International Security

POLICY BRIEF / FEBRUARY 2017

Why Cyber Operations Do Not Always Favor the Offense

Rebecca Slayton

This policy brief is based on "What Is the Cyber Offense-Defense Balance? Concepts, Causes, and Assessment," which appears in the winter 2016/17 issue of *International Security*.

Bottom Lines

Creating unnecessary vulnerabilities. Making offensive cyber operations a national priority can increase instabilities in international relations and worsen national vulnerabilities to attack. But because the skills needed for offense and defense are similar, military offensive readiness can be maintained by focusing on defensive operations that make the world safer, rather than on offensive operations.

Managing complexity. The ease of both offense and defense increases as organizational skills and capability in managing complex technology improve; it declines as the complexity of cyber operations rises. What appears to be offensive advantage is primarily a result of the offense's relatively simple goals and the defense's poor management.

Assessing kinetic effects. It is often more expensive for the offense to achieve kinetic effects—for instance, sabotaging machinery—than for the defense to prevent them. An empirical analysis of the Stuxnet cyberattacks on Iran's nuclear enrichment facilities shows that Stuxnet likely cost the offense more than the defense and was relatively ineffective.

A cyber security threat map is displayed inside a lounge during the RSA Conference on Wednesday, April 22, 2015, in San Francisco. (AP Photo/Marcio Jose Sanchez)

The assumption that cyberspace favors the offense is widespread among policymakers and analysts, many of whom use this assumption as an argument for prioritizing offensive cyber operations. Faith in offense dominance is understandable: breaches of information systems are common, ranging from everyday identity theft to well-publicized hacks on the Democratic National Committee. A focus on offense, however, increases international tensions and states' readiness to launch a counter-offensive after a cyberattack, and it often heightens cyber vulnerabilities. Meanwhile, belief in cyber offense dominance is not based on a clear conception or empirical measurement of the offense-defense balance.

One useful conception of the cyber offense-defense balance is based on cost-benefit analysis: What is the benefit of offense less the cost of offense, relative to the benefit of defense less the cost of defense? The technological complexity of cyberspace does tend to increase the costs of defense, but the costs of offense and defense are ultimately shaped by the complexity of the goals of offense and defense and organizations' capabilities in managing this complexity. Organizational skill can shift the costliness of cyber operations toward the defense. Further, whereas breaching information systems is easy and can be done at relatively low cost, achieving physical effects is far more difficult and costly. Meanwhile, the benefits of cyber operations are highly situational and subjective. Thus, claims that all of cyberspace is offense dominant obscure crucial differences between distinctive kinds of operations and the ways they are valued; such claims should be avoided. It only makes sense to discuss the offense-defense balance of specific cyber operations with specific goals, between specific adversaries with distinctive capabilities.

Creating Unnecessary Vulnerabilities

Prioritizing offensive operations can increase adversaries' fears, suspicions, and readiness to take offensive action. Cyber offenses include cyber exploitation (intelligence gathering) and cyberattack (disrupting, destroying, or subverting an adversary's computer systems). An adversary can easily mistake defensive cyber exploitation for offensive operations because the distinction is a matter of intent, not technical operation. The difficulty of distinguishing between offensive and defensive tactics makes mistrustful adversaries more reactive, and repeatedly conducting offensive cyber operations only increases distrust. A focus on offensive operations can also increase vulnerabilities; for example, secretly stockpiling information about vulnerabilities in computers for later exploitation, rather than publicizing and helping civil society to mitigate those vulnerabilities, leaves critical infrastructure vulnerable to attack.

The skills and organizational capabilities for offense and defense are very similar. Defense requires understanding how to compromise computer systems; one of the best ways to protect computer systems is to engage in penetration testing (i.e., controlled offensive operations on one's own systems). The similarity between offensive and defensive skills makes it unnecessary to conduct offensive operations against adversaries to maintain offensive capability. Thus, rather than stockpiling technologies in the hope of gaining offensive advantage, states should develop the skills and organizational capabilities required to innovate and maintain information and communications technologies.

Managing Complexity

The complexity of information systems gives the offense certain advantages for purely probabilistic reasons. Imagine a race: offense and defense go hunting for randomly distributed vulnerabilities, with the offense attempting to exploit those vulnerabilities and the defense aiming to patch them. The number of vulnerabilities grows with the size and complexity of the computer system, as do the technological advantages of offense—at least in principle. With a vast number of vulnerabilities, it is unlikely that the defense will be able to find and patch every vulnerability before the offense finds and exploits it.

Technology is, however, embedded in social organizations, and organizations can help the defense better manage complexity. Those that develop software can check for common errors before making hardware-software systems available for use. The defender has complete access to its computer system, whereas the attacker has a more limited set of attack vectors. Organizations can help skilled defenders by establishing good cybersecurity processes, such as continually scanning for vulnerabilities and updating software.

Assessing Kinetic Effects

To date, failures of cyber defense have largely been failures of management, and the successes of offense are a result of its relatively simpler goals. Offense, like defense, becomes more difficult as its goals become more complex. In particular, the advantages that complexity offers the offense in cyberspace diminish in the physical world. Computers controlling physical machinery can be hacked, but achieving particular physical effects, such as covertly sabotaging nuclear enrichment facilities, requires knowledge of the physical processes that the computers control, not merely knowledge of the computers. Much of the detailed knowledge needed to run an industrial control system is tacit, passed from one engineer to another but never written down, let alone stored on a computer. Gathering such information requires traditional espionage by humans on the ground, which is both expensive and risky.

A cost-benefit analysis of Stuxnet for both the offense and the defense demonstrates why damaging physical infrastructure is more costly than simply infiltrating information networks. The costs of Stuxnet were likely far greater for the offense (the United States and Israel) than for the defense (Iran), and Stuxnet was relatively ineffective, setting back Iran's nuclear program by fewer than three months. The great expense of Stuxnet was intelligence; though digital espionage can be used to obtain some kinds of information, the knowledge needed to disrupt a physical control system, such as the detailed methods and settings used to control pressure in Iran's nuclear centrifuges, is not generally held in computers. The costs for both sides are dominated not by technology but by skilled labor—for example, hackers who identify and exploit zero-day vulnerabilities, systems administrators who manage and defend computer systems, and the nuclear engineers who understand enrichment processes and the means of disrupting them.

In addition, assessing costs alone is misguided: the perceived benefits of attacking with and defending from Stuxnet (i.e., the value of Iran's nuclear weapons program) greatly exceeded the costs for both the offense and the defense. This is one reason not to be complacent about the need to secure industrial control systems and critical infrastructure: though cyberattacks on such systems will be costly, a determined adversary may be willing to pay the cost to achieve its aims.

Conclusion

The common assumption that the offense dominates cyberspace is dangerous and deeply misguided. The offense-defense balance can be assessed only for specific operations, not for all of cyberspace, as it is shaped by the capabilities of adversaries and the complexity of their goals in any conflict. When it comes to exerting precise physical effects, cyberspace does not offer overwhelming advantages to the offense. Because the capabilities of offense and defense are similar, improving defensive operations allows preparation for cyber offense without risking geopolitical instability or increasing vulnerability to attack.

Related Resources

Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (London: C. Hurst, 2016).

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

William A. Owens, Kenneth W. Dam, and Herbert S. Lim, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009).

Rebecca Slayton is Assistant Professor at Cornell University with a joint appointment in the Science and Technology Studies Department and the Judith Reppy Institute for Peace and Conflict Studies

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* publications coordinator at 617-495-1914.

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.

International Security
International Security Program
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

belfercenter.org/IS