CYBERTECHNOLOGY AS DUAL-USE TECHNOLOGY

JUDITH REPPY

CORNELL UNIVERSITY

11 JANUARY 2012

OVERVIEW

- Conceptual issues
- Cybertechnology characteristics
- From the military to the civilian
- Policy consequences

WHAT IS DUAL-USE TECHNOLOGY?

A technology that can, with some adaptation, have both military and civilian applications.

The concept depends on being able to identify discrete technologies and distinct civil and military sectors.

EXAMPLES OF DUAL-USE TECHNOLOGY

Standard dual-use examples are jet engines, satellites, computers, etc.

These examples are material objects, and policies governing dual-use—especially export controls—implicitly have assumed that the technology can be mapped on to something material.

INFORMATION AS TECHNOLOGY

Conceptually, information (data, equations, blueprints) is a form of technology.

Control of dual-use information has posed special problems, especially in the form of deemed exports.

These problems are acute for cybertechnology.

CYBERTECHNOLOGY IS DUAL USE

Cybertechnology definitely qualifies as a dual-use technology:

- Early developments in computers, software, and the Internet were all funded by the military for use in military applications.

FROM MILITARY TO CIVILIAN

Subsequent development and growth occurred in civilian applications, which now dominate the market. Many civilian services and activities have migrated to the web.

The military has greatly expanded its dependence on cybertechnologies originating in the civilian sector.

EXAMPLE: SMARTPHONES ON THE BATTLEFIELD

The US Army plans to issue smart phones to soldiers. The phones will be limited to unclassified and FOUO information. To make them useful, tactical operational information in the field is to be declassified below the battalion/squadron level. The phones will be standard civilian models (but not iPhones).

DUAL USE—BUT WITH A DIFFERENCE

Cybertechnology is pervasive and globally distributed. In most countries the barriers to access are low.

It is not a single object, but a *system*, one that operates in cyberspace, which is in many respects not amenable to government control.

A QUASI-PRIVATE GOOD

To a considerable extent, the Internet is self-organized within the civilian sphere by a mix of private and voluntary organizations.

In short, the cyber system is a quasi-public good.

WHY "QUASI"? (1)

A public good is a good for which:

1. **access is unlimited and**
2. **use is non-rivalrous (my use does not preclude your use).**

WHY "QUASI"? (2)

Cyber is only "quasi" because access to cyberspace requires a networked device, an internet service provider, and a tolerant government.

Where those are present it operates as a public good.

We might call it a public utility.

PUBLIC GOODS AND DUAL-USE

By definition, all public goods are *potentially* dual-use.

But adoption by the military tends to destroy their public availability.

Examples:

- military air space excludes private planes
- ocean firing ranges are off-limits to fishing boats;

INSTITUTIONS MATTER

As with other public and quasi-public goods, open access to cyberspace depends on supporting institutions and practices.

HISTORICAL DIGRESSION: DUAL-USE IN THE COLD WAR

The concept of dual-use technology had two main impacts on U.S policy during the Cold War:

- It structured an export control regime to prevent the spread of technology to hostile states.
- It underpinned a range of technology policies aimed at increasing the utilization of civilian technologies by the military and vice versa.

POLICY IN THE 1970S AND ‘80S

The problems were:

- The cost of maintaining separate civilian and military technology bases.
- Civilian technology was outstripping military technology in important areas.

POLICY IN THE 1970S AND ‘80S

The response:

- Various schemes for increasing technology transfer across the civil-military divide.
- Always subject to constraint on overt industrial policy.

TECHNOLOGY POLICIES IN THE 1990S

Secretary of Defense William Perry introduced an official dual-use policy for the Department of Defense to promote the use of civilian technologies.

Defense reliance on information technologies continued to grow.

THE RISE OF THE INTERNET

The Internet has became the dominant medium for information exchange: by 2007 it accounted for 97% of the world capacity to telecommunicate information.

An important feature is its global reach. Information from abroad is accessed as easily as information from one's own neighborhood.

POLICY TODAY

The old framework for policy is not relevant.

- Use of cyberspace and cyber-technology is virtually universal—no need to promote it.
- Because the technology is available globally, unilateral controls have limited utility.

THE POLICY DILEMMA

Beyond dual-use:

Cybertechnology is not just similar in its military and civilian uses—the military uses of cyber-technology cannot be disentangled from the civilian uses.

THE POLICY DILEMMA

The benefits of cybertechnology depend on the very characteristics that the government would like to control: ubiquity and global reach.

Because the military and civilian uses overlap, controls on one will affect the other.

LEVELS OF SECURITY

Commercial enterprises and private persons choose a level of protection for their cyber activities which balances convenience with safety.

Governments face more determined attacks and require a higher level of security. For example, computers can be disconnected from the Internet and usb ports disabled.

LIMITS TO CONTROL

The government's freedom of action is constrained by structural features of the Internet.

- Much of the infrastructure of the Internet is privately owned.
- There is strong support for the Internet as an open public space.

The old policy tools are not relevant to the new situation.

A DIFFERENT POINT OF VIEW

Demchak and Dombrowski (2011) have argued that a new Westphalian state system is under construction in cyberspace. They believe that

"A cybered national border is technologically possible, psychologically comfortable, and systemically and politically manageable."

In effect, they argue that the old rules are applicable to the new situation.

BUT WHICH OLD RULES?

Defense against cyberattacks cannot be carried out solely by the military, as with conventional weapon attacks. For example, cybersurveillance at the borders, as proposed by Demchak and Dombrowski, would sweep up civilian traffic as well.

Controls on information flows in the export control regime are a poor model for thinking about protecting cyberspace.

CONCLUSIONS

The dual-use nature of cybertechnology along with its status as a quasi-public good define both the source of the benefits of the technology and the limits to government control.

Actions taken in the name of cybersecurity and national defense will impinge on civilian users and may harm the civilian economy.