The Specter of Non-Obvious Warfare

Martin C. Libicki

Innovations, both technological and organizational, over the last few decades have created a potential for non-obvious warfare,[1] in which the identity of the warring side and even the very fact of warfare are completely ambiguous.

The Stuxnet computer worm is only the most recent widely publicized example. This worm is believed to have infiltrated Iran's Natanz centrifuge facility, causing equipment to destroy itself over a period of weeks and leading to the premature retirement of 10 percent of Iran's uranium enrichment capability. Within several months of the worm's public disclosure (September 2010), Western intelligence sources announced that the earliest date Iran could build a bomb had been pushed back several years. Until the worm was discovered and dissected, the Iranians were uncertain why their equipment wore out so fast. Indeed, when confronted publicly with the possibility, they first denied that any such attack had happened, only to reverse themselves obliquely two months later.

Although non-obvious warfare can be epitomized by cyber warfare,[2] states can attack one another in many ways without the victim being certain exactly who did it or even what was done. Some, like electronic warfare (against nonmilitary targets) and space warfare, have yet to materialize in any strategically significant way. Others, such as naval/land mining or sabotage, have long historical antecedents. What they share is ambiguity. A short list of warfare types that *could* plausibly be conducted in a non-obvious manner includes

- cyber warfare;
- space warfare;
- electronic warfare;

Martin C. Libicki, PhD, is a senior management scientist at RAND Corporation, focusing on the impacts of information technology on domestic and national security. He has published *Conquest in Cyberspace*: *National Security and Information Warfare* and *Information Technology Standards: Quest for the Common Byte*, as well as numerous monographs. Prior employment includes the National Defense University, the Navy Staff, and the GAO's Energy and Minerals Division. Dr. Libicki holds a master's degree and a PhD from the University of California–Berkeley.

- drone warfare;
- sabotage, special operations, assassins, and mines;
- proxy attacks;
- weapons of mass destruction; and
- intelligence support to combat operations.

Non-obvious warfare stands starkly in contrast to, say, a tank invasion across the German-Polish border, an event unlikely to spur questions such as whose tanks are those . . . and why are they here? By contrast, the *uses* of non-obvious warfare are limited. It is quite difficult to take over the capital of another country anonymously (proxies may do so but at that point often cease being proxies and evolve to dependents or even independents). Defensive warfare is almost always carried out by whomever owns what is being defended. Even coercion requires self-identification *if* the "me" in the point—"don't tread on me"—is to be adequately conveyed. But there are some types of warfare that can be satisfactorily or even more advantageously carried out if there is doubt about who did what. Again, Stuxnet provides an example. Retarding the Iranian nuclear program benefitted Israel, whether or not anyone knows for certain whether Israel (or anyone else) did it. Furthermore, if the purpose of warfare is to change minds in the victim's capital, uncertainty may focus subsequent reflection on what such an attack says about the security and (reduced) power of the victim rather than on the malevolence of the undetermined attacker.

Accordingly, this article explores the topic in several steps. The first is to develop a sense of what it means to be non-obvious. The second is to delineate several forms of warfare that may, under some circumstances, be non-obvious and why. The third is to speculate on how states (and non-state actors) might use non-obvious warfare. The fourth is to speculate on how victimized states can respond to the threat of non-obvious warfare.

When is Warfare Non-Obvious?

Ambiguity is the heart of non-obviousness. If the victim is unsure of who carried out an operation, it may hesitate to respond in the same way as if it were certain. Alternatively, the rest of the world might have doubts even if the victim is certain, leaving the victim wary of responding as it might have if *others* were very sure of matters.

Non-obviousness is enhanced if the events in question can themselves be questioned. Some could be accidents or utter mysteries, for example, the unexplained failure of a satellite. Others could be crimes, such as bank robberies by politically inclined groups, or acts of espionage—many events labeled as cyber attacks are really attempts to steal information. Nevertheless, some non-obvious warfare incidents would clearly be acts of war if they were obvious—in which case, the key ambiguity is the actor not the act.

Some forms of warfare are non-obvious because the relationship between the attacker and a state is unclear; for instance, to what extent is Hezbollah working for its own ends, and to what extent is it a puppet manipulated by Tehran? In some cases the perpetrators may be state employees that are not necessarily, or at least not provably, working under the command and control of the state itself. Does the fact that someone close to the Russian political structure claimed credit for having organized attacks on Estonian institutions in Russia mean it was an attack by Russia?[3] Pakistan's ISI intelligence agency has been accused of shielding Taliban warlords; so, is Pakistan at war with Afghanistan? If both questions can be answered "yes," then these are two examples of non-obvious warfare.

Finally, many forms of non-obvious warfare present no personal risk to war fighters—which it would have to, almost by definition, since the capture or identification of the perpetrator may make the source of the attack obvious. But one cannot conclude that *states* that employ such war fighters are off the hook just because their war fighters are. A no-fingerprints approach to warfare may be a logical next step after a no-footprints approach, but the two are still quite different.

Non-obviousness is not an absolute, and the actionable response threshold for the victimized state will vary greatly. The primary criterion is how confidently the victim feels a particular state carried out an attack—if, indeed, what happened really *was* an attack. This perceived likelihood is almost always going to be nonzero. Few states truly believe that no other state wants to harm them. Even what later prove to be accidents (e.g., the explosion in the USS *Maine*) is often blamed on other states (e.g., Spain). If there is a crisis (e.g., Spain's attempt to quell a Cuban insurgency), the tendency to believe that any harmful and unusual occurrence was an attack will be that much higher.

So the attacker who would strike with impunity must ask whether or not the confidence with which the victim believes that it carried out the attack

is likely to be greater or less than the confidence that the victim requires to respond to the attack. Everything depends on what the threshold of response is, and there may be many types of responses. Evidence sufficient to gain a criminal conviction in a US court "beyond reasonable doubt" is rarely the issue, although similarly high levels of confidence may, in fact, be required before the victim decides to go to war. On the other hand, mere suspicion may suffice to curtail active or disapprove prospective cooperative arrangements such as mutual military exercises, joint research, or network peering relationships. With some forms of non-obvious warfare, the target may be uncertain of state sponsorship but may convince itself that such a state has to shoulder some blame if it reasonably could have detected and stopped or hindered such an attack and refused to do so.

Exactly how the target state acquires the confidence that another specific state carried out an attack will also vary, but one cannot go very far wrong by considering means, motives, and opportunity. Opportunity—in the form of some traceable delivery vehicle—often best distinguishes obvious from non-obvious warfare. But opportunity is only one leg of the triad. Consider, for example, how the United States would react to the detonation of a so-called suitcase nuclear weapon circa, say, 1962. The suitcase would be incinerated, leaving little forensic evidence. But at that time, only three other states had the *means* to carry out a nuclear attack, and of those three, only one, the USSR, had a *motive* to do so. In such circumstances, the lack of a visible delivery vehicle would have little dented US confidence in the belief that the USSR had done it. Similarly, for many types of non-obvious warfare, such as attacks on spacecraft, the list of suspects would be fairly short since the number of space-faring nations is limited (although, in that case, the victim must also credibly distinguish accidents from attacks).

Types of Non-Obvious Warfare

What makes various forms of non-obvious warfare, in fact, non-obvious? We examine them individually.

Cyber Warfare

Hackers can sit anywhere and attack systems around the world, disrupting their functioning, corrupting the information they hold and the algorithms they run, and, as Stuxnet showed, even breaking machines by

feeding them harmful commands from hacked systems. Attribution is particularly difficult for a cyber attack. The ones and zeroes that constitute the attack do not bear the physical residues of their operators (especially if these ones and zeroes are copied from others' tools). Successfully attacked systems, almost by definition, cannot distinguish an attack from completely benign inputs at the time (with a distributed denial-of-service attack, it is volume, not content, that matters; the attacking bytes generally come from "innocent" machines that have been tricked into spamming the victim). Forensic methods such as tracing the attack back to its sources can be easily frustrated by bouncing the attack through enough portals, using the services of an innocent machine, or jumping on a third-party Wi-Fi connection. Difficulties in attribution may well be inherent to the medium and unlikely to be improved upon in coming years. States wanting to guess who attacked them find they must rely on means and motive. Means offer only a little help for an unsophisticated attack, since over 100 countries have investigated offensive cyber war and the list of hackers includes organized crime groups, nonstate actors, and individuals. It is generally believed that only a state could have pulled off a sophisticated attack such as Stuxnet, with its four zero-day exploits and two stolen certificates. Iran may have figured, once it realized that it *had* been attacked, only Israel and the United States would have both the reason and the talent to carry out such an attack. But it is not entirely impossible that either Russia or China may have wanted to retard Iran's rush to nuclear weapons.

No one yet knows whether cyber attacks carried out in a non-obvious manner will prove advantageous to those who carry them out. It is by no means clear that Russia's (or Russian) attacks on Estonia or Georgia did it that much good. If Israel attacked Iran in cyberspace, what looks like success may be viewed as the beginning of a new set of military operations, or, alternatively, a very special case that no one else can or need duplicate.

Space Warfare

Satellites normally lose capability from time to time in the depths and darkness of space. An attack on a satellite without the attack vehicle being discovered may come close to the perfect crime. States may want to know what happened, but de-orbiting a satellite may not necessarily be something the satellite was designed to do, may be rendered impossible by the nature of the attack, and will require the expenditure of a substantial amount of fuel. Although post-recovery analysis would likely indicate

what happened, it still may not answer who did it. That noted, getting away with "satellite murder" presents difficulties. The United States has the capability to find every sufficiently large ground-based missile launch and tracks space objects supposedly the size of wrenches (the exact details are undoubtedly classified). Because it has a fairly good idea what every satellite is supposed to be doing, those otherwise employed necessarily get noticed, but the advent of microsats, nanosats, and picosats may complicate detection by subtraction in years to come. Ground-based systems might blind satellites, but the satellites have to be looking at whatever it is that is doing the blinding (hence, indicating where the laser is coming from). The number of states that can buy a launch is much larger than the few that can launch objects into space.

Electronic Warfare

As our wired world becomes increasing wireless, the potential for electronic jamming grows apace. Small generic radiating devices surreptitiously emplaced or scattered about can block GPS signals (at least for commercial receivers) and wreak havoc with communications, ranging from cell phone and emergency communications to machine controllers. Such devices can sometimes be quite difficult to find but not hard to characterize (deliberate jamming is unlikely to be confused with natural causes or accidents for very long). Using generic devices can frustrate trace-back, but the real trick in anonymity is to not get caught emplacing such devices. Once the devices start operating, their lifespan is limited, either because they are discovered or because their batteries die.

Drones

Under some relatively narrow set of circumstances, an attack by drones may be carried out without firm attribution. The requirements are many. The drone has to avoid crashing (or must be recovered if it does); otherwise, there is a fair chance of tracing even a generic drone back to its last buyer. The targeted country either has to have relatively poor radar coverage or abut territory or oceans where there is no radar coverage. If the drone comes from the ocean, the list of possible attackers can be limited to those with ships in the area at the time. The drone itself has to be fairly generic—so that its profile at a distance is consistent with the inventory of many different countries—or else stealthy. Finally, the possibility that a drone attack can be a non-obvious attack by the United States must

await the development of attack drones by countries *other than* the United States—failing that, any such drone will be assumed to be American. For states on the outs with the United States, the combination of motive and means may suffice.

Special Operators, Saboteurs, and Assassins

As with drones, the key to maintaining anonymity in special operations is to avoid getting caught. Ironically, the ability to carry out *many* special operations without getting caught requires so much organizational and professional skill that the number of countries capable of doing this is few—making accusations that much more credible. Hence, perfection may be its own undoing, unless the attacker shows considerable restraint. This category includes mine-laying by stealthy conveyance (e.g., submarines), which gives it a historic resonance, if nothing else, but also contemporary resonance, as in the mysterious—and disputed—damage to an Irish vessel primed to run Gaza's blockade.[4]

Proxy Attacks

This broad category includes terrorists, insurgents, militias, and privateers. Attribution becomes difficult because it generally requires the perpetrators be caught (or use a recognizable modus operandus) but mostly because it requires tying the perpetrator to a major actor. In practice, however, the link between insurgent groups and states really is ambiguous, and not necessarily by design; empowering individuals with organization, ideology, and weaponry tends to make them believe that their goals are important in and of themselves. The Vietcong, for instance, may have been established and sustained by North Vietnam but had somewhat different priorities.[5] Africa provides a more apropos case in which various countries that sponsored insurgencies against their neighbors managed to find themselves under siege by insurgents of their own, similarly backed.

Attacks Using Weapons of Mass Destruction

The so-called suitcase bomb of the Cold War era has been joined by the use of biological and chemical agents—of which there are many types—all of which offer, at least in theory, a method of killing people without a state necessarily getting caught doing it. Because weapons of mass destruction, as a general rule, are relatively small, their use may not require forcible insertion, and modern electronics allow them to be detonated

remotely. However, such attacks are considered particularly heinous, and nearly every state has signed one or more international treaties against doing so. For that reason, more such attacks may well be traced to their ultimate source than a similarly stealthy attack by high explosives. Granted, infectious agents, particularly those that may yet be invented by DNA recombination techniques, can be delivered in a very stealthy manner. But unless a state's own citizens are somehow immune to their effects, it is unclear what that state would gain from using them or, if used in a "doomsday machine" mode, why a state would want to be non-obvious about the matter.

Intelligence Support to Combat Operations

Although technically not warfare, a state with a sophisticated stand-off intelligence collection and processing/distribution mechanism can provide data that can be a great help for its friends. If the assistance is not directly intercepted and its distribution is limited, then others would have difficulty discerning the origin for certain (although states may suspect that opponents punching over their weight may have gotten some help, only a handful of countries could and would supply it). Unlike other forms of non-obvious warfare, helping out with information is not particularly heinous, and denials—or at least "neither confirm nor deny"—are par for the course in the intelligence world. Nevertheless the supplying state may not want to show its hand in the conflict lest it be accused of being a belligerent or if it has a rival that can then justify *its own* assistance to the other side.

It merits repetition that unless the attack looks like a complete accident—and the target is completely credulous—there is no such thing as a completely unattributable attack. Every state has its enemies or untrustworthy friends, and if anything untoward happens, the usual suspects will be trotted out for examination. Conversely, plausible deniability matters only if the victimized state really does need something close to judicial proof to take action or is relieved that the authorship of the attack is not so obvious that its unwillingness to respond is not seen as cowardice. Perpetrators do not have to be caught red-handed to suffer reprisal in the hands of those who can put means, motives, and opportunity together to form a sufficiently robust basis for action.

The Uses of Non-Obvious Warfare

It is often easier to state what *cannot* be done with non-obvious warfare. Its inapplicability for conquest and specific coercion has already been noted. Furthermore, any purpose that requires a sustained series of attacks cannot use a non-obvious warfare technique if the probability of ascription for each attack is nonzero and the probability of ascribing one event is at least somewhat independent of the probability of ascribing another. This rules out space warfare, electronic warfare, drones, and special operations. It may also rule out cyber warfare but is less likely to rule out proxy warfare—where attribution has to be inferred rather than discovered—and intelligence support to warfare.

So what *can* be done with non-obvious warfare? One use is general coercion or dissuasion. Instead of signaling, "if you do this we will do that," the signal is, "if you do this then bad things will happen to you." Because the act of signaling itself may implicate the attacker, it helps if the signals come from someone else. Others may be willing to help if there are multiple states with a common interest, such as Vietnam, Indonesia, and the Philippines all opposing Chinese bumptiousness in the South China Sea. These others may also be co-religionists or co-ideologues (e.g., "disrespect our religion and bad things happen to you"). The use of non-obvious warfare for compellance is trickier to pull off insofar as it is easier for disparate entities to agree on what can be condemned than to agree on what should be done.

Another fairly obvious use is sabotage, à la Stuxnet, carried out to deny its target some capability. The difficulty is that sabotage is rather pointless unless it takes place on a very large scale or is somehow associated with an operation (if it is a combat operation, the target might assume that the saboteurs work for the combatants). Even if the damage is permanent, states can generally recover. The attack on the Iranian centrifuges made sense because of the strong desire felt by some countries to hobble Iran's nuclear program and buy time. Another rationale for sabotage is to push a target past a nearby tipping point, even if this tends to be visible only in retrospect. Otherwise, the consequences of carrying out what could be an act of war may outweigh the gains, even if getting caught is unlikely.

An untraceable attack of sufficient magnitude may also weaken the target prefatory to an armed attack or at least so distract the target that it cannot assign the resources, such as sensors, in-place weapons, or management attention, required to foresee and prepare for what turns out to be

an imminent overt attack. Clearly, if an attack does come, the precursor will cease being a non-obvious attack in retrospect (unless the target has multiple eager enemies, each looking for signs of weakness, in which case, what looks obvious may still be wrong). The advantages of starting in a non-obvious mode are twofold. First, if the initial attack were obvious the target might countermove in ways that would make the attack harder to pull off. It may know where to point its defenses, so to speak; it could rally others to pressure the attacker; or it could even counterattack. Second, if the attack falls short of its objectives, the attacker may cancel the overt attack and remain obscure in hopes of eluding punishment.

Correspondingly, a non-obvious attack may be a test to see if the particular technique works, what the target's defenses are, and where improvements should be sought. It would be an expensive test if the target itself should learn something about its vulnerabilities and thereby have cause to work them and evidence on how to do so.

Non-obvious operations can also help win the wars of third parties. Such help can be non-obvious either if the *fact* of help is not obvious or if the *source* of help could be any of several countries or entities such as insurgent or mercenary groups. This raises the question of why such a state would want not to leave fingerprints. One reason is that the attacks take place in a country other than the one that wanted help (e.g., Syria attacks Iraq, and the United States attacks targets in Syria), thereby becoming an act of war in its own right and an excuse for the attacked country to call on *its* friends to help (e.g., attack Iraq). More likely, however, the assistance supports operations within the state under attack, either by another state or by insurgents, so these factors do not come into play. What *does* matter, however, is the appearance of commitment and how it prevents assuming a commitment to pursue victory or lose face. Intervening and then withdrawing prematurely raises doubts about the state's seriousness of purpose and even trustworthiness, even if such a state never made an explicit commitment to stay the course.

Non-obvious warfare can also be carried out for narrative effect. Normally, in warfare the attacker and the target are both part of the narrative, and unless the attacker's actions are totally baseless, the contest over narratives is likely to be two-handed with each side's fans supporting their own side. However, if the attacker is unknown, or at least unclear, then the focus of the story is necessarily on the target, and the theme is likely to focus on why the target was attacked—and may well dwell on what the target did

that merited the attack or why the target could not secure itself. That, in fact, may be the attacker's motive: to create a crisis of confidence in the target state, either weakening it outright, creating fissures in its body politic, or at least making it more amenable to concession.

Finally, if an attacker can persuade the target that it was hit by a third party, it may catalyze conflict that will be to the attacker's advantage. A non-obvious Taiwanese cyber attack on the United States during a crisis with China, for instance, might put the United States at odds with China and thus more likely to support Taiwan. An attacker that instigates a war between two former trading partners could force both to purchase from the remaining relevant neutral, the attacker. Of course, if attribution follows, the attacker will have made one enemy it did not need and perhaps a second enemy as well—the country that the attacker hoped would be fingered.

The Target's Response Options

In some cases, ambiguity works to the target's advantage by giving it an excuse to avoid responding; it can claim uncertainty about who perpetrated the attack or what, in fact, was done. Not knowing helps the targeted nation ward off popular calls to fight and redeem its honor. In some cases the attacker itself may not necessarily think the worse of the target's honor if no response ensues; in other cases, it will convince itself the target knew but was lying to avoid a confrontation. Consider, analogously, the phantom Israeli nuclear arsenal. Once other powerful Middle Eastern states acknowledge that Israel has nuclear arms, they must answer as to why they do not. No polity is fooled, but neither must it be taunted by the prospect.

Mostly, though, targets would simply want such attacks to stop—but how? Defense is clearly an option and one that would logically assume greater importance the less it can lean on not hitting back because it is unsure about who committed the offense. Another option is to help create pressure from the world community to end the possession of the requisite attack technology, but most of these cannot be effectively banned. Cyber weapons are largely the obverse of system vulnerabilities, the attack code is trivial to hide, and the underlying technologies of offense are required for cyber defense. Electronic jamming is inherent in the ability to generate radio frequency energy. Intelligence support for third parties is identical

to intelligence support for military operations in general. The weapons of sabotage, special operations, and insurgencies are small arms. Conversely, weapons of mass destruction and land mines (but not naval mines) are already banned by treaty. The only weapons not covered by treaties that could conceivably be banned are antisatellite weapons and drones; both have legitimate (overt) military purposes. More broadly, it is how such weapons are used rather than the weapons themselves that determines the characteristics of non-obvious warfare.

A variant on the second approach is to develop a global consensus that the covert use of warfare is far more heinous than its overt use. Thus, if such weapons *are* used—something that may not always be apparent—the world community would support efforts to pressure potential users into allowing investigations that would clarify which state was at fault. After all, most forms of warfare are universally held to be crimes if carried out by those outside the military; thus, even the accused state should have an interest in finding and rooting out its dangerous criminals, assuming it would wish to shift the blame. Where states use proxies and such acts *are* crimes, they may be pressured to cooperate with international police investigations. Satisfaction for the aggrieved party, however, assumes police actions can establish reasonable levels of certainty. More problematically, the closer the trail of investigation comes to the doors of military or intelligence establishments, the greater the reluctance of states to allow matters to proceed. Such reluctance would not be unfounded—if purported acts of non-obvious warfare allow investigators to peer into covert operations, states may go to great lengths to interpret the need for evidence in ways that would also allow them to uncover the secrets of their rivals.

The last recourse is for victimized states and their allies to respond to suspected warring states as if certain they did it. In doing so, they must factor in how certain *others* are that the accusation is correct and, to some extent, whether the purported attacking state believes it is guilty. Many non-obvious warfare techniques can be carried out by rogue elements. As noted, some responses, such as chilling relations between the target and the purported attacker, do not require anything close to conclusive proof; mere uneasiness suffices. Other responses, such as retaliation, normally require high levels of confidence. In the end, the victimized state has to weigh the risks associated with false negatives (doing nothing in the face of aggression) and false positives (retaliating against the innocent). Note further that "plausible deniability" is hardly an absolute in this case. Unless the

victimized state can only respond through the court system—and states cannot go on trial, only their leaders—the balance between responding and not responding may tip well before the confidence meter hits 100 percent. A relatively pacifist state surrounded on all sides by friends (e.g., Belgium) and embraced by alliances may want near certainty and may not react even then; an anxious, well-armed state surrounded on all sides by potential adversaries (e.g., Israel) may be less fussy.

Or the victim could retaliate by using non-obvious warfare itself. Ostensibly, the mutual commitment of both sides to modulate their responses to one another might limit the potential for open and, hence, more destructive warfare—as long as both sides are careful not to reveal themselves. This may create a set of strange incentives wherein both sides' non-obvious warfare communities take pains not to reveal the activities of their counterparts lest power and influence on both sides shift to communities whose warfare methods are quite obvious. Conversely, the perception that it is acceptable to escalate in a non-obvious manner rather than call out the other side may allow the destructive cost of non-obvious warfare to rise to its limits. If matters then become obvious, the warfare level that forms the foundation for the next set of threats starts at the much higher level.

Assessment and Conclusions

Would the spread of non-obvious warfare be a good thing? Even if wielded solely in pursuit of good aims, such techniques corrode both military values and diplomatic norms. Non-obvious warfare, almost by definition, has to be the work of small teams that must isolate themselves from the larger community, much like intelligence operatives, lest word of their adventures leak out. The efforts of the small non-obvious warfare teams would leave the mass of the national security establishment quite uncertain about what exactly was going on and who exactly was behind all the activity (only some of which would appear to be accidental).

Non-obvious warfare is also a poor fit for democratic states and a far better fit for authoritarian or failing states in which the intelligence community has become decoupled from its legitimate governance structure. States with long-term reputations to manage are likely to see the downside from having to lie about their warfare activities when so confronted.

Universal or even wide adoption of non-obvious warfare would likely yield a more suspicious world. Once attacks are shaped to look like accidents,

many accidents will start to smell like attacks. Nations would react (even more than they do now) to suspicions rather than actual substance; attackers might be credited/blamed for far more than they actually merit. In too many countries, *anything* that seems askew is blamed on the United States (or Israel) and their ubiquitous and omnipotent intelligence agencies. Part of their polities' maturity entails improvements in their ability to distinguish fact from fantasy; evidence that such fantasy had a kernel of truth behind it would hardly facilitate the maturation process. Indeed, under crisis circumstances, it is conceivable a conflict could start even though the accused did nothing. And of course, a crisis could start when a state used such techniques thinking it would never be caught—and was.

Notes

1. The term *non-obvious* had an earlier manifestation in Jeff Jonas's data-mining product, Non-Obvious Relationship Analysis.

2. *Warfare*, used here, comprises operations carried out for political ends by states aimed at the destruction, corruption, or significant disruption of assets or interests associated with other states using means that are generally considered illegal if not done by states. Our discussion is limited to states, because nonstate actors do not always have return addresses or even always unambiguous identities, and individuals therein can be subject to legal actions in ways that states cannot be.

3. Sergei Markov, a state Duma deputy from the pro-Kremlin Unified Russia Party, claimed, "About the cyberattack on Estonia . . . don't worry, that attack was carried out by my assistant. I won't tell you his name, because then he might not be able to get visas." "Behind the Estonia Cyberattacks," *Radio Free Europe/Radio Liberty*, 6 March 2009, http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.

4. Robert Mackey, "Irish Flotilla Activists Show Damage to their Boat," *The Lede: Blogging the News*, 1 July 2011, http://thelede.blogs.nytimes.com/2011/07/01/what-flotilla-activists-videos-look-like/.

5. Which came to near naught after the original ranks were greatly reduced in the 1968 Tet offensive.