

# Ethical Issues of Cyberwarfare

by Randall R. Dipert  
Department of Philosophy,  
National Center for Ontological  
Research (NCOR)\*  
University at Buffalo  
Buffalo NY 14260  
[rdipert@buffalo.edu](mailto:rdipert@buffalo.edu)

\*Contract with the U.S. Army's Net-Centric Data Strategy Center of Excellence (ANCDS CoE, FT Monmouth) for the development of an ontology of Command and Control

# Recent Background:

- Pending formation of CYBERCOMMAND in U.S. Department of Defense

Nominated Commander: LTG Keith Alexander (USAF; Director of NSA)

- Organized National Cyberattacks

Russia on Georgia (2008)

Iran on Twitter, etc. (2009)

N. Korea on US Banks and DoD (July 2009)

China on Google, Gmail (Dec. 2009) ....

# What's New:

- Organized Cyberattacks by one state (or political organization) on another.

Past Cyberattacks:

Individual (hackers) or corporate

Motive: mischief or economic

Espionage

- Recent Intent: Deface websites, destroy data, interrupt functioning of information networks with a goal to damage military capabilities and economy.

# What's Needed:

- National Policy/Doctrine/ Strategy of Cyberwarfare
- Implications of Just War Theory for Cyberwarfare? (*Jus ad bellum* and *Jus in bello*)
- New Concepts and Principles of Morality for Cyberwarfare?
- How do international and customary law apply to Cyberwarfare?

# Recent Literature (1 of 3)

## **CYBERDETERRENCE AND CYBERWAR**

**MARTIN C. LIBICKI**

Prepared for the United States Air Force  
Approved for public release; distribution unlimited



**RAND** PROJECT AIR FORCE

# Martin C. Libicki, Cyberdeterrence and Cyberwar (2009)

- Strengths:

  - History and Cyberoperations

  - Deterrence

  - Difficulties of Cyberarms Control

- Weakness:

  - No discussion of ethical or (international) legal issues

# Recent Literature (2 of 3)

“Warfighting in Cyberspace,”

by the designated future commander of U.S.  
CYBERCOMMAND, LTG Keith Alexander  
(USAF)

*Joint Forces Quarterly,*  
46:3 (2007) pp. 61f.

# Recent Literature (3 of 3)

## ***Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities***

William A. Owens, Kenneth W. Dam, and Herbert S. Lin,  
*Editors*

Committee on Offensive Information Warfare  
Computer Science and Telecommunications Board  
Division on Engineering and Physical Sciences  
National Research Council (2009)

# Owens et al., *Technology...Cyberattack Capabilities*

## Strengths:

- Describes command structure
- Extensively discusses ethical and legal issues

## Weaknesses:

- Ethical discussion unimaginatively goes through traditional distinctions in Just War Theory (JWT)
- Mostly Legal
- Sidesteps the question: anything distinctive in Cyberwarfare?

# Defensive vs. Offensive Cyberwarfare

There is a general consensus that *defensive* measures against cyberwarfare are fairly unrestricted: password protection, identification of IP addresses, blocking of information from certain IP addresses, etc. But...

This is just cybersecurity.

# The Hard Moral Questions

- When is *offensive* cyberwarfare justified?
  - Destroy capability of enemy to attack.
  - Inflict damage as justice.
  - Deterrence
- When, if ever, would a conventional (non-cyber) attack be morally justified because of an enemy's destructive cyberattack?

# Clarifying Some Concepts

1. Cyberattack: intentional harm inflicted via a network, especially the internet
2. Act of Cyberwarfare: cyberattacks by one nation (or political organization) on another for political reasons (including economic harm and degrading of military defensive/offensive capacity)
3. Cyberwar: widespread, mutual, severely destructive acts of cyberwarfare.

# Wars and Cyberwars

Brian Orend's definition of 'war': "*actual, intentional and widespread* armed conflict between political communities." (*Stanford Internet Encyc. Of Philosophy*)

Issues:

Armed?

Add: Use of deadly force?

Centrally initiated or controlled.

By military forces? What does it mean to be "military"?

# Wars and Cyberwars

Peculiar fact of cyberattacks and cyberwarfare:

They are not “materially intrusive”:  
they don’t involve the intrusion of material objects into the sovereign territory or airspace of another nation.

# Offensive War and the Military

*Why should* offensive cyberwarfare capacity reside with the military?

- LTG Alexander: Chinese and N. Korean cyberwarriors are already organized into battallions and regiments
- Chain of Command in place; centralized C2.
- Commanders at all levels are trained and aware of the methods of restraining harm: ROEs, military necessity, etc.
- Cyberattacks have the capacity to inflict harm to a country on the level of a massive bombing attack

USAF has been the lead service in cyberwarfare:

Airspace=Cyberspace

Use of force “at a distance”

# Types of Cyberattack

1. Destruction or corruption of data.
2. Destruction or corruption of algorithms
3. Denial of Service (DoS) attack.
4. Distributed Denial of Service Attack (DDoS)
5. Intentional harming to humans, machines, artificial systems, or the environment by (1)-(3)

(Ignore espionage)

# Distinctive Characteristics of Cyberattacks

1. Epistemic (A): difficult to determine the attacker's *identity*. IP source address masking; Distributed; DNA-like forensic tracking.
2. Epistemic (B): difficult to identify *intent* in attack, especially if delayed-effect (Trojan).

# Distinctive Characteristics of Cyberattacks

3. Ontological difficulty: harm need not be killing or wounding of humans, or destruction of material objects. The functioning of *systems* is impaired.

Compare: bombing of nodes of a power grid with the insertion of faulty software for controlling the grid.

# Distinctive Characteristics of Cyberattacks

4. Legal-moral difficulty: territory, sovereignty not violated. The intrusion is by electrons or photons, whose entry pathway the attacked nation has built.

Inadequate Traditional thinking:

U.N. Charter: “threat or use of force against the territorial integrity or political independence of any state” (Article 2, Section 4).

# Cyberattack as *Casus belli*?

A cyberattack is not a paradigmatic “act of war”: invasion or killing.

There are other, traditionally recognized, *casus belli* (give Just Cause for retaliation up to physical force in JWT):

Blockades, mining of shipping lanes,...

Harassment of businesses, diplomats,  
citizens abroad

Interruption of pipelines, etc.

# Cyberattack as *Casus belli*?

We need a more general principle than just being literally an attack, armed aggression, invasion, etc.:

Extensive, deep, intentional *harm* to vital national interests--including economic and information systems--coordinated by another state or military.

# A Cyberattack is morally analogous to ...

An attack by a laser, EMP (Electromagnetic Pulse) weapon, radar/radio jamming, etc.

Most like Electronic Warfare (EW):

- JP 3-13 *Joint Doctrine for Information Operations*, Ch. 3 Offensive Operations(1998)
- JP 3-51 *Joint Doctrine for Electronic Warfare* (2000)
- JP 3-13.1 *Electronic Warfare* (2007)

# Generality necessary for Just Cause in JWT requires

Shift from the *mode* of intentional harm  
(invasion, armed attack, kinetic, projectile  
weapons)

To:

Quantity and quality of intentional harm--  
Widespread, deep, unrecoverable,...harm  
to vital national interests

# Offensive Cyber- or Conventional Attack by B on C justified when:

1. The cyberattack of C on B (or an ally of B) was **unjust and substantial**, and
2. The source of the cyberattack by C was, with overwhelming likelihood, **ordered or permitted** at the highest levels of the **government of C**.

# Offensive Cyber- or Conventional Attack by B on C justified when:

3. **Reasonable measures** had been taken by nation B to **defeat or minimize the cyberharm** that a hostile nation C was causing by cyberattacks, and
4. The expected damage to the enemy (C) is (i) likely to be **commensurate** to the intentional damage B has suffered, or (ii) whatever is **necessary to stop** the cyberattack, or (iii) is the **minimum necessary to deter** future cyberattacks (by C or another nation)

# Especially unusual is:

**3. Reasonable measures** had been taken by nation B to **defeat or minimize the cyberharm** that a hostile nation C was causing by cyberattacks

In conventional warfare, the attacked nation's morally justified counterattack does not require the attacked nation to have taken all reasonable defensive measures (air defenses, bomb shelters)

Why is CyberWarfare different? B's permission of open information pathways (net international connectivity) brings a "burden of defense."

# International Law

Most applicable is:

Protocol I (1977) to the Geneva Convention

“Art 54. Protection of **objects**

indispensable to the survival of the civilian

population ¶1. Starvation of civilians as a

method of warfare is prohibited. ¶2. It is

prohibited to attack, destroy, remove or

render useless **objects** indispensable to

the survival of the civilian population...”

# International Law

The Problem with Protocol I (1977) to the Geneva Convention Article 54 (and other relevant international law) is a lack of ***ontological inclusiveness--***

Prohibits:

Intrusions by physical objects

Destruction of ***objects*** including human beings and ***objects*** necessary to human welfare.

But not **harm** to:

economic/governmental/information **systems.**

# What to Do?

1. Development of Cyberwarfare policy/doctrine; announcing parts of it; acting according to it.

Contrast with NBC warfare: announced, active measures taken (development of delivery; testing), but no demonstrations of policy.

Cyberwarfare permits of degrees; no problem of letting genie out.

# What to Do?

1. Development of Cyberwarfare policy/doctrine.....

Integrate traditional, “intuitionist” theories of morality of war including JWT with game-theoretic understanding of the effects of policies. (Rule-consequentialism.)

# What to Do?

2. Development of forensic cyberattack techniques: exactly who attacked and why?

Private sector has not developed this: interested in blocking or blunting attacks, not in counterattack.

# What to Do?

3. Muzzle U.S. hackers' cyberattacks on international targets in the interests of foreign policy.

Easily mistaken for U.S. government decision to attack or permit attack.

# Just War Theory and Cyberwarfare: *Jus ad bellum*

- Just Cause
- Proper Authority
- Right Intention
- Likelihood of success
- Proportionality—instance of a policy likely to minimize harm to all in the long run
- Last Resort

# Just War Theory and Cyberwarfare: *Jus in bello*

- Proportionality
- Discrimination. Target (in order):
  - Offensive cyberattack capability
  - Offensive conventional capability
  - Non-vital National interests
  - Defensive conventional capability
  - Conventional attack, vital national interests

# The Way Ahead: A Long Cyber Cold War

- Extensive cyberattacks by nations on other nations—will eventually achieve an equilibrium with regard to low level of harm. (Like espionage.)
- Retaliation and Deterrence
- Multilateral: by states; large, especially multinational, corporations; non-state political actors.
- No prospect for Cyber Arms Control (Epistemic problems; widely distributed tools for harm)

# The Way Ahead: A Long Cyber Cold War

Unless:

- (i) A nation's defensive cyber operations are sufficient to minimize harm to it, or
- (ii) All nations with advanced cyberattack capability “play nice” and withhold attacks

Then:

A nation should retaliate in order to protect its economy, government, and informatics integrity.

- (i) and (ii) are false now and will remain false for the foreseeable future.