HARVARD Kennedy School
BELFER CENTER for Science and International Affairs
Policy Brief • January 2014

QUARTERLY JOURNAL: *INTERNATIONAL SECURITY*

Making Sense of Cyberwar

BOTTOM LINES

- **Differentiate means from ends:** There are many ways to cause harm, cyber or otherwise. The real issue is whether (and how) perpetrators of cyberattacks can convert virtual harm into tangible benefits for themselves.
- **Cyberwar is not "war."** By itself, internet conflict typically cannot achieve the objectives that are commonly associated with threats or uses of traditional military force.
- **Cyberwar benefits the strong**. Rather than serving to undermine the status quo, internet aggression further advantages those with traditional military and economic power.
- **Cyberwar does not destabilize**. Even if the offense dominates in cyberspace, advantages do not translate into incentives to attack unless actors are also capable in other domains.

By Erik Gartzke

This policy brief is based on "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," which appears in the Fall 2013 issue of International Security.

U.S. Defense Secretary Leon Panetta's warning that "the next Pearl Harbor" might arrive via the internet has captured considerable attention. The internet is said to be revolutionary because it is a leveler—reducing Western military advantages—and because dependence on the internet makes developed countries more vulnerable to attack. The conviction that the internet is an Achilles' heel for the existing world order is based on narrow conceptions of the potential for harm. The internet cannot perform functions traditionally assigned to military force. To the contrary, cyberwar creates another advantage for powerful status quo nations and interests.

DIFFERENTIATE MEANS FROM ENDS

The ability to harm is ubiquitous. Anyone passing on the street could punch you in the face. Still, violence is relatively rare in large part because most uses of force, while feasible, are probably not effectual. Perpetrators must ask themselves not just "what harm can I inflict?" but "how can I benefit by inflicting harm?" Cyberwar, like any behavior, requires a logic of consequences.

States, groups, and individuals threaten violence to conquer, to compel others to cooperate, or to deter aggression. Actors can also exercise violence to alter the balance of power. If the damage violence inflicts is temporary, however, then the initial act of aggression must be followed up with other actions, or an attack serves no purpose. Actions like the Pearl Harbor attack create "a window of opportunity," a temporary change in the balance of power, but aggression that does temporary damage is only useful if it is followed with a plan to exploit the opportunity.

War is a political process, not a separate and isolated exercise, as Karl von Clausewitz sought to make clear. Even the loser in a confrontation typically retains some capacity to harm. Cyberwar thus requires an explanation of how one side can conquer or compel over the internet, something that appears surprisingly difficult to construct. A morbid fear of being sucker punched may be misplaced if it is only based on capabilities, just as concern about cyberwar can be exaggerated if there is no evidence or reason to suggest how internet aggression achieves objectives useful to potential perpetrators.

CYBERWAR IS NOT WAR

The internet is a poor venue for achieving objectives typically pursued through the threat or use of military violence. Traditional military capabilities are observable. Armies appear near city gates. Missiles can be spotted in firing positions ready for launch. Military capabilities coerce because their effects can be anticipated. A city does not need to be stormed for the inhabitants to imagine the feasibility and consequences of an attack. Cyber coercion is more problematic in this regard because capabilities are difficult to communicate without degrading the potency of an attack. Targets cannot accurately assess credibility without information about key details of a planned cyberattack. At the same time, attackers cannot share this information with defenders without weakening the effectiveness of their potential attacks. Furthermore, if a defender accedes to unverified threats, then it invites a multitude of false claims.

Harm inflicted can be used to threaten future harm, but only if one act of harming serves as a good indicator of the effectiveness of future attacks. This works pretty well when attacks involve infantry brigades, war elephants, or high-speed penetrating bombers, whose capability may not be much affected by whether the enemy knows they exist. The success of cyber aggression, however, usually relies heavily on conditions of surprise. Past performance is also difficult to use to coerce; even an internet attacker that has succeeded in the past will be tempted to bluff.

The bigger issue with internet attacks, however, is that their effects are temporary. Unlike a rocket strike on an oil refinery or destruction of elements of a nation's military, cyberwar generally involves "soft kills," temporary incapacitation that can be reversed quickly and at moderate cost. Without a direct or lasting effect on the balance of power, internet aggression serves as either an irritant or as an adjunct to other, more traditional, forms of military force.

Imagine that some unspecified cyberattack disables communication or transportation nodes in a target country. What then? While inconvenienced, the target will eventually get the lights back on and vehicles running. The target will then attempt to retaliate. Permanent harm inflicted over the internet could weaken an opponent and might well serve as a motive for aggression. Such an attack could even be made anonymously, though anonymity would mean forfeiting the potential for coercion. However, internet attacks typically involve temporary damage, not permanent harm.

The Japanese attack on Pearl Harbor did considerable damage to the U.S. Pacific Fleet, but it failed to force the United States to the bargaining table, a critical component of Japan's grand strategy. Although Japan's leaders knew that total war with the United States would result in their defeat, they hoped for a limited contest. Cyberwar with no follow-on strategy is much more foolish than the Japanese plan in 1941, because the effects of a cyberattack can be repaired more quickly. Any attack over the internet must either convert short-term advantages into long-term effects or wager that the enemy will acquiesce to defeat in cyberspace, something particularly unlikely if damage is superficial or of short duration. A cyber Pearl Harbor has no military role unless it is accompanied by a terrestrial attack, precisely because the target can and will respond to any serious attack with a vigorous reprisal. If the target is unlikely to succumb to traditional forms of aggression, then cyberattack makes little sense, either. Being vulnerable on the internet is then much like being vulnerable to passersby on the street. An attack is certainly possible, but it serves no logical purpose and can be deterred in most circumstances by the threat of retaliation.

CYBERWAR BENEFITS THE STRONG

The few examples of cyberwar to date involve capable nations attacking much weaker countries. Incidents like Stuxnet and the denial of service attacks in Estonia and Georgia suggest that cyberwar works best when the attacker can deter reprisal in kind with other forms of violence or when the internet is used in conjunction with more traditional applications of force. As such, cyberwar is really an adjunct to modern warfare, not a replacement or even a particularly important modifier. Its presence is evolutionary rather than revolutionary. This is because cyber attacks by themselves can neither conquer nor effectively compel. Internet aggression can harm and may even expose an opponent to further attack, but it does not physically subdue. Without access to this final arbiter of conflict, practitioners of cyberwar must assume that opponents will not escalate, either because they are permanently unable to do so, or because they cannot be bothered to carry out retaliation. Unless cyberwar can serve as a final arbiter of conflict, there is no reason to believe that warfare on the internet will remain on the internet, unless both sides prefer this. Keeping conflict on the internet, however, implies that the stakes are not (yet) very high. Traditional forms of power create the discretion to escalate or to contain cyberwar, meaning that internet warfare is subordinate.

States with capable conventional militaries or considerable economic clout are best positioned to exploit windows of opportunity created by internet conflict. These same countries are also the ones best equipped to deter or defend against cyberattack through asymmetric threats and uses of force. Although many might be able to imagine a cyberattack on the United States, few will find it plausible to speculate about physical invasion of U.S. territory. It is far less difficult to imagine powerful countries invading weaker states. The internet age thus increases the options available to powerful states, augmenting rather than undermining, existing hierarchies.

CYBERWAR DOES NOT DESTABILIZE

Another assumption widely applied to cyberwar is that it is offense dominant. Nations and other actors will use the internet to attack each other, thus destabilizing world affairs. Yet, for the same reasons discussed above, it does not follow that incentives to strike in cyberspace equal a call to open warfare. Winning war on the internet could be a problem for countries unable to defend themselves from more traditional forms of warfare. Internet offense dominance might even lead to a decline in non-internet aggression, as powerful nations reconsider the use of force for fear that it will lead to reprisal. Further, details are available in the longer published version of this study.

• • •

Statements and views expressed in this policy brief are solely those of the author and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

RELATED RESOURCES

Biddle, Stephen. *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, N.J.: Princeton University Press, 2004).

Blainey, Geoffrey. *The Causes of War* (New York: Free Press, 1973).

Lindsay, Jon. “Stuxnet and the Limits of Cyber Warfare,” *Security Studies*, Vol. 22, No. 3 (August 2013), pp. 365–404.

Mao Zedong. *On Guerrilla Warfare* (New York: Praeger, 1961).

Rid, Thomas. “Cyber War Will Not Take Place,” *Journal of Strategic Studies*, Vol. 35, No. 1 (February 2012), pp. 5–32.

ABOUT THE BELFER CENTER

The Belfer Center is the hub of the Harvard Kennedy School's research, teaching, and training in international security affairs, environmental and resource issues, and science and technology policy. The Center has a dual mission: (1) to provide leadership in advancing policy-relevant knowledge about the most important challenges of international security and other critical issues where science, technology, environmental policy, and international affairs intersect; and (2) to prepare future generations of leaders for these arenas. Center researchers not only conduct scholarly research, but also develop prescriptions for policy reform. Faculty and fellows analyze global challenges from nuclear proliferation and terrorism to climate change and energy policy.

ABOUT INTERNATIONAL SECURITY

International Security is America's leading peer-reviewed journal of security affairs. It provides sophisticated analyses of contemporary, theoretical, and historical security issues. *International Security* is edited at Harvard Kennedy School's Belfer Center for Science and International Affairs and is published by The MIT Press.

For more information about this publication, please contact the International Security editorial assistant at 617-495-1914.

ABOUT THE AUTHOR

Erik Gartzke is Professor of Government at the University of Essex and Associate Professor of Political Science at the University of California, San Diego.

FOR ACADEMIC CITATION:

Gartzke, Erik. "Making Sense of Cyberwar." Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School, January 2014.

**Belfer Center
for Science and
International Affairs**

Harvard Kennedy School
79 JFK St.
Cambridge, MA 02138

TEL: 617-495-1400
FAX: 617-495-8963
http://www.belfercenter.org