The Strategic Uses of Ambiguity in Cyberspace

Martin C. Libicki

Strategic ambiguity has an honored place in the mores of statecraft. The studied unwillingness of states to say what they have done (or would do) coupled with the lack of proof that they have done it (or would do it) liberates other states. They can argue that something was done, but if their purposes so dictate, they can pretend that it was not done. The degree of doubt can vary: from thorough (no one is sure what has happened or would happen) to nominal (no one is fooled). In either case, however, those who did it have provided a fig leaf, however translucent, that other states can adopt.

Examples of Strategic Ambiguity in Physical Space

One time-honored example is Israel's refusal to admit (or deny) that it has nuclear weapons. No reputable analyst believes that Israel does not have nuclear weapons. But since Israel has never announced whether it has any, other states are free to pretend that Israel has not crossed the nuclear barrier. This is convenient for states that would be pressured by their people to respond with nuclear programs of their own were Israel's status overt. It also helps states that could not ship certain classes of exports to Israel were Israel's status more open.[1] At the same time, no sane country behaves as if Israel lacked a nuclear retaliation capability.

A parallel ambiguity concerns the putative US use of Predator attack flights and cruise missiles against al-Qaeda members in countries such as Yemen or Pakistan. Official policy is to deny that such flights take place. When Yemen's leader claimed that these were Yemenite operations, very few analysts were fooled. But at least until recently, the leaders of

Dr. Martin C. Libicki is a Senior Management Scientist at the RAND Corporation.

these countries did not have to contend with admitting that sovereignty violations were taking place, with at least their tacit permission.

Another longstanding example is US policy towards Taiwan's independence. The United States has declared both that it opposes a Taiwanese declaration of independence and any attempt to resolve the status of Taiwan by force. The United States does not recognize Taiwan as a state and so has no mutual aid pact with it. However, if Taiwan declared independence and China decided to take the island, would the United States intervene on Taiwan's side? It is clearly in the US interest for China to think so in order that China does not start a war. But it is almost as clearly in the US interest for Taiwan to think otherwise, so that Taiwan does not provoke China into starting a war. Assume the odds of a US intervention are literally a coin toss and perceived that way on both sides of the Straits. If so, Taiwan may well calculate that the expected value from declaring independence is negative (whereas it would have been positive if the US were definitely coming to help), due to the fact that the United States might decide not to intervene. Similarly, China could conclude that the expected value of a cross-Straits invasion is also negative because the United States might intervent. Anything less ambiguous could well prompt one or the other to do something foolish.

Cyberspace is Tailor-Made for Ambiguity

Cyberwar is, literally, inside work. When hackers enter a computer system to misdirect its workings, the direct results are often literally invisible to the outside world. Depending on how such systems have been misdirected, the indirect results may be invisible as well. True, the results of a cyber attack on a power grid that turns off the lights can be viewed even from space. But without further investigation and revelation, it will not be clear whether a blackout was a deliberate attack, or the result of human error, bad software, or (most frequently) Mother Nature. Even if it were clear that a system misbehaved because it had been attacked, exactly who attacked may be shrouded in mystery. Finally, even if the fact and the author of the cyber attack were clear, the purpose may be quite obscure: after all, cyberwar alone cannot kill anyone, or even break very much (but see Stuxnet), much less seize territory or change a regime (and whereas cyberwar can facilitate other applications of force, it is those other applications that are more visible). Nearly all intrusions are meant to steal information or "rent" the capacities of the target machine (as in a bot) and otherwise leave the

system alone. Deliberate attacks can often be framed as attempts to mislead people (e.g., false radar images) or their equipment (see Stuxnet). In the latter cases, obviousness is self-defeating; once it is clear that you have successfully deceived a system, the system's administrators are unlikely to allow the system to operate as it has.

Is Stuxnet an Exception?

One would imagine that a cyber attack that actually broke something might have passed the point where everyone could be try to hide its existence. The Stuxnet worm was discovered in June, 2010, and its target was identified as an Iranian nuclear facility in September. The earliest suspicions tagged the Bushehr reactor as its target,[2] and the Iranians denied that any such reactor was affected. Within a few weeks, the Natanz centrifuge plant was identified (more plausibly) as its target. Initial Iranian denials were contradicted in late November, 2010, the day that assassins killed two Iranian nuclear scientists, and when Ahmadinejad admitted that there was a worm that had caused a great deal of trouble, which was then taken care of.[3] How badly did Stuxnet, in fact, hurt Iran's nuclear development? Statistics from the IAEA would indicate that it may have led to the premature retirement of 10 percent of Iran's centrifuges and thus, at most, it bought the worm's creators several months reprieve from the data at which Iran would have enough nuclear material to build its first bomb.[4] Other reports quote officials predicting that the earliest that Iran can (as of early 2011) assemble such material would be 2015, a delay of several years.

There is a lot more (apart from what it accomplished) that is currently unclear about Stuxnet.[5] One question is how it got into Natanz in the first place; suspicions that the worm's designers received witting or unwitting help from Russian contractors appears to have soured Iran's working relationship with them.[6] More important is exactly who wrote and released the worm. Was it an individual (its sophistication says otherwise)? Was it Israelis – as suggested by several clues internal to the code – but who knows that these clues were not planted to mislead suspicion? Was it Americans? Was it both, working together?[7] Or, was it the Chinese?[8] With all the ambiguity, it is no wonder that Iran has yet to retaliate (at least in any noticeable way). That noted, Syria did not respond to the strike on its suspected nuclear facility, and Iraq did nothing but complain when its Osiraq reactor was bombed – and there was no ambiguity who did it in both cases. Conversely, Iran's strong ties to Hamas and Hizbollah suggest that

it may have had ways of expressing its displeasure that were unavailable to Syria (in 2007) or Iraq (in 1981). Furthermore, Iran has yet to make much of a big deal about the incident; likening it to an act of war after months of silence and denials would be quite a volte-face.

The advantages of using Stuxnet rather than airpower to degrade Iran's nuclear capability are fairly clear (assuming the worm, in fact, did as its designers hoped): comparable effect, and induced distrust among its victims as to which of its suppliers or supplies may still be contaminated, but with less condemnation (indeed, perhaps a sneaking admiration) and fewer strategic risks.

The Uses of Ambiguity

The working hypothesis is that a cyber attack used in lieu of kinetic methods creates more ambiguity in terms of effects, sources, and motives. Thus, if cyber attacks work – and this is a tremendous if – they change the risk profile of certain actions, and usually in ways that make them more attractive options. What follows are some hypothetical uses of cyber attacks.

One, cyber attacks may be used by a victim of small scale aggression to indicate its displeasure but with less risk of escalation than a physical response would entail. In late 2010, for instance, North Korean forces shelled a South Korean island, killing two civilians and two service members. A retaliatory cyber attack that disrupted an important industrial facility (ignoring the fact that North Korea is not well digitized and has nearly zero network connections to the rest of the world) could have conveyed displeasure. North Korea, if it wanted to respond, would have had to (1) admit that one of its facilities had been hacked, and (2) take steps to indicate why it was South Korea, and only South Korea that was at fault (it could be the United States or even Japan, and China). Conversely, if North Korea did not react publicly, it stood a good chance of limiting the number of people with a good idea of why some facility ceased working. This introduces another advantage of cyber warfare over physical combat: although being attacked may be a source of pride (e.g., you can play David to the enemy's Goliath), being hacked primarily means that you ventured into cyberspace with inadequate attention to maintaining control over your systems. Victimhood is not something worth boasting about. Thus, states that can hide having been attacked may well do so, thereby saving face – but doing so also making an obvious response less likely. They could,

of course, respond in kind and so a tit-for-tat struggle that started in the physical worlds ascends (or descends) into the virtual one. But that course may be safer all around than coming to blows.

Two, a state rich in cyber warriors may also use the threat of cyberwar to deter the potential target against support proxy war fighters: e.g., Israel could threaten Iran with cyber attacks if Israel is attacked by Hizbollah, a group with known links to Iran.[9] In this situation, Israel may not want to make such a threat public. A public threat would allow Hizbollah to coerce Iran by claiming a desire to wreak the sort of mischief that would prompt Israel to strike Iran in cyberspace. But there are private ways to convey the threat, and such a threat has logic. The usual problem with cyber deterrence is that attribution (of the starting attack) is a problem, but a physical attack – say, Hizbollah rockets striking Israel – would be obvious. Conversely, although a state like Iran may not fear a direct Israeli attack even in response to a Hizbollah attack (no such attack materialized in 2006, for instance), it may fear a cyber attack given the clear superiority of Israeli hackers over Iranian ones. Such superiority mitigates (although it does not erase) the fear that having declared the intention to carry out a cyber attack, Israel would have no accessible targets in Iran; even if the success of any one attack is uncertain, the odds that enough will succeed and hurt are sufficiently good. Iran's blaming the United States afterwards may be a problem for the United States but make things easier for Israel. Escalation into violence is not really an option for Iran given Israel's conventional combat dominance (at least if the battle were close to Israel). More to the point, Iran would have to admit its systems had been conned and make a convincing case that it knew who did it. Finally, while Israel is more wired than Iran, again, with Israel's cyber capabilities, that fact may not be enough to turn the tide towards Iran's favor should it strike back.

Three, cyber attacks can be used by one state to affect the outcome of conflict in another state without having to make any sort of visible commitment, even an implied one. Consider the civil war in Libya. If Libya's military was sufficiently wired so that cyber attacks could conceivably make a difference in its capabilities,[10] then Western hackers, by disabling the central government's forces, could conceivably tilt the direction of the fight. If the rebels won, Western governments would be better off as a result. Rebel forces, at worst, would have no way of knowing they had received assistance, and that may be just as well (particularly regarding

the more jihadist of Libya's rebels who greet the intervention of US forces by switching sides). Or, hints could be offered (e.g.: if this capability fails tomorrow, you will know why). Conversely, if the government won, it may suspect that its information systems were tampered with by Western forces, but it may not be able to prove as much. It may complain, but if Libya were expected to blame its shortfalls on the West, then such complaints, in the absence of evidence, would have little force. More to the point, it may not want to claim as much if it wants to pretend afterwards that it has no reason to make enemies of the West all over again. If the civil war drags on, the West can pretend that it had made no prior help and thus had made no commitment to escalate its assistance (even if hints were dropped to the rebels, they would have an even harder time proving to others that Western hackers were offering assistance, since unlike the government, they would likely have no access to the tampered computers). The greatest problem in offering such assistance is the possibility of getting caught, but if the target of the attacks is on the outs with the rest of the world, it is unlikely that it will get much help tracing the attacks. So attractive is such assistance (at least from the helper's perspective) that it may be a routine feature – on both sides – of any conflict where the outcome is uncertain and networks matter to war fighting capabilities. And again, admitting that one's systems have been hacked is always at least a little embarrassing.

Four, cyber attacks do not need to be directed towards adversaries, although the risks of making new enemies if the source of the cyber attacks are discovered are obvious. Consider a situation in which two neutral states are inching towards war that one might prefer not take place. Suppose that a third state is capable of introducing faults into both sides' surveillance and/or command-and-control systems that raise doubts whether they have pierced the fog and overcome the friction enough to undertake military operations. If systems go haywire, either target state is more initially likely to blame the other for its woes (if they understand that such woes were obvious *and* induced rather than non-obvious or accidental) rather than a third party; chances are that the initial presumption is likely to color their forensic activities and conclusions. Furthermore, there is a good chance that such blame will be kept private given the embarrassment involved. Yet risks exist in such maneuvers; such machinations may drive states towards war if one side or both comes to convince itself, for instance, that the cyber attacks from the other side are precursors to an immediate movement of forces, or are indications that their foes' forces are not just posturing.

A variant on this technique is to use cyber attacks to disable a capability in a state whose leadership is reluctant to use it anyway (either because the leadership feels itself to be on shaky political ground vis-à-vis its excitable populace, or because the leadership is exercised by a consensus among factions[11]). Once such a capability is found inoperative, the political leadership announces to its military leaders that it has no option but to stand down. Perhaps the military unearths evidence that a third party was behind such an incapacity – the political leadership, relieved at not having to act, may deem such evidence inconclusive or not credible it in the first place.

Five, ambiguity may be useful in declaratory policy, one that indicates how a state would respond to a cyber attack. Ambiguity has both costs and benefits. The cost is that others may think they can get away with attacks that they would have forborne if they had understood that reprisals would follow. But the benefit is that the target state may not want to strike back, particularly if it lacks the confidence to attribute the attack. A state that fails to strike back because it is unsure may not lose stature in its own eyes – attribution really is difficult. Yet if the attacker (and others) come to believe that such a state *did* know but pretended otherwise for fear of a full-scale fight, then any threat to retaliate rings hollow – and not just in cyberspace. If a state leans too far forward in promising reprisals in response to cyber attacks and cannot deliver, its ability to deliver against all other threats may be further doubted.

Conclusion

Cyberwar's many tactical ambiguities lend force to a strategy built on strategic ambiguities. There may be many cases in which an aggressor state does not want what it has done it to be obvious. Even the target state in some cases may conclude that pretending as much (even if it must turn a blind eye to the evidence) has advantages over trying to clarify matters or even claiming clarity in absence of the real thing.

But the downside to strategic ambiguity should be noted. States may arrogate the right to carry out all sorts of mischief in cyberspace on the belief that they will never be called into account. The lack of accountability, however, is inherently dangerous. Sometimes it is unwarranted (the state is only fooling itself), and even if warranted, it provides hackers a degree of freedom that history suggests is dangerous in and of itself.

Notes

1 By contrast, legislation had to be passed in 2006 to permit the United States to share civilian technology with India, which like Israel is a non-signatory to the Non-Proliferation Treaty, but unlike Israel, a declared nuclear power. See Peter Baker, "Signs India Nuclear Law: Critics Say Deal to Share Civilian Technology Could Spark Arms Race," *Washington Post*, December 19, 2006, www.washingtonpost.com/wp-dyn/content/article/2006/12/18/AR2006121800233.html.

2 Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?" IDG News, taken from *PCWorld*, September 21, 2010.

3 William Yong, Alan Cowell, "Bomb Kills Iranian Nuclear Scientist," *New York Times*, November 30, 2010.

4 Joby Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack," *Washington Post,* February 16, 2011. See also the report by the Institute for Science and International Security, http://media.washingtonpost.com/wp-srv/world/documents/stuxnet_update_15Feb2011.pdf.

5 What *is* most clear about Stuxnet is how it worked because the worm was captured alive, so to speak, in the wild before it could self-destruct (which it should have done if it was unable to find a specific programmable logic device that met certain preset parameters associated with a particular type of centrifuge).

6 "The Stuxnet Worm: A Cyber-Missile Aimed at Iran?" *Economist*, September 24, 2010, www.economist.com/blogs/babbage/2010/09/stuxnet_worm.

7 William Broad, John Markoff, David Sanger, "Israel Tests on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

8 Jeffrey Carr, "Stuxnet's Finnish-Chinese Connection," December 14, 2010, blogs.forbes.com/firewall/2010/12/14/stuxnets-finnish-chinese-connection/.

9 Many observers take issue with the characterization of Hizbollah as a puppet of Iran. Yet there is a difference between Hizbollah acting only on Iran's orders, and Iran having enough influence on Hizbollah to discourage it from unwise actions.

10 An influential article reviewing the possibilities of Western intervention in Libya mentioned electronic warfare in the form of communications jamming, but nothing about cyber warfare. See Thom Shanker, "U.S. Weighs Options, on Air and Sea," *New York Times*, March 6, 2011, http://www.nytimes.com/2011/03/07/world/middleeast/07military.html.

11 If the fact that China's stealth fighter surprised Hu Jintao when meeting with Secretary of Defense Gates is any indication, its military is not absolutely beholden to its political leadership and thus the country's effective leadership may also be somewhat of a coalition.