The Meaning of the Cyber Revolution:
Perils to Theory and Statecraft

Lucas Kello
Postdoctoral Research Fellow, Harvard Kennedy School

This poster is based on an article by the same title published in *International Security,* Vol. 38, No. 2 (Fall 2013), pp. 7-40 | www.mitpressjournals.org/loi/isec

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University
Workshop on
Cyber Security & the Governance Gap
MIT, 6-7 January 2014

The Problem

Do cyberweapons require a revolution in thinking about force and conflict?

Practitioner's predicament in addressing this question: the cyber revolution gives rise to novel threats and opportunities requiring immediate policy responses; yet grasping its implications is a slow learning process.

The result is a lag in strategic understanding.

•No consensus "on how to characterize the strategic instability" of cyber interactions. (Gen. Keith Alexander)

•Range of conceivable cyber conflict is poorly understood

•Principles of cyber offense and defense are rudimentary

•Not clear how traditional security mechanisms apply

There is an evident need for international relations and security scholars to contribute to the theoretical evaluation of the cyber revolution.

Yet there is little systematic analysis from a security studies perspective.

Degrees of Skepticism

Some scholars are skeptical about the importance – or even the feasibility – of cyber studies.

Deep skeptics emphasize methodological obstacles:

•A paucity of cases

•Limited data

•The technology's scientific complexity

Other skeptics focus on substantive aspects. They invoke the logic of Carl von Clausewitz: the cyber threat is overblown because the related technology does not alter the nature of interstate war. They claim the following:

•Cyberattacks are not overtly violent and do not create 'collateral' damage

•Destructive cyberattacks will be rare owing to high costs of execution

•The defense, not the offense, holds the strategic advantage

Such skepticism has resulted in considerable neglect of the cyber issue. The resulting scholarly gap hinders the intellectual progress and policy relevance of the security studies field.

The Argument

The skeptics misconstrue the meaning of the cyber revolution. True, the virtual weapon has not fundamentally changed the nature of war. Further, insofar as cyberattacks do not rise to the level of interstate violence, there will be no cyber 'war.'

Yet the Clausewitzian philosophical framework misses the essence of the cyber revolution: the new capability is expanding the range of possible harm between the concepts of war and peace – with important security implications.

The disanalogy of war conveys only what the cyber issue is not; it does not reveal the true significance of the danger and may even conceal it. Three factors underscore the cyber danger.

1. Potency of Cyberweapons

The virtual weapon has produced no fatalities or physical destruction comparable to a traditional war. Two problems nevertheless persist for the cyber skeptics:

(1)The upper threshold of proven harm has steadily risen – it now includes destruction of physical infrastructures

(2)Nondestructive cyber artifacts can inflict considerable harm on the political, economic, and social world

The trajectory of proven harm has few clear limits; we should not seek to impose them on so novel and volatile a technology. At any rate, destructive action may not pose the most pressing concern.

The analogies of 'sanctions' and 'sabotage' do not apply to the cyber phenomenon.

•Sanctions are a form of negative power, yet cyberattacks inflict direct loss on the victim

•Sabotage is an empty concept: it has no precise definition in this or other domains of conflict

2. Complications of Cyber Defense

The costs of cyber defense are enormous. Five problems weigh on the defender:

(1)Offense unpredictability and undetectability

(2)Defense denial

(3)Complex defense surface

(4)Defense fragmentation

(5)Supply chain risks

The thesis of defense dominance misses a crucial truth: the offense-defense equation is relative. Thus, the attacker's absolute costs have meaning only in reference to the defender's expenses, which are far higher.

The high price of mounting a high-impact cyberattack limits the asymmetrical gains available to weak players. It does not eliminate the significant tactical advantages of advanced code.

3. Strategic Instability

The cyber revolution is exerting a limited but observable influence on regularized patterns of international security competition.

One problem is **'instrumental' instability**, whereby poor 'if-then' knowledge of a new genus of conflict produces misinterpretation and accidents. Five factors of the cyber age contribute to this:

(1)Offense superiority

(2)Attribution difficulties

(3)Technological volatility

(4)Poor strategic depth

(5)Escalatory ambiguity (e.g., Equivalence Doctrine)

Another problem concerns **'fundamental' instability**, in which the empowerment of nontraditional players undermines interstate strategic stability.

Nonstate actors may perpetrate a 'catalytic' cyber event that instigates an unwanted diplomatic or military showdown.

In sum, the cyber domain exhibits **two 'states of nature'**:

(1)The traditional anarchic states system featuring an untested weapon whose use is difficult to model and regulate even among rational contenders

(2)A chaotic 'global' system comprising nonstate actors who may disturb the delicate political framework of international anarchy

The diversity of cyber players and the possibilities of cooperation among them will strain familiar models of security competition.

Follow-on Research

The next stages of this project will seek to identify and elaborate on the implications of the cyber revolution for logics of (1) collective defense, (2) deterrence, and (3) escalation control following a failure to deter cyberattacks.

Acknowledgements

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research.

This work was prepared under the aegis of the Science, Technology, and Public Policy Program and the Cyber Project at the Harvard Kennedy School's Belfer Center for Science & International Affairs.