U.S. Immigration and Customs Enforcement (Ron Rogers)

Personnel inspect cross-border drug-smuggling tunnel discovered inside warehouse near San Diego, California, 2011

Thinking About Strategic Hybrid Threats—In Theory and in Practice

BY FRANK J. CILLUFFO AND JOSEPH R. CLARK

As the United States resets in the wake of Iraq and Afghanistan, and in the face of growing uncertainty in the South China Sea, a good and important debate is occurring about how best to provide for our national security. Reasonable arguments can be made about the threats posed by potential peer competitors such as China, rogue nations such as North Korea, and prospective revisionist powers such as Russia. Arguments can be made about threats arising from political instability or intrastate conflicts, such as in Pakistan, Uganda, and Syria. Arguments can also be made about the threats posed by jihadi terror groups, organized crime syndicates, and drug trafficking organizations. The dangers highlighted by any one of these arguments are real and perhaps grave. They are not, however, novel.

For each of these dangers, we have established procedures, tools, and resources for deterring, mitigating, and perhaps even resolving their associated risks. Yet there are threats for which we lack well-established security mechanisms. Chief among them are the hybrid threats woven from the hazards above to directly endanger the safety and security of our society and citizens at home—as well as our national interests abroad.

What follows is an argument for casting greater focus on the dangers posed by hybrid threats at the strategic level.[1] We use Iran and the availability of proxy capabilities to illustrate the mechanics of, and risk posed by, strategic hybrid threats. We also offer a general model for what is needed to detect and respond to hybrid threats. Still, increased attention is not enough. It is our intent that this argument serve as fuel for a richer discussion about the doctrine, strategies, material resources, and organizational behaviors the United States ought to develop to respond to strategic hybrid threats in both theory and practice.

Frank J. Cilluffo is an Associate Vice President at The George Washington University and serves as Director of the university's Homeland Security Policy Institute (HSPI). Dr. Joseph R. Clark is a Policy Analyst at HSPI.

Hybrid Threats

Hybrid threats have been part of the security vernacular since the late 1990s. Despite a surge of recent attention, the concept remains ill-defined. Various authors, proponents and opponents of the idea, have added or removed defining traits. This has often confused rather than clarified the issue. As a result, discussions tend to devolve into debates about whether hybrid threats represent a novel class of security challenges. The two central issues—the degree to which such threats currently pose a danger and how the United States ought to deal with them—risk being lost in the rhetoric.[2] To correct this and return to the crux of the matter, this argument begins with a proposal of how *hybrid threats* might be better defined and differentiated from other threats.

As a means of clearing away the conceptual confusion produced by past debates, let us begin by explaining what we would remove from past treatments of the term. We are not talking about multimodal wars or the threats they pose. The ability of adversaries to move up or down the spectrum of warfare, or engage in multiple phases of warfare simultaneously, may be intensifying—but it is not new.[3] Such was the case during many of the insurgencies and civil wars of the 20th century, including those in Russia, China, Vietnam, and Nicaragua. We are not talking about *asymmetric threats*. That idea has itself devolved to a level of questionable utility. The principle of attempting to match one's strength against an enemy's weakness is a well-established military dictum. All combatants seek to maximize asymmetric threats or engage in asymmetrical warfare, for the successful asymmetrical alignment of capabilities maximizes one's leverage and increases the probability of success. Nor are we talking about *irregular tactics* or *unconventional warfare*. Those terms describe indirect actions taken by an actor to undermine the legitimacy, influence, or position of an occupying power or government.[4] Because they may be employed in the service of nation-states and their interests, hybrid threats should not be confused with the irregular use of forces or capabilities that is commonly, but not exclusively, observed during insurgencies.

hybrid threats are "custom-designed" capabilities crafted by a principal actor to overcome the predominant power or position of an adversary

Hybrid threats do, however, share some similarities with irregular tactics and unconventional warfare. Hybrid threats may target a wide range of military and civilian targets (including the general population of an adversary) and may be undertaken to weaken a defender's power, position, influence, or will—rather than to strengthen those attributes for the attacker. These characteristics explain much of the difficulty in defending against hybrid threats and why they warrant so much attention.

A clear conceptual definition of *hybrid threats* should start by acknowledging that they are "custom-designed" capabilities crafted by a principal actor to overcome the predominant power or position of an adversary.[5] From there, it should be noted that hybrid threats are innovative stand-alone capabilities designed to achieve the principal actor's goal(s). What truly differentiates hybrid threats from others, however, are the following three elements. Hybrid threats are unique in that the desired objective of a threat, the endstate it is to achieve, lies beyond the endogenous capabilities of

the principal actor motivating the threat's creation and deployment. This condition forces the principal actor to find exogenous entities who can act as agents supplying the desired skills, materials, and/or access. It is from this principal-agent relationship, and the resulting weaving together of disparate capabilities, that the hybrid threat emerges.

A *strategic hybrid threat*, building on the concept above, should be defined as a customized capability produced through a principal-agent relationship for the purpose of seriously decreasing or adversely changing vital elements or instruments of a defender's national power. Strategic hybrid threats are undertaken for the express purpose of achieving the objective(s) of the principal actor—though the target of the threat and the goal may be only indirectly related.[6]

Core Characteristics

Strategic hybrid threats can be delineated and demarcated by three core characteristics—their origin, their composition, and their fungibility.

Their origin is the product of the principal actor's nature, the actor's strategic context, and the actor's strategic goal(s). For instance, the origin of a specific hybrid threat will be determined by whether the principal actor is a nation-state, terrorist organization, or criminal syndicate; that actor's geographic location, relative distribution of power vis-à-vis other actors, and existing alliance structures; and the particular endstate the actor is trying to bring about. These elements give rise to the threat's purpose and objectives. In this, the strategic hybrid threat is no different from any traditional threat. It is the inability of the principal actor to develop the threat endogenously that differentiates it.

The composition of a strategic hybrid threat is characterized by the capabilities of the potential agent, goals of the agent, and most exploitable vulnerabilities of the defender that align with the principal actor's strategic goal(s). The capabilities of the potential agent affect how the purpose and objectives of the desired threat are realized. They form the avenue of attack (or threatened attack). The agent's goals shape whether the principal-agent relationship is a transactional payment for goods or services, a longer term business arrangement, an ideologically driven partnership, or some combination of these. The agent's goals determine whether the hybrid is the product of a one-time exchange or a longer term coordinated effort. They also shape the duration of the threat and how easily it can be reconstituted or modified once used (or detected and defended against). The vulnerabilities of the defender lead to the identification of targets by the principal-agent partnership. The alignment between the defender's vulnerabilities and hybrid threat determine at what target the attack or threat may be directed—so as to produce the highest probability of achieving the principal actor's goal(s).[7]

The threat's level of fungibility is the product of its composition. It determines the range of targets that may be successfully threatened, the likelihood of a priori detection, and the ease with which the defender may correctly attribute the threat (or attack). The range of potential targets determines the scope of what, where, and when the principal actor may attack or threaten to attack. For example: if the hybrid threat may be used equally well against civilian and military targets, or both simultaneously, the scope of what may be threatened expands. Fungibility also

determines the ease and speed with which the principal actor may shift the target of the threat (or attack) in response to actions by the defender. Furthermore, a strategic hybrid threat that may be easily and quickly deployed against a wide scope of targets has fewer target-unique attributes and provides the defender with less warning.

High levels of fungibility make attribution and deterrence much more difficult. This difficulty arises from the fact that the strategic hybrid threat is the product of multiple actors. Attribution and deterrence may be masked by the principal's lack of capabilities or the agent's lack of intent.

Perversely, the intelligence services of the defender may rule out the principal actor behind the threat because it lacks the capability to carry out the threat. Lacking obvious intent, the defender may not consider the agent an imminent danger. The situation becomes more complex with the fact that the principal need not make itself known. If the principal actor's strategic goals do not require that it signal its responsibility, the actor may choose to remain anonymous (possibly allowing attribution to fall upon another). This is likely to be the case if the hybrid attack was simply meant to block or delay a given response. For example, if a regional power wanted to seize the territory of a neighboring nation-state allied with the United States, it might launch a hybrid attack designed to slow the American response.

Regardless of the success of its territorial ambitions, the actor would have no compelling interest in divulging its responsibility for the hybrid attack. Finally, the principal-agent relationship of the hybrid threat makes deterrence more difficult. As fungibility increases, the defender is confronted with an increasing number of potential suspects or combinations of suspects that may have the intent or capability to level the threat. Under such conditions, deterrence becomes nearly impossible. The defender cannot credibly threaten to retaliate against a range of potential yet unproven suspects.

Although it is unlikely that any single actor is in a position to pose a grave threat to the United States, it is increasingly conceivable that a revisionist actor could seek out third-party capabilities for the creation of a customized capacity to threaten or strike against America's ability or willingness to use military force—undermining the deterrent threat that ultimately provides national security. It is for this reason that hybrid threats deserve increased attention. With that in mind, we offer the following illustration of the potential mechanics and risks that hybrid threats could pose to the United States.

Figure 1. Utility of Strategic Hybrid Threats and Principal Actors

PROS

- Acquire capabilities beyond endogenous skills and resources.
- Relatively quick development time.
- Leverage unexpected avenue of attack.
- Anonymity.

CONS

- Potential lack of control over agent.
- Potential dependence on agent may flip the nature of the relationship.
- Threat/Attack may not be sustainable.

Iran's Potential Hybrid Threats

To be clear, much of what follows is evidence-based conjecture. It is presented to illustrate the danger posed by strategic hybrid threats. Nonetheless, what is described occupies the

realm of the possible, if not probable—and may be unfolding at this very moment.

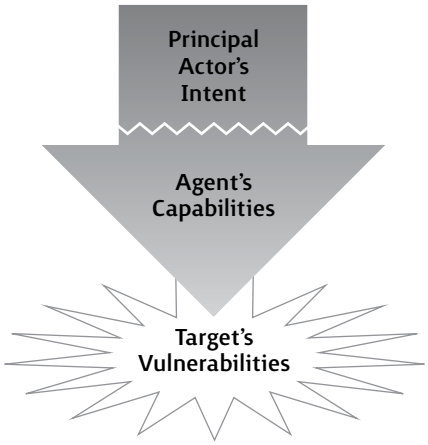
Threats emerge out of the conflicting objectives of a given set of actors and the context of current conditions; we use these as our start point. From the perspective of the United States and the status quo, the government of Iran represents a revisionist power. It seeks to rework the politics and power of the Middle East, establishing regional hegemony for itself while promoting the relative position of its political ideology and Shia Islam. These are Iran's maximum strategic objectives. Its minimum strategic objectives are to prevent regime change in Tehran.[8] To achieve these objectives, it has employed a grand strategy designed to frustrate and weaken the ability of neighboring powers (and the United States) to buttress the current system or challenge Iran's domestic regime. To operationalize its grand strategy, the government of Iran has employed state-sponsored terrorism and occasionally conventional force. Iran's maximum strategies have thus far failed. Policies in support of its minimum objectives have been successful.

Current geopolitical conditions now present opportunities for Iran. The political upheaval in (and U.S. exit from) Iraq, a combat-weary United States, and the effects of the Arab Spring have weakened the regional status quo. Still, Tehran lacks the endogenous capability to realize its maximum strategic objectives, and even a relatively drained United States poses a threat to the regime's minimum objectives. This creates motivation for the government of Iran to find innovative solutions that would allow it to exploit current conditions. Developments outside the geography of the Middle East hint at the possibilities for hybrid threats in support of Iran's strategic objectives.

the principal-agent relationship of the hybrid threat makes deterrence more difficult

In Mexico, President Enrique Peña Nieto has promised to commit more resources to fight his country's narco-insurgency.[9] This is good. In the short term, however, violence and

Figure 2.



Strategic Hybrid Threats are produced through principal-agent relationships that combine one actor's intent with another's capabilities for the purpose of seriously decreasing or adversely changing vital elements or instruments of the target's power.

CORE CHARACTERISTICS

Origin - gives rise to the threat's purpose and objective.

Composition - determines the avenue of attack and the duration of the threat.

Fungibility - determines the range of potential targets and the ease of a priori detection and defense.

instability are likely to continue. Trafficking on the part of the drug cartels poses a threat to both the United States and Mexico. Their routes into the United States will continue to provide a conduit for the transport of money, weapons, drugs, and people between the two countries. Furthermore, Mexico's internecine warfare creates within the cartels an ever-increasing need for greater weaponry and tactical expertise—something Iran could supply in return for access to the cartel's smuggling routes.

In the United States, dependency on ever-denser cyber networks is growing. These networks pay great dividends. They make the energy sector more efficient, fuel economic growth, support the health and well-being of American business and educational endeavors, and are central to its modern military capability. They have become intertwined with the vital instruments of U.S. national power. They have also shifted and diffused American vulnerabilities. Furthermore, these changes have been accompanied by a diffusion of the knowledge and resources needed to threaten those cyber networks. Iran may not possess sufficiently robust cyber capabilities with which to attack the United States, but others do.

Iran may not possess sufficiently robust cyber capabilities with which to attack the United States, but others do

With their objectives and these conditions in mind, it is plausible that Iran could move to custom engineer two different types of strategic hybrid threats against the United States. One is a hybrid guerrilla threat and the other a hybrid cyber threat. Each has the capability of supporting Tehran's minimum goal of preventing regime change in Tehran and its maximum goal of regional hegemony.

Hybrid Guerrilla Threat

What might a hybrid guerrilla threat from Iran look like? More than likely, it would take the form of a small-scale attack against the American population, infrastructure, or military targets. It would be designed to divert attention and resources away from, or to undermine the political will to take, certain actions. Consistent with the definition above, the strategic objective of the assault would be determined by the government of Iran. For example, the objective might be to prevent U.S. actions against Iranian nuclear facilities or prevent U.S. involvement in Syria. Depending on how much risk the regime in Tehran might be willing to accept, its perceptions about U.S. intentions, and/or the strength of its domestic position, a hybrid guerrilla threat could also be deployed in an attempt to force an easing of U.S.-led oil sanctions or as a means for opening up space for Iranian policies in the Middle East. In short, a hybrid guerrilla threat could serve as an ultimatum to gain concessions.

Because Iran likely lacks the expertise and experience to successfully execute such a strategic attack, including the ability to confidently transport the necessary men and materials onto U.S. soil without detection, Tehran would need to establish principal-agent relationships to acquire capabilities and increase its probability of success.

Hizballah, long an Iranian proxy against Israel and Lebanon, could provide the expertise necessary for such an attack. Hizballah excels at small unit tactics. It has proven skills in the operation of 6- to 10-man teams in dense urban environments against a militarily superior adversary.[10] It possesses the tactical

knowledge needed to carry out a guerrilla attack within the United States and has proved willing to target U.S. interests overseas. Given its longstanding relationship with and deep ideological ties to the government of Iran, it can be assumed that Hizballah would be willing to coordinate and carry out such attacks.[11] Getting its fighters and the necessary equipment onto American soil, however, represents a capability that is not only beyond Iran, but Hizballah as well. This would necessitate a second agent to complete the crafting of the hybrid threat. Enter the cartels.

Mexican drug cartels have access to the United States and to the weapons, explosives, and communications equipment that would be needed to facilitate an attack. The cartels have established routes into at least 233 American cities in 48 states.[12] They have proven adept at securing weapons or improvising them when necessary. Why might the cartels agree to help Iran? As criminal enterprises, they have traditionally sought to avoid bringing attention (and heat) upon themselves. The short answer is that they are at war. Things have changed. It is not hard to imagine a cartel being willing to serve as a transactional agent of the Iranian regime. They could supply transport to American targets in exchange for more sophisticated weapons and explosives (including rockets, antitank weapons, and Semtex) and tactical knowledge—all of which could then be employed in their fight against Mexican authorities and/or rival organizations.

Essentially, the hybrid guerrilla threat is that of a Mumbai-style assault on U.S. soil carried out by Hizballah fighters at the direction of the government of Iran and facilitated by Mexican drug cartels. What makes this a strategic hybrid threat is the fact that it could divert U.S. attention or sap American political will at a critical moment, allowing Iran to further its maximum goals. The fungibility of this threat adds to its danger. It could deploy against a range of targets, and easily shift to avoid detection or in response to the strengthening of U.S. defenses. A threat against Los Angeles could become a threat against Kansas City. For this reason, even if U.S. intelligence became aware of such a threat, it could be difficult to stop.

Figure 3. Potential Hybrid Guerrilla Threat from Iran Against the United States

From the Iranian perspective, a hybrid guerrilla threat makes sense; it is cost-effective, fungible, and hard to detect. It has a good chance of accomplishing the range of objectives for which it might be used. For all these reasons, it would be foolish to ignore this threat—or dismiss the likelihood that it could occur. Yet it has limits.

A Mumbai-style assault that kills American citizens on U.S. soil would bring about an overwhelming punitive strike against Iran. Logically (but not assuredly), the government of Iran knows this. Furthermore, it can be expected that Iran's military would reinforce this point by reminding the current regime that even a weakened United States possesses the ability to unleash a crippling strike from the air and sea without the need to engage ground forces. An attack on U.S. soil would certainly give the United States casus belli to attack Iran and would threaten the Iranian government's minimum and maximum objectives. Yet actors miscalculate and at times behave irrationally. Under the pressure of the sanctions regime, under the belief that no other course of action existed—or in an attempt to quell internal divisions and rally the Iranian people around the regime—the government of Iran might unleash such an attack. U.S. national security should not be dependent upon sound judgment in Tehran.

Hybrid Cyber Threat

In the last few months, Iran has engaged in a heavy degree of cyber saber rattling, promising a "teeth-breaking" response to the cyber attacks launched against it.[13] Because Tehran has itself suffered cyber attacks, it may be motivated to respond in kind. Yet as discussed, a hybrid cyber threat would be most likely undertaken to forestall U.S. action to gain Tehran time and space to achieve its strategic objective(s). Thus, a hybrid cyber threat would be customized to neutralize American capabilities by diverting attention and resources—and/or undermining the political will of the United States. Although impossible to rule out, it is unlikely the government of Iran would instigate an attack designed to produce mass casualties and/or gravely harm the United States. As in the earlier illustration, triggering a full-scale and potentially unlimited U.S. military response threatening the existence of the current regime could not conceivably serve the government of Iran's strategic objectives—but it cannot be ruled out, especially if the current regime feels cornered or believes such would assuage domestic pressure against the regime.

The most likely hybrid cyber threat scenario is one in which a threat (or actual attack) is deployed either to distract vital instruments of U.S. power away from Iranian actions or to render those instruments blind, deaf, mute, and/or ignorant of Iranian activity. This could be done in three general ways. First, cyber attacks against the electrical grid (including American nuclear reactors), water supply, air traffic control system, or the financial system—including banking, commerce, and/or stock and commodities markets—could easily produce sufficient distraction. To be successful, such attacks need only divert the attention of the national security apparatus. They need not be devastating in effect or national in scale. They need only generate sufficient discomfort and concern within the general public that they foster the perception of crisis. Second, a hybrid cyber attack could take the form of a psychological operations campaign. Such a campaign could involve the theft and release of sensitive information

designed to create political turmoil to block a U.S. response. This could be accomplished by releasing information that calls into question the legitimacy of Washington's motives and creates domestic and international resistance to U.S. action. Doing this could raise the costs of any given American response to the point that it becomes prohibitive. Third and finally, depending on the strategic objectives of Iran and its perceptions concerning risk and reward, a cyber attack could be launched directly against U.S. civilian and military communications networks. An attack against these could disrupt message traffic and deceive sensor data. It could conceivably replace them with false information. Such an attack could be launched to conceal Iranian movements by preventing U.S. or allied sources from observing or reporting on it. An attack against U.S. communications networks could also be used to alter deployment or resupply orders, in the hope of ensuring U.S. forces were out of place or unable to execute a timely response. Regardless of its exact manifestation and whether it is aimed at civilian or military targets, a cyber attack in support of Iran's strategic objectives could increase the frictions of war faced by any U.S. response to Iranian aggression. Still, at this point, Iran cannot execute such a strike alone.

A sophisticated and grave cyber attack against the United States is not confidently within the reach of Tehran—yet. It is true that the government of Iran has begun investing in its cyber capabilities. At this point, however, those investments are primarily aimed at securing its minimum objective of regime security from domestic threats. These cyber investments have increased the regime's ability to monitor the online activities of its citizens. To launch a cyber attack against the United State that is sufficient in scale to achieve the goals above—one significant enough to be more than a nuisance—would require technical expertise beyond that actually demonstrated by the Iranian government.

Short of the actions of a well-placed spy or traitor, a significant cyber attack against the United States would require the creation of a large and sophisticated botnet, worm, or other exploit. Regardless of the instrument used, it would have to be capable of attacking the cyber infrastructure of the private sector and/or penetrating those of American military, Intelligence Community, and national security entities. The programming code used to craft the assault would need to have unique encryption protocols for its command and control. Such sophistication would be necessary to deploy the attack, prevent detection (and a subsequent spoiling attack), and execute the threat at a moment synchronized with the execution of regional actions taken to secure Iran's strategic objective(s). To develop such a customized hybrid cyber threat, Iran needs agents willing to provide the required technical capabilities.

a hybrid cyber threat would be customized to neutralize American capabilities by diverting attention and resources

As in the earlier illustration, Hizballah represents one potential agent with which the government of Iran could fabricate a hybrid cyber threat. Its standing relationship and ideological alignment with Iran makes it a trusted and willing partner. Hizballah has demonstrated offensive cyber expertise beyond that of the current Iranian regime. The Central Intelligence Agency has noted Hizballah's

growing cyber capabilities for more than a decade. Furthermore, its technical expertise was displayed during its 2006 summer war with Israel. During that war, Hizballah proved capable of data interception and hijacking Internet and communications infrastructures. It has been implicated in cyber attacks against

Hizballah represents one potential agent with which the government of Iran could fabricate a hybrid cyber threat

targets in Saudi Arabia and other countries and is continuing to expand its cyber capabilities. In June 2011, the Cyber Hizballah was established to train and mobilize hackers.[14] Nonetheless, Hizballah does not represent the best choice for a hybrid cyber threat from Iran; its technical expertise, while greater than Iran's, is likely insufficient to the challenge. Furthermore, its close relationship with the current Iranian regime makes it difficult for Tehran to capitalize on one of the benefits of such an attack—the ability to remain anonymous, shielded by the difficulty of attribution. Anonymity would be of no importance for a hybrid threat in support of Iran's minimum objective, but could prove vital in support of its maximum objectives.

Hacktivists, disaffected and technically sophisticated individuals, represent another potential source of agents for the crafting of a hybrid cyber threat. Such individuals might self-identify with the principle behind the creation of the hybrid threat. Media reports suggest this may have been the case with the 2011 cyber attacks that brought down the Dutch firm DigiNotar. The attacks, sanctioned and supported by the government of Iran, appear to have been carried out by a single individual of Iranian descent living in Europe. Using fake security certificates, his attacks compromised the security and communications of Dutch government Web sites. The attacks also inflicted significant damage to the cyber infrastructure of the Netherlands. DigiNotar collapsed under the weight of the attacks; its security certifications had to be quarantined and were rendered useless.

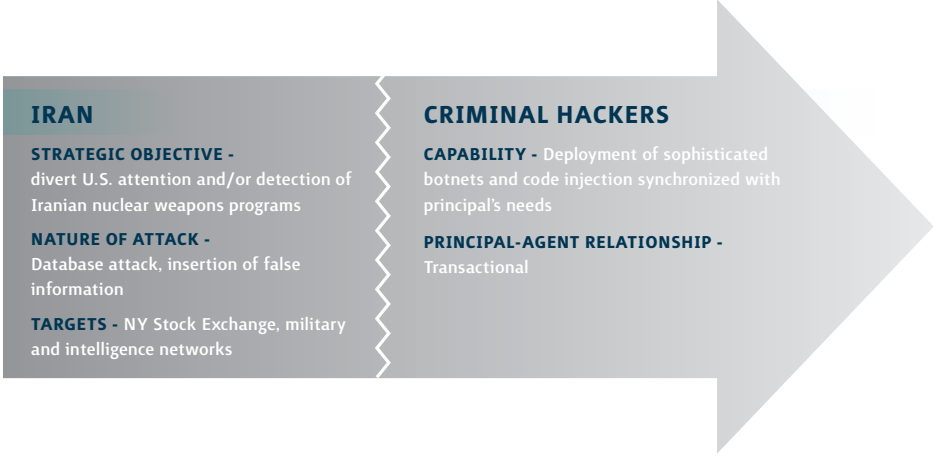
Purportedly, the hacker was motivated by the desire to avenge Muslims massacred at Srebrenica during the Balkan wars of the 1990s. The hacktivist held the Dutch responsible because of the failure of their peacekeepers to prevent the slaughter. Like Hizballah, hacktivists present problems as potential agents in a hybrid cyber attack against the United States. Uneven levels of technical expertise and questions about their ability to carry out the level of synchronization necessary to achieve the strategic objectives motivating the attack would likely lead the government of Iran to seek out more proven and disciplined agents.

Criminal hackers represent the most likely agents for an Iranian-led cyber attack against the United States. Several groups, including organizations operating in Eastern Europe, Russia, China, and Taiwan have a history of operating as hackers-for-hire. They have proven adept at both cyber-spying and denial-of-service attacks. Criminal hackers have proved to be at the forefront of the weaponization of malware—including the development of techniques for corrupting computer programs through the injection of additional coding that can consume processor functions and bring down large databases. Many criminal hackers specialize in helping clients evade detection. Most importantly, they have proved capable of synchronizing their attacks

with the coordinated efforts of a principal actor. The best example can be found in the cyber attacks against Georgia that preceded the Russian invasion. The motivation behind their willingness to act as an agent of Iran would be simple and persuasive: money. Their skills and motivation make criminal hackers the best, most reliable set of agents with which the Iranian regime could construct a hybrid cyber threat against the United States.

How exactly might a hybrid cyber threat manifest itself? Let us consider what is perhaps the worst-case possibility: a strategic campaign in support of Iran's nuclear ambitions. Consider this potential sequence of events. In the furtherance of its maximum objective of regional hegemony and its minimum goal of preventing regime change, the current government of Iran decides to develop nuclear weapons. To achieve that, the regime undertakes a sprint toward the weapons-grade enrichment of uranium and the construction of a bomb. Such a strategy would require the regime to prevent detection, and then (if necessary) delay any American response. Knowing this, the government of Iran could turn to a hybrid cyber threat as an effective mechanism for avoiding detection by distracting, blinding, and deceiving the U.S. Government. To craft the threat, Iran could decide to enter into a transactional principal-agent relationship with criminal hackers to launch an attack against the New York Stock Exchange to distort prices, interfere with trade activity, and even bring down the electronic systems of the exchange—wiping out economic activity and halting the markets. Such an attack would easily rattle the confidence of global markets. It would precipitate a crisis likely to engulf the attention of the White House and Congress without drawing attention toward Tehran. At the same time, or perhaps as Iran neared the nuclear finish line, Iran could craft another hybrid cyber attack, again with the support of criminal hackers. This time the attack could be aimed at U.S. communications and sensor networks. Information could be fed into the system to create white noise, making it harder for American analysts to develop solid intelligence. If the United States became suspicious,

Figure 4. Potential Hybrid Cyber Threat from Iran Against the United States



Iran could decide to feed misinformation into U.S. communications and intelligence networks to draw attention to a false nuclear site in Iran, providing diversionary targets for U.S. military strikes, protecting the site of Iran's actual weaponization process, and buying the regime time to achieve its objectives.

How realistic is the above scenario? Why might Iran go the hybrid route? Why not develop these capabilities internally? From the Iranian perspective, a hybrid cyber threat provides three benefits to the current regime. First, it is fast. There is an arms bazaar of cyber weapons available from criminal hackers, and using it to acquire offensive capabilities would be quicker than domestic development. This lowers the bar to the level of point and click.

there is an arms bazaar of cyber weapons available from criminal hackers, and using it would be quicker than domestic development

Second, transactional principal-agent relationships avoid one potential pitfall of internal development—the fact that domestically held cyber skills could be turned against the regime itself. As the 2009 Iranian elections and Green Movement demonstrated, cyber tools have the potential not only to secure the current regime, but also to threaten it. Third, the hybrid route offers a heightened chance of avoiding attribution. A hybrid threat would offer the government of Iran the ability to hide behind the agent of the attack. This would introduce doubt into the political processes of the United States and international community, which could forestall (or reduce the severity of) any response. Given this, and given the strategic risk-to-reward ratio for Iran, dismissing the potential of such a threat would be foolish.

Countering Strategic Hybrid Threats

Strategic hybrid threats have the potential to directly threaten the safety and security of American citizens, society, and interests at home and abroad. They manifest themselves in novel combinations. They are fungible. They may strike municipal, state, or national targets. This last point magnifies the intrinsic difficulty of countering hybrid threats; it ensures that any defense against them is inherently a complex operation. It defies a hierarchical top-down response. It requires multiple agencies at various levels of governance (including state and local) to assume complementary roles and operate in close proximity—"often with similar missions but conflicting mandates."[15]

Given the above, what advice and prescriptions do we offer American practitioners and policymakers? We begin by recognizing the fact that the critical tasks that must be accomplished to defend against hybrid threats are beyond the capability and operational purview of any single actor. Strategic hybrid threats present a unique challenge. Because they may manifest themselves at any or all levels of governance, they confound modern approaches to national security. They cannot be solely or adequately addressed by an executive authority who directs actions abroad to provide security at home. When it comes to responding to strategic hybrid threats, no single service solutions exist. Each critical task—detection, analysis, and response—is itself a set of complex operations that must be coordinated among private and public sector entities at the local, state, and national levels. This requires a high degree of coordination among actors that may have little history of working together. Luckily, history provides a model for

how such challenges may be undertaken, managed, and accomplished.

Beginning with Spain's King Charles V, Western governments have employed war councils composed of public- and private-sector actors to address complex threats to national security.[16] Before the rise of our modern bureaucratic security structures, war councils were employed to determine strategy and select courses of action. They were also employed to manage the current and future material needs of military operations. Historically, the use, composition, and authority of war councils were of an ad hoc nature in the United States. American war councils operated at the state and Federal levels—and at times both, acting as a mechanism for uniting state and Federal efforts. For example, this was the case during World War I when the Federal Government asked the states to create councils of defense to support the national Council of Defense. Although American councils of war varied in their levels of statutory authority, and some existed as purely political bodies while others were created by legislative act, they shared a common trait. They were customized in response to the specific threat faced and expired once it had been defeated. Interestingly, war councils (in both the United States and in other Western governments) normally lacked operational authority or control. These were traditionally left to the constituent members of the council, which served as a mechanism for deliberation, decisionmaking, and coordination.

We recommend that the war council concept be dusted off, updated, and tailored to meet the specific characteristics and challenges of hybrid threats. It provides the best model for the establishment of customized (and by necessity, decentralized) responses to meet customized threats. In many ways, we expect that threat councils should mirror the principal-agent relationship that gives rise to the threat. At the core of a threat council would be a principal actor, one responsible for the national security of the defender. In the United States, that role would be fulfilled by the President or by another actor or entity entrusted to act under Presidential authority—for example, the National Security Staff (historically known as the National Security Council staff). The direction or management of the council might fall to the Director of National Intelligence or another designee. The important point is that under the constitutional architecture of the United States, any threat council could have only a limited hierarchical nature. To be successful, it must find a way to leverage decentralized actors by providing a seat at the table for state and local entities, which any defense against strategic hybrid threats would require. Even outside the United States, the fungible nature of hybrid threats results in a situation in which no strict principal-agent relationship is possible in the defense. This is the value of the war council model—where the principal actor at the core must negotiate, coordinate, and at times accept a role subservient to the other actors comprising the council.

In practice, once a hybrid threat has been identified (either through observation or theorization), a threat council should be organized. It must then be tied into existing national security structures. Logically, the most effective way to accomplish this would be to connect the newly established threat council to an existing forum for interagency coordination. Such forums are a mainstay of the modern White House. Labeled Interagency Policy Committees in the Obama

administration and Policy Coordinating Committees in the Bush administration, these forums coordinate national security policy and provide policy analysis for other senior committees. Tying a threat council to the appropriate executive body for coordination would ensure that national policy and decentralized action are unified to the greatest degree possible. Given the fungibility of hybrid threats, council membership ought

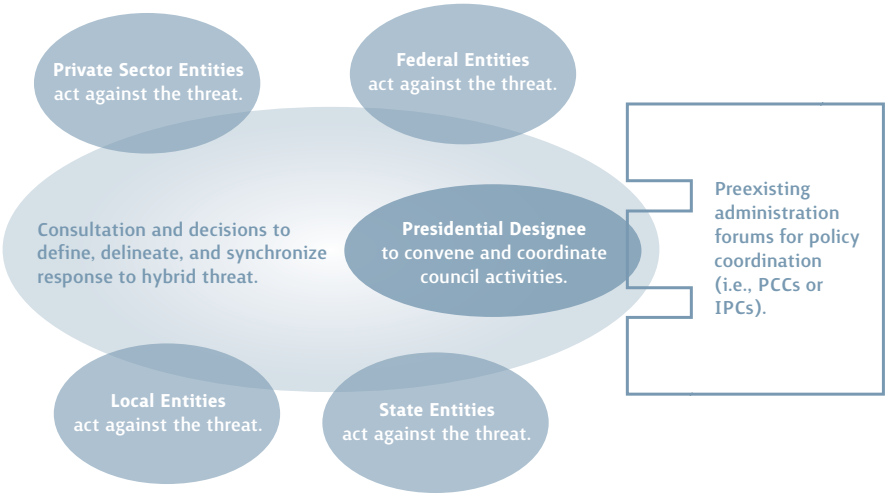
tying a threat council to the appropriate executive body for coordination would ensure that national policy and decentralized action are unified

to be as inclusive as possible. The number of assembled stakeholders and experts should be expansive enough to provide appreciation for strategic context as well as operational truths. Furthermore, council membership must provide for the multidimensional and interdisciplinary perspectives necessary to question conventional assumptions, evaluate standard operating procedures, foster learning, and provide for red teaming between the council's conclusions and recommendations.

Once established, the council must analyze the hybrid threat to define and delineate its specific character. Based on that, the council must deliberate and coordinate a response. Its actions must be unified. In the United States, this means bringing concert to the application of a response across various agencies and jurisdictions at the local, state, regional, and Federal levels of governance. This can only be accomplished through a well-defined mission statement. The mission statement itself should be a product of the council's work and should identify the core elements of the threat and the causal relationships and motivations that give rise to it.

Based on this information, the council should identify and implement actions to break the principal-agent relationship. Everything possible should be done to counter the enemy's partnership and cleave the

Figure 5. Threat Council Model within U.S. Constitutional Architecture



agent from the principal.[17] The threat council's mission statement must also simplify the threat by highlighting the key weaknesses of both the attacker and defender, which is vitally important for the facilitation of the response. Once that is done, council members must coordinate orders of battle, attack plans, and arrests to maximize strategic impact. They must also evaluate the consequences of such actions, including their second- and third-order effects.

Council members must also coordinate actions to harden the defender's vulnerabilities. In doing this, the council should strive to reduce the defender's area of vulnerability to the hybrid threat. At the very least, it should endeavor to shift the defender's point of vulnerability outside the area where it directly threatens the lives and security of civilians.[18] As that suggests, the success of the threat council depends on its ability to produce a clear understanding of the hybrid threat. This understanding becomes the touchstone upon which activity will be coordinated and the concept that unifies the activity of the council's constituents.

Our final recommendation is a direct one: act now. Under the leadership of the Director of National Intelligence (or other designee), threat councils ought to be established based on the two potential avenues of attack outlined above, the potential guerrilla threat and potential cyber threat. Each of these scenarios represents growing dangers whether carried out by the principal-agent relationships we describe or some other combination of actors. Because of that, now is the time to constitute councils that can begin coordinating the work of detection. Other avenues of attack may exist. If so, those too deserve attention. We need to be on watch; it is vitally important that we begin to act.

Conclusion

We have attempted to illustrate the risks strategic hybrid threats present to the national security of the United States. The Iranian examples represent but one set of dangers. They are the most pressing examples, but others exist. General Carter Ham, commander of U.S. Africa Command, recently warned of emerging trends with al-Shabaab and Boko Haram.

to meet the customized challenges hybrid threats present, the United States needs a customized response

General Ham's comments suggest that al-Shabaab and Boko Haram may be fostering principal-agent relationships to enhance their capabilities.[19] Similarly, General Douglas Fraser, commander of U.S. Southern Command, has warned of developments in the Tri-Border Region of Brazil, Paraguay, and Argentina. General Fraser has highlighted growing relationships among Hizballah, al-Gama'a al-Islamiyya, al-Jihad, al Qaeda, Hamas, al-Muqawamah, and local actors in the region.[20] Still other reports suggest that Revolutionary Armed Forces of Colombia (FARC) guerrillas have established a principal-agent relationship with entities in Venezuela and offshoots of al Qaeda. The Venezuelans supply FARC with safe haven airstrips, and al Qaeda supplies access to safe havens and routes through Africa and Europe. The threat brings drugs into Europe and the United States, generating revenue for all parties.

Strategic hybrid threats pose a unique and growing danger to the United States. Their origin, composition, and fungibility present novel challenges, not the least of which is the

fact that their nature reduces detection and response times to the point that single-service defenses are practically useless. To meet the customized challenges hybrid threats present, the United States needs a customized response, and the establishment of threat councils provides a model and starting point.

As with all national security discussions, we do not expect complete agreement with our argument. It is important, however, that we engage in an honest debate that differentiates strategic hybrid threats from other dangers, considers the risks they pose, and examines how best to mitigate their effects. Strategic hybrid threats warrant increased attention and thought, thus we welcome the debate. PRISM

Notes

[1] Most of the debate over hybrid threats has thus far been focused on the tactical or operational levels and whether or how the uniformed armed services ought to adapt in response. What has received far less attention is how hybrid threats might be used to achieve strategic goals.

[2] Robert G. Walker, "Spec Fi: The United States Marine Corps and Special Operations" (Master's thesis, Naval Postgraduate School, 1998), 4–5, 7–12; James N. Mattis and Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Wars," *Proceedings* 132, no. 11 (2005), 30–32; Frank G. Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs," *Orbis* 50, no. 3 (2006), 397–399; Gian P. Gentile, "The Imperative for an American General Purpose Army That Can Fight," *Orbis* 53, no. 3 (2009), 461; Russell W. Glenn, "Thoughts on 'Hybrid' Conflict," *Small Wars Journal* (2009), available at <http://smallwarsjournal.com/jrnl/art/thoughts-on-hybrid-conflict>; T.X. Hammes, "How Will We Fight?" *Orbis* 53, no. 3 (2009), 372–373; Fulvio Poli, "An Asymmetrical Symmetry: How Convention Has Become Innovative Military Thought" (Master's thesis, U.S. Army War College, 2010), 1–8.

[3] John J. McCuen, "Hybrid Wars," *Military Review* 88, no. 2 (2008), 107–113; Hammes, 373; Frank G. Hoffman, "Hybrid vs. Compound War," *Armed Forces Journal*, 2010, available at <www.armedforcesjournal.com/2009/10/4198658/>.

[4] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 8, 2010, amended April 15, 2012), 166, 334; Mark Grdovic, "Developing a Common Understanding of Unconventional Warfare," *Joint Force Quarterly* 57 (2nd Quarter 2010), 136–138.

[5] Hoffman, "Complex Irregular Warfare," 397–398.

[6] This conceptualization borrows the definition of strategic vulnerability from JP 1-02. Thus, we assume that strategic hybrid threats could be aligned against a defender's political, geographic, economic, informational, scientific, sociological, or military factors. See JP 1-02, 307.

[7] It is this aligning of the agent's capabilities with the defender's vulnerabilities that erroneously leads to the equating of asymmetric warfare with hybrid threats.

[8] Anoush Ehteshami, "Iran: Regional Power with a Global Strategy," Podcast, International Relations and Security Network, Zurich, Switzerland, Swiss Federal Institute of Technology, available at <www.isn.ethz.ch/isn/Digital-Library/Podcasts/Detail/?lng=en&id=140438>; Vali Nasr, "When the Shiites Rise," *Foreign Affairs* 85, no. 4 (2006), 58–74.

[9] Adam Thomson, "Mexico's President-elect to Shift Drug War focus with 40,000-strong force," *Financial Times*, July 3, 2012, A1.

[10] Steven Erlanger and Richard A. Oppel, Jr., "A Disciplined Hezbollah Surprises Israel With Its Training, Tactics, and Weapons," *The New York Times*, available at <www.nytimes.com/2006/08/07/world/middleeast/07Hezballah.html?pagewanted=all>; Andrew Exum, "Learning from Hezbollah," Middle East Strategy at Harvard Blog, available at <https://blogs.law.harvard.edu/mesh/2007/12/learning_from_Hezbollah/>; Casey L. Addis and Christopher M. Blanchard, *Hezbollah: Background and Issues for Congress*, R41446 (Washington, DC: Congressional Research Service, January 3, 2011).

[11] Cyrus Miryekta, "Hezbollah in the Tri-Border Area of South America," available at <http://usacac.army.mil/cac2/call/docs/11-15/ch_11.asp>.

[12] Tyler Hayden, "How Do You Solve a Problem Like the Panga? Sheriff Meets with Federal Officials on How to Deal with Increased Maritime Smuggling," *Santa Barbara* [CA] *Independent*, available at <www.independent.com/news/2012/jul/09/how-do-you-solve-problem-pangas/?on>; "Mexican Cartels: Drug Organizations Extending Reach Farther into U.S.,"

Associated Press, available at <www.npr.org/templates/story/story.php?storyId=124703094>.

[13] Richard Adhikari, "Iran Promises Knuckle Sandwich if US Cyberattacks Persist," *TechNewsWorld*, available at <www.technewsworld.com/story/Iran-Promises-Knuckle-Sandwich-if-US-Cyberattacks-Persist-75736.html>.

[14] Hilary Hylton, "How Hizballah Hijacks the Internet," *Time.com*, available at <www.time.com/time/world/printout/0,8816,1224273,00.html>; Kevin Coleman, "Hizballah's Cyber Warfare Program," *DefenseTech*, available at <http://defensetech.org/2008/06/02/Hizballahs-cyber-warfare-program/>; Greg Grant, "Hizballah Claims It Hacked Israeli Drone Video Feeds," *DefenseTech*, available at <http://defensetech.org/2010/08/10/Hizballah-claims-it-hacked-israeli-drone-video-feeds/>; "Spotlight on Iran (Week of September 21–28, 2011)," The Meir Amit Intelligence and Terrorism Information Center, available at <www.terrorism-info.org.il/en/article/17844>.

[15] Michael Miklaucic, "Introduction," in *Commanding Heights: Strategic Lessons from Complex Operations*, ed. Michael Miklaucic, x (Washington, DC: NDU Press, 2010).

[16] I.A.A. Thompson, "The Armada and Administrative Reform: The Spanish Council of War in the Reign of Philip II," *The English Historical Review* 82, no. 325 (1967), 698–725; Elizabeth Greenhalgh, "Myth and Memory: Sir Douglas Haig and the Imposition of Allied Unified Command in March 1918," *The Journal of Military History* 68, no. 3 (2004), available at <www.jstor.org/stable/3396728>; Nicholas A. Lambert, "Strategic Command and Control for Maneuver Warfare: Creation of the Royal Navy's 'War Room' System, 1905–1915," *The Journal of Military History* 69, no. 2 (2005), available at <www.jstor.org/stable/3397404>.

[17] McCuen, 111.

[18] Peter W. Chiarelli, "Complex Operations in Practice," in *Commanding Heights*, 50–51; William H. McRaven, *Special Operations Case Studies in Special Operations Warfare: Theory and Practice* (New York: Presidio Press Books, 1995), 1–25.

[19] David Lerman, "African Terrorist Groups Starting to Cooperate, U.S. Says," *Bloomberg.com*, available at <www.bloomberg.com/news/2012-06-25/african-terrorist-groups-starting-to-cooperate-u-s-says.html>; Carter Ham, "Statement of General Carter Ham," testimony before the House Armed Services Committee, available at <www.africom.mil/fetchBinary.asp?pdfID=20120301102747>.

[20] Wayne Simmons and Kerry Patton, "Southern Command's Critical Mission," *The Washington Times*, March 20, 2012, available at <www.washingtontimes.com/news/2012/mar/20/southern-commands-critical-mission/>; Douglas M. Fraser, "Posture Statement of General Douglas M. Fraser," testimony before the Senate Armed Services Committee, available at <www.armed-services.senate.gov/statemnt/2012/03%20March/Fraser%2003-13-12.pdf>.