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

QUARTERLY JOURNAL: *INTERNATIONAL SECURITY*

The Shape of the Cyber Danger

BOTTOM LINES

- **The Lag between Cyber Realities and Strategic Theory.** The growth of cyber arsenals is outpacing the design of doctrines to limit their risks.
- **The Potent Effects of Cyber Weapons.** Even if a cyberattack does not produce destruction comparable to war, it can still cause significant political, social, and economic harm.
- **Challenges to Defense.** Those with advanced code have significant tactical advantages over defenders.
- **Disturbances to Strategic Stability.** The cyber domain exhibits many features of strategic instability, including the potential for nonstate actors to disrupt interstate dealings.

By Lucas Kello

This policy brief is based on "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," which appears in the Fall 2013 issue of International Security.

DELAY IN STRATEGIC ADAPTATION

There is little consensus among scholars and practitioners on how to confront or even characterize the contemporary cyber threat. The range of conceivable cyber conflict is poorly understood by strategic thinkers, and it is unclear how conventional security mechanisms, such as deterrence and collective defense, apply to this phenomenon. The cyber revolution's strategic quandaries need urgent resolution.

Mastery of the cyber issue requires an ability to break free from familiar conceptions of security and conflict. Insofar as the consequences of a cyberattack do not rise to the level of traditional interstate violence, the notion of cyber "war" is meaningless. Nevertheless, the virtual weapon is expanding the range of possible harm and outcomes between the concepts of war and peace—with important consequences for national and international security. Three main factors underscore the cyber danger: (1) the potency of cyberweapons, (2) complications relating to defense, and (3) problems of strategic instability.

POTENCY OF CYBERWEAPONS

The payload of a cyberweapon is intangible: it operates by manipulating a remote object, such as an industrial controller, with complex coding. Nevertheless, the new capability can have potent effects on the political, social, and economic world. Operation Olympic Games, which impaired hundreds of nuclear centrifuges in Natanz, Iran, proved that weaponized code can damage physical facilities. Yet a cyberattack need not produce physical destruction to pose serious dangers to national security. The nonviolent cyberattacks against Estonia in 2007, which convulsed the country's government and financial activities for several weeks, underscore the point.

Because cyber artifacts can inflict harm short of traditional war, they expand the choice of actions and outcomes available to the strategic offense. Take, for example, Olympic Games: the operation achieved some of the same tactical results as a conventional military strike while diminishing the risk of a regional conflagration.

COMPLICATIONS RELATING TO DEFENSE

The current high cost of mounting a high-impact cyber operation limits the asymmetrical gains available to weak state and nonstate actors. It does not confer advantages to the defense over the offense. The offense-defense balance is relative: the absolute measurement of offensive costs has meaning only in reference to the defender's expenses, which are enormous. At least five factors weigh on the defender.

OFFENSE UNPREDICTABILITY. The vast universe of manipulable "zero-day" or unknown weaknesses in computer systems renders the method of cyberattack difficult to predict, hindering the design of measures to repulse it. Moreover, the abundance of possible access vectors complicates the interception of malware in transit.

DEFENSE DENIAL. The ability of attack code to reside undiscovered in a defender's computer system is perhaps the most worrisome feature of the cyber strategic landscape. It gives the invader means to foil the defense—for example, by using peer-to-peer monitoring to adjust the attack sequence in real time.

COMPLEX DEFENSE SURFACE. Computer systems are becoming more intricate, resulting in a fundamental offense-defense imbalance. Whereas an attacker need understand only the procedures of intrusion and attack that it decides to employ, the defender must continuously protect the entire network surface against the vast universe of conceivable attacks.

DEFENSE FRAGMENTATION. The authority to execute proactive cyber defenses rarely belongs to the operators of computer systems subjected to attack; instead, it resides with the government and internet service providers. Such fragmentation of defense responsibilities is a limiting factor when formulating a coherent response to a major cyberattack.

SUPPLY CHAIN RISKS. Computer systems increasingly rely on off-the-shelf and offshore components, introducing vulnerabilities into the supply chain. An adversary could decide to execute a preloaded "sleeper" payload during a diplomatic or military crisis.

PROBLEMS OF STRATEGIC INSTABILITY

The cyber revolution can disturb conventional patterns of interstate rivalry in two main ways. First, the absence of clear or agreed upon assumptions and rules of cyber conflict creates dangers of miscalculation and misinterpretation even among rational state adversaries. Second, more fundamentally, the diffusion of cyber technology in modern society is empowering nontraditional players with subversive motives and aims. The six factors presented below contribute to strategic instability in one or both of these ways.

OFFENSE DOMINANCE. Offense superiority has instigated a race to arms as states seek to avert strategic upsets in the cyber domain. While "active defenses"—which neutralize cyber threats by infiltrating or disrupting an opponent's computer systems before they are carried out—may help to close the defensive gap, they obscure the offense-defense boundary in weapons systems. Consequently, a player may misconstrue an opponent's defensive acts as overt aggression, producing pressures for an accidental exchange of blows.

ATTRIBUTION DIFFICULTIES. Authentication of the source of a cyberattack may not be prompt enough to enable timely retaliation. By the time their identity is known, the attackers may have relocated beyond the ability of the victim to respond. This problem weakens deterrence by reducing an assailant's expectation of unacceptable penalties.

TECHNOLOGICAL VOLATILITY. Cyberweapons are so novel and variable that it is difficult to model or predict probable effects of their use. While customization of the payload can reduce the possibility of unintentional civilian harm, the indirect effects of a cyberattack can still be enormous if the affected computer systems support essential social and economic activities. There is also the potential for unforeseen "blowback," in which the attacker experiences negative effects, whether through the self-propagative tendencies of malware or through cascading economic damage.

POOR STRATEGIC DEPTH. The extremely short period between the detection and impact of a cyberattack, which unfolds in milliseconds, can strain existing crisis management procedures, which operate at the speed of bureaucracy. The implementation of automated response mechanisms can go far toward resolving this problem, but by removing humans from the response procedure, these mechanisms introduce unknown risks of inappropriate reaction.

ESCALATORY AMBIGUITY. Tactical and strategic ambiguities impede the design of escalatory models of cyber conflict. What may begin as a low-intensity cyber exchange could intensify into a major showdown—possibly of conventional proportions. Cyber exploitation (i.e., the penetration of a computer system to seize data but not disrupt it) could set a crisis in motion if the defender misconstrues the intrusion as a step preparatory to attack, instigating a preemptive blow.

DIVERSITY OF PLAYERS. The cyber domain features a variety of relevant players, ranging from states to private groups and even individuals. As the number of cyber-capable states rises, the transaction costs of cooperation among them increase. Moreover, the rising number of players in the domestic cyber establishment can impede the ability of states to interact as coherent units. A more important source of instability stems from the dispersion of cyberpower away from governments. Although states remain the principal players in the cyber domain, they are not alone. The cyberattacks against Estonia and Georgia (in 2008) demonstrate the ease with which civilian actors can cause serious harm across national borders.

The diversity of cyber players and the possibilities for cooperation among them establish conditions for fundamental instability. In effect, policymakers must grapple with two distinct challenges: (1) a traditional system of states locked in familiar contests for security but featuring a largely untested weapon whose use is difficult to model or regulate; and (2) a chaotic world of nontraditional actors who may seek to subvert national or international order.

The greatest test of strategy may be its ability to address the convergence and collision of these two universes. On the one hand, the wide diffusion of cyber technology enables new modes of cooperation among state and nonstate players that share certain goals and adversaries. On the other, a cyber event perpetrated by civilian culprits could precipitate a major interstate conflict. Thus a dangerous separation of power and diplomacy is occurring. Even if some problems of instability in the cyber domain were soluble through intergovernmental agreement, private actors could still unsettle the interstate equilibrium by defying the consensus.

CONCLUSION

The cyber revolution presents formidable challenges to security policy. The risks of inadvertent or accelerating cyber crises are significant but poorly grasped. The penalty for falling behind in terms of strategic adaptation may be disastrous.

• • •

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

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010).

Nye, Joseph S. *The Future of Power* (New York: PublicAffairs, 2011), chap. 5.

Rid, Thomas. *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

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 THE AUTHOR

Lucas Kello is a Postdoctoral Research Fellow in the International Security Program and the Project on Technology, Security, and Conflict in the Cyber Age at the Harvard Kennedy School's Belfer Center for Science and International Affairs.

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.

FOR ACADEMIC CITATION:

Kello, Lucas. "The Shape of the Cyber Danger." Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School, March 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