did not have information to definitively accuse them publicly, U.S. officials could accuse the actor privately and leak that fact that they blamed them publicly—potentially the thinking behind *New York Times* reporting of CIA Director Burns' private threat to Moscow on Havana Syndrome.[40] In this way, the target could potentially gain some of the benefits of naming and shaming without having to admit outright that they were not fully confident in their accusation.

SolarWinds

In late 2020, evidence began to emerge that SolarWinds' Orion software, which monitors and manages access on private sector and federal networks, had been hacked.[41] SolarWinds is an software and information technology company headquartered in the United States that provides services to nearly all Fortune 500 companies and multiple federal agencies. This was the largest confirmed digital supply chain attack, in which a compromised computer system propagated the threat to downstream clients. The malware was hidden inside a routine software update, which SolarWinds estimates 18,000 Orion customers downloaded between March and June 2020.[42] Unlike other cybercrime, this attack was unusual in that it does not appear that financial institutions were the primary targets. Instead, the hackers accessed U.S. federal departments and agencies, including the departments of Defense, State, and Justice, as well as 37 defense industry companies.[43]

The attackers were highly sophisticated and, as a result, there is still uncertainty surrounding who was responsible for the attacks.[44] The code was wiped of any country-of-origin signifiers, and the attackers reverse-engineered SolarWinds' communication protocols with servers, mimicking the company's syntax and formats. In fact, the attack was first detected only when an employee with FireEye, a cybersecurity firm using Orion, happened to notice that a colleague had two phones registered on their network.[45] The U.S. government says it confirmed that the actor that perpetrated the attack was Cozy Bear, a hacker group associated with the Russian Foreign Intelligence Service. However, Russia has denied responsibility.[46]

Another, possibly China-based group separately hacked Orion.[47]

Although there is no definitive evidence, the goal of the SolarWinds hack appears to have been information monitoring and extraction, not theft, capability degradation, sabotage, or subversion. However, the same access that gave the actor the ability to steal data could also have allowed the actor to alter or destroy the data.[48] The Department of Defense declared that, although about one-third of its systems were infected, none were used before the security gap was patched.[49]

Containing and fixing the damage caused by the SolarWinds attack could cost "hundreds of billions of dollars."[50] More worrying still, this attack's dwell time—the length of time between when a hacker gains system access and when the attack is actually discovered—was well over a year, as compared to 95 days for the average attack.[51] The attackers had sufficient time to develop and implant further, unknown malware on affected systems. The hacker could have applied its sophisticated mimicry and fingerprint wiping techniques to these programs, making it even harder to detect these digital surprises. Indeed, FireEye's initial detection of the malware was almost accidental, and the threat actor could have easily continued monitoring affected networks.

Response Options

Like Havana Syndrome, the SolarWinds attack was a threat of uncertain origin, and there were questions regarding whether coercive violence was actually deployed. U.S. options for deterring the possible antagonist in the SolarWind attacks are determined by the unique characteristics of the threat:

- **Attribution**: The U.S. government claims that the hackers were linked to the Russian foreign intelligence service. However, the attacker did an impressive job of wiping any possible digital trails, such that specific, unclassified attribution may not be possible.[52]
- **Sponsorship**: Given the attack's sophistication, the threat actor is likely state-sponsored. Russia has denied responsibility, and there is no public dispositive evidence of sponsorship. Another shade of sponsorship may be if a state sponsor, such as Russia, has the ability to control Cozy Bear but chose not to do so.
- **Motivation**: The attackers selected around 100 largely government or government-affiliated targets for exploitation. There is little evidence that they altered information on affected networks. Consequently, SolarWinds appears to be an espionage campaign, although it is unclear whether the actor left additional, unknown malware while it had access or if it has the intent to alter or destroy data in the future.

Denial by Defense

Denial by defense would harden U.S. government and private-sector companies' digital networks to deny an adversary confidence in the expected benefit of an cyberattack. In the aftermath of SolarWinds, affected companies and agencies increased funding for cybersecurity, adopted Zero Trust frameworks for digital acquisition and interaction, and increased information-sharing related to cyber threats. In a 2021 survey, 90 percent of cybersecurity respondents reported that their company's security posture had improved in response to SolarWinds and other hacks since 2020 such that the companies are more likely to share best practices with other organizations now.[53] The U.S. federal government established cyber unified coordination groups, which enhanced interagency cooperation and coordination with the private sector.[54] The Biden administration issued an Executive Order to remove barriers to sharing information on threats, standardize federal responses to cyber incidents, and establish the Cyber Safety Review Board.[55] Nevertheless, cyber defenses are typically penetrable and generally fail to stop all attacks. But building cyber resilience and the organizational capacity to recover quickly and fully can reduce the incentive of an attack by making it look futile. Strong defenses can also raise the cost of a cyberattack and the risk of discovery—factors that drive the expected benefits for an attacker down.

Threat of Punishment

Despite Moscow's denials of its involvement in the cyberattack, the Biden administration imposed sanctions on Russia in retaliation for the SolarWinds breach.[56] However, to blur its own role, Russia is skilled at using nonstate or quasi-state actors as proxies for its own policies in cyberspace.[57] The U.S. government was not able to definitively link Moscow to the attack in public. Meanwhile, Cozy Bear—the hacking group purportedly responsible for the attack—has continued to operate. The United Kingdom's National Cyber Security Centre and Canada's Communications Security Establishment found that the group was attempting to steal information related to coronavirus 2019 vaccine development.[58] The group also breached Synnex, an information technology contractor providing services to the Republican National Committee in July 2021.[59] Retaliatory threats of punishment will be less effective in cyberspace, where the identity of the attacker and the extent of its association with the Russian state are uncertain.

Entanglement

The United States and Russia jointly signed the United Nations cyber norms agreement in October 2021.[60] The agreement reaffirmed that states should not hack each other's critical infrastructure in peacetime or shelter cyber criminals who conduct attacks on other countries.[61] That act broke decades of stalemate between Washington and Moscow over internet governance, although the agreement itself does not commit signatories to specific actions or policies. In particular, the agreement does not address the problem of anonymity in cyberspace, which incentivizes deniable intrusion. Moreover, the Russia-Ukraine war has prevented further discussions to deepen the agreement.[62]

Normative Taboos

Attempts to name and shame Cozy Bear and Russia have not stopped further cyberattacks. Indeed, CrowdStrike noted that hacker groups with links to governments in Turkey, India, Pakistan, Colombia, and others have joined Russia, China, Iran, and North Korea in launching cyber intrusions and attacks on enemies. Moreover, Chinese and Russian cyber strategy is predicated on the belief that they are subject to persistent cyberattacks from supposedly superior U.S. hackers.[63]

Chinese Government Connections to Organized Crime

In July 2019, groups of armed and masked men attacked prodemocracy demonstrators returning from protests in Hong Kong.[64] Analysts wrote that these men were low-level Chinese mafia affiliates who had been paid by the Hong Kong and Chinese governments to target and terrorize the demonstrators.[65] Demonstrators who participated in Hong Kong's prodemocracy Umbrella Movement in 2014 were also attacked by alleged Chinese mafia members. The Chinese government has reportedly employed organized crime affiliates to similar effect in Taiwan,[66] Australia,[67] and Mainland China.[68] Chinese organized crime is also active in the international narcotics trade. The Chinese government does not disrupt the mafia's control of the production and distribution of fentanyl's precursors to other countries, including the United States (via Mexico), and Chinese organized crime is also central to trade-based money laundering schemes.[69]

Beijing has disavowed any direct relationship with these groups and is, in fact, claims to be targeting Chinese mafia affiliates operating abroad via Chinese Ministry of State Security operations.[70] Despite these claims, it is clear that the Chinese government benefits from these groups, leveraging their networks to wield political influence abroad and also to support legitimate economic activity.[71]

While target governments can pursue and prosecute criminal groups operating within their countries, assistance from the Chinese government is essential to cutting off domestic sources of funding and support. Beijing is reluctant to do so unless its direct economic or security interests are at stake. For example, through its legal front operations, Chinese organized crime provides services to Chinese businesses abroad connected with government officials and the Chinese Communist Party.[72]

Response Options

The relationship between Chinese organized crime and the Chinese government presents targeted states with a difficult threat picture, complicating possible responses:

- **Attribution**: As criminal networks, the Chinese mafia avoids clear attribution for its actions. In addition, these organizations' front operations are by definition legal and serve to hide illicit activities. Chinese criminal syndicates are less violent than Latin American cartels, so their illicit activity is less likely to be detected and pursued.
- **Sponsorship**: Various echelons of the Chinese government "hire" the Chinese mafia because this offers deniability, enabling the government to evade responsibility for violence and avoid political blowback. Moreover, specific practices "intertwine and blur the relationship between criminality (black) and the state (red)," obscuring distinctions between those activities.[73]
- **Motivation**: The Chinese mafia's criminal activities typically align with the government's own economic and organizational interests, making it difficult to determine whether the criminal networks are following Beijing's directions.

Denial by Defense

Target countries can prosecute state-sponsored criminal organizations, although this disruption may only be temporary (because these organizations may draw on additional personnel in China to reconstitute their structures). Such prosecutions may stop only the attackers and fail to dissuade state sponsorship of these operations. Furthermore, some of the undesirable activities—such as the importation of chemical precursors used in illegal narcotics—may be difficult to halt because they are legal and desirable for other purposes.

Threat of Punishment

Sponsors work through organized crime in part for deniability. If gangsters are caught, governments can always claim the individuals were acting on their own, and, indeed, such activities as drug smuggling fully align with these organizations' interests. Furthermore, such activities as intimidating political dissidents or beating up protesters present target nations with a resource-intensive policing problem. It is impossible to fully identify, let alone protect, all potential targets from these criminal organizations. Although China gains significantly from quieting unwanted political dissent from these operations, the target country's gains are much more limited.[74]

Entanglement

China generally views organized crime as the target country's problem, and Beijing has been reluctant to cooperate on transnational policing. Securing that cooperation also raises difficult policy and human rights questions, given China's authoritarian political system. For example, the United States, Canada, Australia, the United Kingdom, France, and New Zealand recently suspended extradition treaties with Hong Kong, fearing that Beijing would use this mechanism to pursue political dissidents overseas.[75] China suspended its cooperation on extradition in turn and would likely demand a policy reversal to secure its help in prosecuting criminal organizations.

Normative Taboos

Naming and shaming requires clear attribution and mutually agreed on standards. Neither exists in this case. Chinese officials employ organized crime to avoid political blowback and to deny involvement. Disagreement over the legitimacy of dissent means that accusations and evidence of political and human rights abuses may not generate sufficient opprobrium among international audiences. However, if the Chinese government can control the organized criminal group but chooses not to, the United States might be able to hold China equally responsible.

Policy Implications

The United States is limited in its ability to effectively respond to threats in which the attribution, nature, and method of the threat are ambiguous. Maintaining this level of ambiguity likely constrains

the scale at which U.S. adversaries can deploy these approaches, but the cost imposed in the three case studies surveyed here—Havana Syndrome, SolarWinds, and China's use of criminal organizations—demonstrates that these threats should be taken seriously.

In addition to illustrating that this approach to competition may be more widespread than just Havana Syndrome, our analysis of these three cases produced new insights on the potential efficacy of the four response options. These core findings follow directly from Table 2, which summarizes the insights for the three case studies.

Implications for Strategies of Deterrence and Compellence

Denial by Defense

Ambiguity increases the cost of deterrence by denial. Each case featured some degree of uncertainty about the adversary's method of attack. Moreover, potential targets were numerous, broadly distributed, and vulnerable. The adversary also set the place, time, and pace of the attack. This offensive advantage for the adversary made attacks difficult to forecast and required comprehensive defense or denial. These conditions make denial by defense both financially expensive and logistically complicated to implement. While hardening all targets may be impractical, denial by defense can negate some or much of the intended effect. Moreover, active denial that deliberately leaves certain objects vulnerable to attack could be beneficial. Honeypot computer systems, for example, are deliberately set up to attract attacks that defenders can then analyze.[76]

Threat of Punishment

Retaliatory threats of punishment are less likely to be effective when the method and identity of the attacker are uncertain. In each case, clearly identifying the attacker, then unambiguously linking the attacker to possible sponsors, is challenging. Without this critical information, publicly issuing a clear and credible deterrent threat—including specifics on what the United States plans to do to whom in response to what—is difficult. Sponsors can always deny the operations while still reaping their benefits.[77] Targets may attempt to compel the attacker to stop its behavior by inflicting pain and promising future pain, such as by responding in kind by launching similar operations against a suspected sponsor or responding horizontally, in another domain. However, without certainty about the identity of the attacker, the target risks escalation and will likely fail to muster the international support necessary for effective punishment.

Entanglement

Competing powers might take a general interest in arrangements that maintain the stability of the status quo, but undetected cheating still confers advantages. Entanglement is challenging because it relies on having an adversary who prefers the status quo, sees benefits to its continuation, and perceives that it has something valuable to lose by attacking. In all three cases, the adversary has a general interest in

TABLE 2
Possible Response Options

	Havana Syndrome	SolarWinds	Organized Crime
Denial by defense	Increase detection and deflection capability	Enhance cybersecurity	Pursue criminal prosecution in third countries
Threat of punishment	Issue retaliatory threats in public or private	Impose sanctions	Limited
Entanglement	Promote mutual dependence on safe diplomatic operations overseas	Promote mutual dependence on cyber stability	Limited
Normative taboos	Name and shame	Name and shame	Name and shame

and depends to some degree on the status quo: sustaining the safety of diplomats overseas; maintaining stability in cyberspace, including avoiding the most dangerous forms of cyberattacks; and limiting the violence of criminal organizations. However, each case featured an adversary approach that undermined the status quo with little to no blowback to the adversary, an ancillary of the ambiguity (in terms of actor and method) of these approaches. Options for forming structural entanglement do exist, such as seeking international cooperation—and perhaps even subsidizing this cooperation—in collectively deterring unknown threats without assigning attribution and blame to a particular nation state. Over time, states may develop an interest in the stability of the system. But entanglement relies to some degree on the attacker's cooperation, and targets must be able to clearly observe compliance with agreements. Each case highlights some form of deniability, allowing sponsors to evade monitoring. Moreover, entanglement approaches may be too slow to initiate and too rigid to rapidly adjust to the wide variety of possible approaches of this ilk.

Normative Taboos

Enforcing norms without attribution is difficult, and rivals may perceive that violation does not result in prohibitive reputational costs. Gathering the support of other countries to define standards of acceptable behavior and attaching clear punishments for violation are feasible and potentially effective in these cases, particularly as third-party nationals have been affected directly or indirectly in each case. The challenge here is twofold. First, without clear attribution, it is not possible to impose reputational costs. If attackers and sponsors are known, publicizing that information could garner the normative support of other countries and isolate the activities' sponsors, although revealing the evidence for either step may undermine intelligence-gathering techniques. Moreover, it is possible that the reputational costs of these norms may be insufficient to dissuade the attackers. China, for example, probably cares much more about the benefits of silencing overseas dissidents through proxy violence than local law enforcement does about protecting those under its jurisdiction from seemingly random violence. The SolarWinds hackers took advantage of the fact that, even among organizations working with sensitive information, cybersecurity is often a much lower priority than efficiency and convenience.

Concluding Thoughts

This report explored the applicability of existing baseline concepts for deterrence and compellence to three brief contemporary case studies of coercive violence from unknown or uncertain origins: Havana Syndrome, SolarWinds, and the Chinese mafia. Few of the standard tools are effective against the types of threats these three cases represent. Similar to classic studies, we found that denial-by-defense strategies are more reliable than punishment strategies. Threat-of-punishment and norms strategies are more difficult. The United States cannot issue clear threats to respond to given actions when it has little certainty about who is conducting the actions. The United States also cannot rally international condemnation of given actions without being certain who the actor is.

Notes

[1] Corera, "'Havana Syndrome' and the Mystery of the Microwaves."

[2] National Intelligence Council, "Intelligence Community Assessment: Updated Assessment of Anomalous Health Incidents." Two agencies assessed it was "very unlikely" that a foreign adversary is responsible for the anomalous health incidents with moderate to high confidence; three agencies assess it was "very unlikely" with moderate confidence; and two agencies judge it is "unlikely" with low confidence.

[3] Schelling, *Arms and Influence*, pp. 69–91.

[4] Grocholski et al., *How to Effectively Assess the Impact of Non-Lethal Weapons as Intermediate Force Capabilities*.

[5] Long, *Deterrence—From Cold War to Long War: Lessons from Six Decades of RAND Research*, p. 7.

[6] Art and Greenhill, "Coercion: An Analytical Overview," p. 5.

[7] Biddle, "Coercion Theory: A Basic Introduction for Practitioners," p. 102.

[8] We adopted these four mechanisms from Joseph Nye. In Nye, "Deterrence and Dissuasion in Cyberspace," he writes about deterrence and dissuasion in cyberspace, but we apply his mechanisms more broadly to coercion. In his article, Nye covers the threat of punishment first. In this report, we chose to cover denial by defense first because it is a simpler concept.

[9] Snyder, *Deterrence and Defense: Toward a Theory of National Security*; Nye, "Deterrence and Dissuasion in Cyberspace."

[10] Mazarr, *Understanding Deterrence*, p. 2.

[11] See, for example, Mallory, *New Challenges in Cross-Domain Deterrence*; Borghard and Lonergan, "Deterrence by Denial in Cyberspace"; and Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War.*

[12] Biddle, "Coercion Theory: A Basic Introduction for Practitioners," p. 102.

[13] Mazarr, *Understanding Deterrence*, p. 2.

[14] Fearon, "Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs."

[15] Kurizaki, "Efficient Secrecy: Public Versus Private Threats in Crisis Diplomacy," pp. 543–544.

[16] Mazarr et al., *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression*, p. 35.

[17] Biddle, "Coercion Theory: A Basic Introduction for Practitioners," p. 102.

[18] Sweijs and Zilncik, "The Essence of Cross-Domain Deterrence," p. 150.

[19] Jasper, "Deterring Malicious Behavior in Cyberspace," p. 72.

[20] Nye, "Deterrence and Dissuasion in Cyberspace," p. 60.

[21] Egloff and Smeets, "Publicly Attributing Cyber Attacks: A Framework," p. 6.

[22] Nye, "Deterrence and Dissuasion in Cyberspace," p. 60.

[23] Mazarr, *Understanding Deterrence*, pp. 8–11.

[24] The estimated number of cases is as reported in Barnes, "Most 'Havana Syndrome' Cases Unlikely Caused by Foreign Power, C.I.A. Says." Earlier estimates suggest a total of a couple hundred cases.

[25] U.S. personnel have reported acute symptomology while in residences, on the street, in moving vehicles, in secure U.S. facilities, and in front of the White House. Victims have included an intelligence officer traveling in India with the CIA director and members of the President's advance team in London.

[26] Intelligence Community Experts Panel on Anomalous Health Incidents, "Executive Summary."

[27] Office of the Director of National Intelligence, "Complementary Efforts on Anomalous Health Incidents."

[28] Relman and Pavlin, *An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies*. Critics noted that this NASEM effort was incomplete because the Trump administration had not given the team access to classified information.

[29] National Intelligence Council, "Intelligence Community Assessment: Updated Assessment of Anomalous Health Incidents."

[30] Relman and Pavlin, *An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies*, p. 44.

[31] "Wearable Radio Frequency Weapon Exposure Detector."

[32] Relman and Pavlin, *An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies*, p. 44.

[33] Power and Miner, "Havana Syndrome: American Officials Under Attack."

[34] Mazarr et al., *What Deters and Why: Applying a Framework to Assess Deterrence of Gray Zone Aggression*, p. 13.

[35] Nye, "Deterrence and Dissuasion in Cyberspace," p. 51.

[36] Entous and Anderson, "The Mystery of the Havana Syndrome."

[37] Schumaker, "Before Havana Syndrome, There Was Moscow Signal."

[38] Barnes and Goldman, "Review Finds No Answers to Mystery of Havana Syndrome."

[39] Myre, "'Moscow Rules': How the CIA Operated Under the Watchful Eye of the KGB."

[40] Barnes and Goldman, "Review Finds No Answers to Mystery of Havana Syndrome,"

[41] Mandiant, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor."

[42] Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack."

[43] Barnett, "Nearly 40 Defense Companies Were Impacted in SolarWinds Breach."

[44] Microsoft estimates that more than 1,000 engineers worked on the malware (Whitaker, "SolarWinds: How Russian Spies Hacked the Justice, State, Treasury, Energy and Commerce Departments"; Sharwood, "Microsoft Says It Found 1,000-Plus Developers' Fingerprints on the SolarWinds Attack").

[45] Aspen Institute, "A Moment of Reckoning: Understanding the Russian Cyber Attack."

[46] U.S. Government Accountability Office, "Federal Response to SolarWinds and Microsoft Exchange Incidents."

[47] Kovacs, "China-Linked Hackers Exploited SolarWinds Flaw in U.S. Government Attack."

[48] Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack."

[49] McKeown, Joyce, and Chase, testimony.

[50] Ratnam, "Cleaning Up SolarWinds Hack May Cost as Much as $100 Billion."

[51] Oladimeji and Kerner, "SolarWinds Hack Explained: Everything You Need to Know."

[52] Adam Meyers, who led SolarWinds' cyber forensics team, claimed that the "tradecraft was phenomenal" (Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack").

[53] IronNet. "2021 Cybersecurity Impact Report."

[54] U.S. Government Accountability Office. "Federal Response to SolarWinds and Microsoft Exchange Incidents," pp. 22, 33.

[55] Executive Order 14028, "Improving the Nation's Cybersecurity."

[56] White House, "Imposing Costs for Harmful Foreign Activities by the Russian Government."

[57] Mazarr et al., *Competition and Restraint in Cyberspace*.

[58] National Cyber Security Centre, "Advisory: APT29 Targets COVID-19 Vaccine Development."

[59] Turton and Jacobs, "Russia 'Cozy Bear' Breached GOP as Ransomware Attack Hit"; Campbell, "Russian Hackers Reportedly Attacked GOP Computer Systems."

[60] United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security."

[61] Nakashima and Marks, "Russia, U.S. and Other Countries Reach New Agreement Against Cyber Hacking."

[62] Tennant and Walker, "Cyber, Fire and Fury"; United Nations Office on Drugs and Crime, "First Session of the Ad Hoc Committee."

[63] Xiao, *Science of Military Strategy*; Lilly and Cheravitch, "Past Present and Future of Russia's Cyber Strategy and Forces."

[64] In 2019 and 2020, protesters in Hong Kong demonstrated against a proposed extradition bill, which would allow the city government to send fugitives to Mainland China for prosecution. At the height of the protests, about one-quarter of Hong Kong's population marched against the bill, considering it a violation of the city's political autonomy. See Kuo, "Hong Kong: 1.7m People Defy Police to March in Pouring Rain."

[65] Taylor, "Infernal Affairs: How Triads Embraced Communist China"; Lo, "Hong Kong Police to Launch Raids on White-Clad Thugs"; Shih. "China's Backers and 'Triad' Gangs Have a History of Common Foes. Hong Kong Protesters Fear They Are Next"; see also Weinrich, "The Triad Trials."

[66] Cole, "On the Role of Organized Crime and Related Substate Actors in Chinese Political Warfare Against Taiwan"; Cole, "Nice Democracy You've Got There. Be a Shame If Something Happened to It."

[67] In 2008, anti-Chinese government protests were held in Australia along the Olympic torch relay. However, the head of Canberra's Chinese Students and Scholars Association dismissed that concern in his city, suggesting that the Triads had "quietened them [i.e., protesting groups] down" (Garnaut and Li, "China Calls for a People's Army to March on Canberra to Defend Torch").

[68] Taylor, "Infernal Affairs: How Triads Embraced Communist China"; Lian, "Gangs of Hong Kong"; Lim, "The Thugs of Mainland China."

[69] U.S. Government Accountability Office, "Trade-Based Money Laundering"; "'Chinese Triads' in Kidnap for Ransom Scam."

[70] These operations are referred to as Operations Fox Hunt and Skynet (Zhang, "Repatriation and Recovery Targeted to Combat Graft"; Cao, "Success of Fox Hunt Campaign Continues"). China claims that these operations are to bring people accused of financial crimes back to China; however, the U.S. government has assessed that, in reality, the program targets Chinese nationals living abroad who are political rivals, dissidents, and critics of the Chinese Communist Party (Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States").

[71] Felbab-Brown, "China and Synthetic Drugs Control: Fentanyl, Methamphetamines, and Precursors," p. 31.

[72] Felbab-Brown, "China and Synthetic Drugs Control: Fentanyl, Methamphetamines, and Precursors."

[73] Silverstone, Chung, and Whittle, "China: the 'Red-Black Nexus', Organised Crime and Politics."

[74] Ohlberg, "The CCP's Ambitions to Control and Manipulate Information Spaces: Theory and Practice."

[75] Tiezzi, "US Becomes Latest Country to Suspend Extradition Treaty with Hong Kong."

[76] During the Cold War, the Soviet Union beamed microwaves at the U.S. embassy in Moscow, possibly to activate listening devices within the building. For years, the U.S. government did not tell its embassy personnel about "Moscow Signal," despite collecting blood samples. When the government eventually revealed the signal and the purpose of its medical investigations, staff were incensed. Several filed lawsuits against the Department of State, and the ambassador threatened to resign. See Schumaker, "Before Havana Syndrome, There Was Moscow Signal."

[77] See Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War."

References

Art, Robert J., and Kelly M. Greenhill, "Coercion: An Analytical Overview" in Kelly M. Greenhill and Peter Krause, eds., *Coercion: The Power to Hurt in International Politics*, Oxford University Press, 2018.

Aspen Institute, "A Moment of Reckoning: Understanding the Russian Cyber Attack," video, January 7, 2021.

Barnes, Julian E., "Most 'Havana Syndrome' Cases Unlikely Caused by Foreign Power, C.I.A. Says," *New York Times*, January 20, 2022.

Barnes, Julian E., "Panel Says Some Havana Syndrome Cases May Stem from Radio Energy," *New York Times*, February 2, 2022.

Barnes, Julian E., and Adam Goldman, "Review Finds No Answers to Mystery of Havana Syndrome," *New York Times*, December 2, 2021.

Barnett, Jackson, "Nearly 40 Defense Companies Were Impacted in SolarWinds Breach," Fedscoop, May 18, 2021.

Biddle, Tami Davis, "Coercion Theory: A Basic Introduction for Practitioners," *Texas National Security Review*, Vol. 3, No. 2, Spring 2020.

Borghard, Erica D., and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies*, August 3, 2021.

Campbell, Ian Carlos, "Russian Hackers Reportedly Attacked GOP Computer Systems," webpage, The Verge, July 6, 2021.

Cao Yin, "Success of Fox Hunt Campaign Continues," *China Daily*, November 5, 2015.

Carson, Austin, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War," *International Organization*, Vol. 70, No. 1, Winter 2016.

"'Chinese Triads' in Kidnap for Ransom Scam," *Chosun Ilbo*, December 19, 2006.

Cole, J. Michael, "Nice Democracy You've Got There. Be a Shame If Something Happened to It," *Foreign Policy*, June 18, 2018.

Cole, J. Michael, "On the Role of Organized Crime and Related Substate Actors in Chinese Political Warfare Against Taiwan," *Prospect and Exploration*, Vol. 19, No. 6, June 2021.

Corera, Gordon, "'Havana Syndrome' and the Mystery of the Microwaves," BBC, September 9, 2021.

Egloff, Florian J., and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," *Journal of Strategic Studies*, 2021.

Entous, Adam, and Jon Lee Anderson, "The Mystery of the Havana Syndrome," *New Yorker*, November 8, 2018

Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021.

Fearon, James D., "Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs," *Journal of Conflict Resolution*, Vol. 41, No. 1, 1997.

Felbab-Brown, Vanda, *China and Synthetic Drugs Control: Fentanyl, Methamphetamines, and Precursors*, Brookings Institution, March 2022.

Garnaut, John, and Maya Li, "China Calls for a People's Army to March on Canberra to Defend Torch," *Sydney Morning Herald*, April 16, 2008.

Grocholski, Krista Romita, Scott Savitz, Jonathan P. Wong, Sydney Litterer, Raza Khan, and Monika Cooper, *How to Effectively Assess the Impact of Non-Lethal Weapons as Intermediate Force Capabilities*, RAND Corporation, RR-A654-1, 2022. As of January 25, 2023: https://www.rand.org/pubs/research_reports/RRA654-1.html

Intelligence Community Experts Panel on Anomalous Health Incidents, "Executive Summary," redacted, 2021.

IronNet, *2021 Cybersecurity Impact Report*, 2021.

Jasper, Scott, "Deterring Malicious Behavior in Cyberspace," *Strategic Studies Quarterly*, 2015.

Kovacs, Eduard, "China-Linked Hackers Exploited SolarWinds Flaw in U.S. Government Attack," *Security Week*, February 3, 2021.

Kuo, Lily, "Hong Kong: 1.7m People Defy Police to March in Pouring Rain," *The Guardian*, August 18, 2019.

Kurizaki, Shuhei, "Efficient Secrecy: Public Versus Private Threats in Crisis Diplomacy," *American Political Science Review*, 2007.

Lian, Yi-Zheng, "Gangs of Hong Kong," *New York Times*, August 2, 2019

Lilly, Bilyana, and Joe Cheravitch, "Past Present and Future of Russia's Cyber Strategy and Forces," presented at the 2020 12th International Conference on Cyber Conflict, NATO CCDCOE Publications, 2020.

Lim, Louisa, "The Thugs of Mainland China," *New Yorker*, October 8, 2014.

Lo, Clifford, "Hong Kong Police to Launch Raids on White-Clad Thugs, Including Members of 14K and Wo Shing Wo Triad Gangs, Who Unleashed Terror on Protesters and Bystanders in Yuen Long," *South China Morning Post*. July 22, 2019.

Long, Austin, *Deterrence—From Cold War to Long War: Lessons from Six Decades of RAND Research*, RAND Corporation, MG-636-OSD/AF, 2008. As of January 24, 2023: https://www.rand.org/pubs/monographs/MG636.html

Mallory, King, *New Challenges in Cross-Domain Deterrence*, RAND Corporation, PE-259-OSD, 2018. As of January 24, 2023: https://www.rand.org/pubs/perspectives/PE259.html

Mandiant, *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor*, December 13, 2020.

Mazarr, Michael J., *Understanding Deterrence*, RAND Corporation, PE-295-RC, 2018. As of January 24, 2023: https://www.rand.org/pubs/perspectives/PE295.html

Mazarr, Michael J., Arthur Chan, Alyssa Demus, Bryan Frederick, Alireza Nader, Stephanie Pezard, Julia A. Thompson, and Elina Treyger, *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression*, RAND Corporation, RR-2451-A, 2018. As of January 24, 2023: https://www.rand.org/pubs/research_reports/RR2451.html

Mazarr, Michael J., Joe Cheravitch, Jeffrey W. Hornung, and Stephanie Pezard, *What Deters and Why: Applying a Framework to Assess Deterrence of Gray Zone Aggression*, RAND Corporation, RR-3142-A, 2021. As of January 24, 2023: https://www.rand.org/pubs/research_reports/RR3142.html

Mazarr, Michael J., Bryan Frederick, Emily Ellinger, and Benjamin Boudreaux, *Competition and Restraint in Cyberspace*, RAND Corporation, RR-A1180-1, 2022. As of January 24, 2023: https://www.rand.org/pubs/research_reports/RRA1180-1.html

McKeown, David, Robert Joyce, and William Chase, testimony, hearing on Future Cybersecurity Architectures, U.S. Senate Committee on Armed Services, Subcommittee on Cybersecurity, April 14, 2021.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe, *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, RAND Corporation, RR-2942-OSD, 2019. As of January 24, 2023: https://www.rand.org/pubs/research_reports/RR2942.html

Myre, Greg, "'Moscow Rules': How The CIA Operated Under the Watchful Eye of the KGB," NPR, June 10, 2019.

Nakashima, Ellen, and Joseph Marks, "Russia, U.S. and Other Countries Reach New Agreement Against Cyber Hacking, Even as Attacks Continue," *Washington Post*, June 21, 2021

National Cyber Security Centre, "Advisory: APT29 Targets COVID-19 Vaccine Development," press release, July 16, 2020.

National Intelligence Council, "Intelligence Community Assessment: Updated Assessment of Anomalous Health Incidents," March 1 2023.

Nye, Joseph S., Jr., "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3, Winter 2016–2017.

Office of the Director of National Intelligence, "Complementary Efforts on Anomalous Health Incidents," infographic, February 2, 2022.

Ohlberg, Mareike, "The CCP's Ambitions to Control and Manipulate Information Spaces: Theory and Practice," Strategic Multilayer Assessment speaker series, June 22, 2022.

Oladimeji, Saheed, and Sean Michael Kerner, "SolarWinds Hack Explained: Everything You Need to Know," WhatIs website, June 29, 2022.

Power, Sean, and Michael Miner, "Havana Syndrome: American Officials Under Attack," Belfer Center for Science and International Affairs, November 4, 2021.

Ratnam, Gopal, "Cleaning Up SolarWinds Hack May Cost as Much as $100 Billion," webpage, Roll Call, February 11, 2021.

Relman, David A., and Julie A. Pavlin, eds., *An Assessment of Illness in U.S. Government Employees and Their Families at Overseas Embassies*, National Academies Press, 2020.

Schelling, Thomas C., *Arms and Influence*, Yale University Press, 1966.

Schumaker, James, "Before Havana Syndrome, There Was Moscow Signal," *Foreign Service Journal*, January/February 2022.

Sharwood, Simon, "Microsoft Says It Found 1,000-Plus Developers' Fingerprints on the SolarWinds Attack," *The Register*, February 15, 2021.

Shih, Gerry, "China's Backers and 'Triad' Gangs Have a History of Common Foes. Hong Kong Protesters Fear They Are Next," *Washington Post*, July 23, 2019.

Silverstone, Danie, Alex Chung, and Joe Whittle, "China: The 'Red-Black Nexus', Organised Crime and Politics," in Felia Allum and Stan Gilmour, eds., *Handbook of Organised Crime and Politics*, Elgar Publishing, 2019.

Snyder, Glenn H., *Deterrence and Defense: Toward a Theory of National Security*, Princeton University Press, 1961.

Sweijs, Tim, and Samuel Zilncik, "The Essence of Cross-Domain Deterrence," in Frans Osinga and Tim Sweijs, eds., *NL ARMS Netherlands Annual Review of Military Studies*, 2020.

Taylor, Jerome, "Infernal Affairs: How Triads Embraced Communist China," AFP, July 23, 2019.

Temple-Raston, Dina, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *All Things Considered*, NPR, April 16, 2021.

Tennant, Ian, and Summer Walker, "Cyber, Fire and Fury," webpage, Global Initiative Against Transnational Organized Crime, March 17, 2022.

Tiezzi, Shannon, "US Becomes Latest Country to Suspend Extradition Treaty with Hong Kong," *The Diplomat*, August 20, 2020.

Turton, William, and Jennifer Jacobs, "Russia 'Cozy Bear' Breached GOP as Ransomware Attack Hit," Bloomberg, July 6, 2021.

United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security, and Advancing Responsible State Behavior in the Use of Information and Communications Technologies," resolution, October 8, 2021.

United Nations Office on Drugs and Crime, "First Session of the Ad Hoc Committee," webpage, February 28–March 11, 2022.

U.S. Government Accountability Office, *Trade-Based Money Laundering: U.S. Government Has Worked with Partners to Combat the Threat, but Could Strengthen Its Efforts*, GAO-20-333, April 2020.

U.S. Government Accountability Office, *Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO-22-104746, January 2022.

"Wearable Radio Frequency Weapon Exposure Detector," Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) website, December 8, 2020.

Weinrich, Brody, "The Triad Trials," *St. Antony's International Review*, Vol. 15, No. 1, May 2019.

Whitaker, Bill, "SolarWinds: How Russian Spies Hacked the Justice, State, Treasury, Energy and Commerce Departments," CBS News, July 4, 2021.

White House, "Imposing Costs for Harmful Foreign Activities by the Russian Government," fact sheet, April 15, 2021.

Wray, Christopher, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," remarks delivered at the Hudson Institute, July 7, 2020.

Xiao Tianliang [肖天亮], ed., *Science of Military Strategy* [战略学], National Defense University [国防大学], 2020.

Zhang Yi, "Repatriation and Recovery Targeted to Combat Graft," *China Daily*, May 6, 2016.

About the Authors

Daniel Egel is an economist at the RAND Corporation who focuses on U.S. policymaking at the nexus of security and prosperity.

Gabrielle Tarini is a policy researcher at RAND whose research focuses on regional security issues in Europe and Asia, security cooperation, the NATO alliance, special operations forces, and civilian protection issues.

Raymond Kuo is the inaugural director of the RAND Taiwan Policy Initiative and a political scientist at RAND.

Eric Robinson is a research programmer and analyst at RAND whose research focuses on special operations and irregular warfare.

Anthony Vassalo is an international and defense policy researcher at RAND who focuses on U.S. national security strategy, risk, deterrence, counterterrorism, and the intelligence Community.

About This Report

The mystery surrounding the so-called Havana Syndrome—an unexplained illness first experienced by U.S. Department of State personnel stationed in Cuba in late 2016—illustrates the challenge of mustering a response to a national security threat when the threat, the underlying method, and the actor behind the threat are not understood with certainty. How should states deter acts of violence perpetrated by unknown or unclear actors? And once such violence begins, how should states seek to compel such actors to cease their aggression? This report explores the applicability of existing baseline concepts for deterrence and compellence to three brief contemporary case studies of coercive violence from unknown or uncertain origins. In addition to Havana Syndrome, the authors explore the SolarWinds cyberattack, in which hackers linked to Russian intelligence conducted a massive cyberattack against American companies and government agencies, and the Chinese Communist Party's connections to organized crime syndicates around the world.

This research for this report was completed in November 2022. In March 2023, the U.S. Intelligence Community judged that it was unlikely or very unlikely that a foreign adversary bore responsibility for Havana Syndrome, although agencies varied from low confidence to moderate to high confidence in this judgment. The Intelligence Community has not reached consensus and may not for some time. Havana Syndrome remains a useful case to examine options for responding to a threat where the underlying method and actor are uncertain.

RAND National Security Research Division

This research was sponsored by the Office of the Secretary of Defense and conducted within the International Security and Defense Policy Program of the RAND National Security Research Division (NSRD), which operates the RAND National Defense Research Institute (NDRI), a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND International Security and Defense Policy Program, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Acknowledgments

We are grateful to the leadership of NDRI for their support of this study. We would also like to thank our peer reviewers, Richard Girven and Mick Mulroy, for their insightful comments and suggestions that greatly improved the report.

For more information on this publication, visit www.rand.org/t/RRA1598-1.

www.rand.org