The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis.

This electronic document was made available from www.rand.org as a public service of the RAND Corporation.

Skip all front matter: Jump to Page 1 ▼

Support RAND

Browse Reports & Bookstore
Make a charitable contribution

For More Information

Visit RAND at www.rand.org
Explore the RAND National Defense Research Institute
View document details

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND electronic documents to a non-RAND website is prohibited. RAND electronic documents are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see RAND Permissions.
This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.
Brandishing Cyberattack Capabilities

Martin C. Libicki
The research described in this report was prepared for the Office of the Secretary of Defense (OSD). The research was conducted within the RAND National Defense Research Institute, a federally funded research and development center sponsored by OSD, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community under Contract W74V8H-06-C-0002.

The RAND Corporation is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND’s publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2013 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND website is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (http://www.rand.org/publications/permissions.html).

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org
Summary

Background and Purpose

The U.S. military exists not just to fight and win wars but also to deter them, that is, to persuade others not to start them (or even prepare for them). Deterrence is possible only when others know or at least have good indications of what the U.S. military can do. Such acknowledgment is at the heart of U.S. nuclear deterrence strategy and, to a lesser extent, the U.S. maintaining strong mobile conventional forces that can intervene almost anywhere on the globe.

Cyberattack capabilities resist such demonstration. No one knows exactly or even approximately what would happen if a country suffered a full-fledged cyberattack, despite the plethora of hostile activity in cyberspace. For one thing, there has never been a cyberwar—attacks with destruction and casualties comparable to physical war. Theory also works against demonstration. Flaws in target systems enable cyberattacks. To reveal which flaws enable attack is to inform others how to fix the flaws and hence neutralize them. It is no wonder that national cyberwar capabilities are a closely guarded secret.

That cyberattack capabilities cannot easily be used to shape the behavior of others does not mean they cannot be used at all. This report explores ways that cyberattack capabilities can be “brandished” and the circumstances under which some deterrence effect can be achieved.\(^1\) It then goes on to examine the obstacles to realizing such achievement and sketches out some realistic limits on the expectations.

As a matter of policy, the United States has never said that it would use cyberattacks, but neither has it said that it would not. It has also not vigorously disputed the notion that it had some hand in the Stuxnet attacks on the Iranian nuclear facility.

The Broad Effects of Brandishing Cyber Capabilities

Any state that would discourage other states from aggression in the physical or cyber world by brandishing cyberattack capabilities should first ask itself whether the point of doing so is to look powerful or to make others look powerless. Although both aims are useful, the need to concentrate on one message in a strategic communications campaign suggests the usefulness of making a choice. Emphasizing one’s power has the advantage of inducing caution in all actual or potential opponents and deflects predators to easier prey. It may also reflect well on other

\(^1\) Note that the usage of *brandishing* here is intended to invoke the imagery of warriors displaying their weapons (and hence their capabilities) before battle, by way of warning, rather than that of a criminal displaying a gun to threaten a victim.
sources of national power. But trumpeting the weaknesses of others deters troublesome states by reminding them of their vulnerabilities. It also deflects the accusations of self-promotion by turning the focus toward potential victims.

A bigger challenge is how to demonstrate cyberwar capabilities. The most obvious way to demonstrate the ability to hack into an enemy’s system is to actually do it, leave a calling card, and hope it is passed forward to national decisionmakers. If the attack can be repeated at will or if the penetration can be made persistent, the target will be forced to believe in the attacker’s ability to pop into his system at any time. This should force the target to recalculate its correlation of forces against the attacker.

But as with many things in cyberspace, it sounds simpler than it is. Hinting at outright success is difficult without conceding one’s participation in mischief in the first place and hence cyberwar’s legitimacy as a tool of statecraft, something countries only started acknowledging in mid-2012. Targets of little value tend to be easy, but penetrating them is unimpressive. Targets of some value are, for that reason, much harder, often because they are electronically isolated. Finally, the ability to penetrate a system does not necessarily prove the ability to break a system. The latter requires not only breaking into sufficiently privileged levels but also figuring out how to induce a system to fail and keep on failing. But penetration may be sufficiently scary in itself if the target leadership cannot discern the difference between breaking into and breaking.

Breaking a system is more hostile and more difficult than breaking into one. It requires an understanding of what makes the system fail. Getting the desired results also requires shaping the attack so that those who administer the system cannot detect the attack and repair the damage quickly. Conveying to others the ability to bring their systems down and keep them down is not easy. Intended audiences of such demonstrations may subsequently identify the flaw that would allow such an attack and fix it. If so, for brandishing to work, cyberattack capabilities may require repeated demonstration. Alternatively, a less hostile demonstration could be to manipulate the system but not to the point of harming it, a fine line.

Can brandishing help dissuade other states from pursuing a network-centric high-technology force to counter U.S. military capabilities? The best way to demonstrate the risk of network-centricity is to hack into military systems to show their fragility (claiming responsibility is unnecessary; the point is to emphasize not U.S. power but the vulnerability of the enemy’s network-centric systems). In other circumstances, making what is vulnerable clear may be unnecessary, perhaps unwise. Every hack leads to fixes that make the next exploitation much harder. But the hint of an attack that leaves no specific trace leaves nothing specific to fix. The point is to convince others that they cannot protect their systems even after paying close attention to their security. The vulnerability of less sophisticated states to unseen manipulation may be higher when the target does not really understand the technology behind its own weapon systems. Often, the target’s lack of access to others’ source code and not having built any of its own complicates figuring out what went wrong and how to fix it.

Not all states will throw up their hands, though. Some may reason that, because the effects of cyberattacks are temporary and difficult, their systems can survive the initial exchange and recover for subsequent rounds. So, they pursue high technology and ignore the demonstrated possibility that high-technology military campaigns might last days rather than months or years. A subtler counterstrategy is to network warfighting machines (configured not to touch the Internet) and forget about networking people; isolation avoids some of the pesky vulnerabilities arising from human error (notably those associated with authentication, such as pass-
words and tokens). Or they simply renounce network-centric warfare and conclude that they avoided the pitfalls of depending on technology.

It is unclear whether brandishing cyberattack capabilities can curb the enthusiasm of potential foes for war. Some states may feel they have little choice. Others may feel that they can succeed even if their high-technology systems fail. Yet others may discount the possibility entirely, believing their systems—when called on for war—would be disconnected from the rest of the world. Last, the target may simply not believe its own vulnerability, not during peacetime and certainly not when the war drums sound. Going to war requires surmounting a great many fears; digital ghosts may simply be another.

The unwanted effects of making even some third parties believe that we have invaded their systems warrants note. All other militaries may also shy away from foreign sources for logic-processing devices (whether software or hardware) and may redouble their efforts to increase their indigenous production capability or, alternatively, pressure their suppliers to hand over source code with their systems, a negative if their supplier is a U.S. corporation. The problem does not go away if the threat turns out not to work. Countries certain that their military systems have been invaded may blame the United States for any military failures even with no evidence of U.S. involvement. Conversely, the United States may be accused of complicity with a rogue state whenever its equipment does not fail because this could only mean that the United States condoned the rogue’s actions.

**Brandishing Cyberattack Capabilities in a Nuclear Confrontation**

Are there circumstances in which the United States might usefully hint that it could interfere with a rogue state’s nuclear weapons and thereby defuse a nuclear confrontation? Posit a rogue state with dozens of weapons capable of hurting neighbors but not the United States. Assume further the United States has a robust cyberwar capability from which the rogue state’s nuclear arsenal is not provably immune. To the extent that the rogue state is far more willing to go to the brink than the United States is, it may not be completely deterred by the U.S. promise of a devastating reaction to its nuclear use. The rogue nuclear state, we further posit, threatens that, if the United States crosses its “red line,” it could or would respond with a nuclear shot.

We first model a two-state confrontation and then introduce a friendly third state on whose behalf the United States is acting.

The question is, which is more implacable: the United States determined to cross the red line or the rogue state equally determined to respond with nuclear weapons? If one side can communicate enough confidence in its willingness to keep pressing, the other side may feel that the first side will not back down and would thus logically recognize that the choice is between yielding and catastrophe. The more that the other side indicates it might yield, the greater the impetus for the first side to stand firm, making it seem even more implacable to the other side.

The purpose of brandishing a cyberwar weapon is to threaten the other side’s ability use its nuclear capability in a crisis. This purpose is less to make the other side doubt its own nuclear capability—although that can help—but to project a belief that the United States will press on either because the rogue state’s weapons will not work or because the rogue state will respond to the brandisher’s confidence (underwritten, of course, by its deterrence capability) and back down. Note that the logic works even if the target state believes that the brandisher’s
confidence has no basis in reality (i.e., its own nuclear command and control is rock solid). The rogue state needs only to believe that the brandisher believes it can act with impunity to conclude that the choice is between disaster and backing down. To be sure, because a cyberwar capability cannot be tested in the same way that an antismissile capability can be tested, the rogue state may conclude that the brandisher's confidence is unwarranted and therefore that such confidence should not exist and hence does not exist. But that could also be wishful thinking on the rogue state's part.

If brandishing a cyberthreat created a use-it-or-lose-it dilemma for the rogue state leading to nuclear use, brandishing could backfire on the United States. But it should not, largely because it is not a threat of what will happen but what has already happened: The flaw has already been exploited. However, brandishing a cyberwar capability, particularly if specific, makes it harder to use such a capability because brandishing is likely to persuade the target to redouble its efforts either to find or route around the exploited flaw (the one that enabled the United States to neutralize its nuclear threat). Brandishing capabilities sacrifices the ability to manage a war in exchange for the ability to manage a crisis.

One possible component of the brandishing process is to convey that a nuclear shot that failed will be noticed—and responded to—even if the failure would be invisible to outside observers. Otherwise, the rogue state may reason that failure is costless and that success, while potentially very costly, at least demonstrates that the rogue state is serious. But if the induced failure is not obvious (e.g., the button is pushed and nothing happens), can the United States retaliate against an attempted action that only the United States saw?

Once third parties are in a position to veto U.S. military actions, they can complicate the use of brandishing. Although third parties may have greater animus against the nuclear-armed state and, correspondingly, a greater willingness to see it humiliated, and certainly deterred, they may well blanch at the cyberwar-backed bluff. First, they and their citizens are likely to be at greater risk by dint of sitting within range of the rogue state's nuclear weapons. Second, they would know little about U.S. cyberwar capabilities and may thus have less confidence that such capabilities would work than the United States (supposedly) has. The rogue state may figure that it need not stare down the United States if it can scare the third party whose concurrence is needed for U.S. actions.

The United States may need options to convince the third party that it can stand fast because, among other things, its cyberwar capabilities will neutralize the nuclear threat. It could say, “trust me on this” or else. But a U.S. response that goes beyond asking for trust may have to reveal much more about the details of U.S. cyberwar capabilities than the United States seems comfortable doing today. A crisis makes revelation problematic: Even though steadfastness requires pro-U.S. forces to project faith in the U.S. ability to nullify a nuclear threat, those nervous of taking such a huge risk, skeptics of cyberwar’s power, or opponents of the United States within the government have every incentive to cast doubt on the proposition or even leak the information entrusted to them. (Incidentally, a similar logic applies if the friendly third party is domestic, such as the U.S. Congress, opinion makers, and the public.) It may be to the rogue state's advantage to imply that cyberwar capabilities (rather than the confidence in the deterrence effect of its nuclear weapons) are the primary basis for the firm stance the United States has adopted. This could pressure the United States to demonstrate what it can do.
Conclusions

Brandishing a cyberattack capability would do three things: declare a capability, suggest the possibility of its use in a particular circumstance, and indicate that such use would really hurt. In the era of the U.S.-Soviet nuclear standoff, the suggestion of use was the most relevant. Possession was obvious, and its consequences were well understood. The same does not hold true for cyberweapons. Possession is likely not obvious, and the ability to inflict serious harm is debatable. Even if demonstrated, what worked yesterday may not work today. But difficult does not mean impossible.

Advertising cyberwar capabilities may be helpful. It may back up a deterrence strategy. It might dissuade other states from conventional mischief or even from investing in mischief-making capabilities. It may reduce the other side’s confidence in the reliability of its information, command and control, or weapon systems. In a nuclear confrontation, it may help build the edge that persuades other states that the brandisher will stay the course, thereby persuading them to yield.

Yet proving such capability is not easy, even if it exists. Cyber capabilities exist only in relationship to a specific target, which must be scoped to be understood. Cyber warriors can illustrate their ability to penetrate systems, but penetration is not the same as getting them to fail in useful ways. Since cyberattacks are essentially single-use weapons, they are diminished in the showing. It can be hard to persuade your friends that you have such capabilities when skepticism is in their interest.

Furthermore, brandishing may backfire. Touting an ability to strike back in cyberspace may communicate a tendency to shy from violence. Claiming the power to alter reality may convince others to blame the claimant when reality is disagreeable. Interfering with others’ command and control may allow them to justify rules of engagement that abdicate their own responsibility over subordinates. And asserting an ability to nullify opposing nuclear systems may spur them to call what they perceive as a bluff.

Should the United States put the world on notice that it has cyber capabilities and knows how to use them? The wisdom of that course is not obvious. Evidence is scant that others act because they do not believe the United States has or can develop cyber capabilities. Conversely, the gains from brandishing such capabilities depend on the context and can be problematic even then.

There is both promise and risk in cyber brandishing, in both the conventional and nuclear cases. It would not hurt to give serious thought to ways in which the United States can enhance its ability to leverage what others believe are national capabilities. Stuxnet has certainly convinced many others that the United States can do many sophisticated things in cyberspace (regardless of what, if anything, the United States actually contributed to Stuxnet). This effort will take considerable analysis and imagination, inasmuch as none of the various options presented here are obvious winners. That said, brandishing is an option that may also not work. It is no panacea, and it is unlikely to make a deterrence posture succeed if the other elements of deterrence (e.g., the will to wage war or, for red lines drawn in cyberspace, the ability to attribute) are weak.