

Testimony
of
Pat Choate
Director, The Manufacturing Policy Project

“Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American
Technology”

Before

The Oversight & Investigations Subcommittee
The House Committee on Foreign Affairs
United States Congress
Washington, D.C.
April 15, 2011

Mr. Chairman and Members of the Committee:

My name is Pat Choate. I direct The Manufacturing Policy Project, a non-profit public policy research institute that studies the U.S. and global economy. I am pleased to share some thoughts with you on “Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology.”

I will limit my comments to Cyber-Espionage and the effects of existing patent publication policies on U.S. economic and national security.

The Internet and Espionage

The Internet is now the principal tool of modern espionage. Cyber-spying allows intruders to place Trojan horse software inside target computers. This spy ware is most often undetectable to operators, the system and any cyber guards. The mission of this software is to send proprietary information back to the cyber spy on whatever schedules the intruder desires.

While China’s companies and governments are major sources of cyber-spying, they are hardly alone. Interviews with cyber security experts, both in and out of the federal government, reveal that many other nations do the same, though not on the same scale as China.

The economics of cyber-theft is simple: Stealing technology is far easier and cheaper than doing original research and development. It is also far less risky to the spy than historic cloak and dagger economic espionage.

A major problem for cyber-spies working in the U.S. with its rich technology base is the identification of the most promising targets. The U.S. government assists in that selection process by requiring the Patent Office to post on the Internet patent applications 18 months after the filing date. Thus, in one place, -- the open computers of the U.S. Patent Office -- a cyber spy can find virtually all the newest, cutting-edge U.S. technologies in virtually any field.

Once the cyber-spy has identified an inventor or company with worthy technology, the spy can then concentrate on stealing all of their technology secrets. Computer security experts report that these targeted inventors can expect a continuing barrage of cyber-spy attempts, sometimes 50 per day, until their cyber security is penetrated.

Cyber-spying can be a lucrative business. Many private firms now exist that will cyber-spy for a contracted fee, no questions asked.

The only sure defense against such intrusions, many security experts say, is to unhook a secure computer from the Internet and transfer data in ways that will not be vulnerable to any Internet connection.

Mandated Revelations of Technology Secrets

The idea of a patent is simple. Someone has an idea for a new creation. If they will share fully their knowledge of it, society will grant them exclusive use for a limited time.

Until the fall of 2001, the Patent Office was required to keep secret all the details in a patent application. If it granted a patent, the information was made public. If the Patent Office rejected the request for a patent grant, it destroyed the application and the inventor could try again or use the creation as a trade secret.

The Patent Act of 1999 altered this 210-year relationship between inventors and society. It required the Patent Office to publish patent application 18 months after the earliest filing. The only exception was for those inventors who agreed not to seek a foreign patent.

Suddenly, the Patent Office was required to reveal to the world the inventor's secrets, including the best mode of creating it. In addition, if the patent was rejected, which now happens with about half of all applications, the inventor's

information became prior art available to anyone, anywhere in the world at no cost.

Since 2001, the Patent Office has made public massive amounts of information about applications that have not yet been processed. In the period FY 2001 through FY 2010, the U.S. Patent Office published more than 2.3 million patent applications. Of these about half came from U.S. inventors and companies and about half came from other nations that also require publication at 18-months after filing.

These mandated publication requirements make cyber-spying ridiculously easy. All another nation or foreign corporation need do is place engineers at a high-speed Internet terminal and have them harvest the technology disclosed as part of the patent process. In conducting this information gathering, the intruder can locate cutting-edge work by inventors, large and small, and then target them with cyber attacks designed to penetrate their computers.

While it is tempting to blame foreign corporations and governments for such technology theft, ultimately they are not responsible for our stupidity in making it so easy.

Secrecy and Export Controls

The Patent Office and numerous other Departments have a long experience that goes back to World War I in restricting the proliferation of technologies that might affect our national security and the issuance of secrecy orders that prevent vital technologies from slipping into the hands of those hostile to the United States.

Today, however, the USPTO lacks the ability to protect the economic security interests of the nation because it lacks the authority to refuse the grant of the license to file for a foreign patent on economically sensitive technologies. In a world in which the distinctions between military and civilian uses of technology are quickly disappearing, national and economic security is complexly entwined, often indistinguishable.

While agencies, such as the Commerce Department's Bureau of Industry and Security, the State Department, Homeland Security and the Defense Department, can impose export controls on economically sensitive technologies, the USPTO in effect undermines those controls by publishing the patent application, and later the patent itself, on the Internet. Many foreign producers can take this information and duplicate the technology. Thus, the United States loses export sales, even as it makes available to anyone in the world all the secrets of vital

technologies.

While the requirement that no patent or application subject to a secrecy order is to be published protects national security, economic security cannot be similarly defended because of the existing publication rules. It is a major gap in our economic and national security since so many technologies are dual use in nature. Any remedy is likely to require legislation. Certainly, it will require changes in present administrative procedures.

The issue is not one of agency or administrative failure at the Patent Office or any other federal department, but one of a structural gap created by the 1999 Patent Act. This gap merits immediate examination and would ideally focus upon creating:

1. The legal authority, rules and procedures for the USPTO and other agencies to screen applications for foreign filing licenses that implicate economic security concerns.
2. A unified package of criteria to be used by the USPTO and those screening export of economic security technologies, including a declassified version of the criteria that would be made publicly available.
3. More transparency in the process of screening patent applications for both national security and economic security concerns, including the publication of annual statistics on the number of secrecy orders and foreign export control filing licenses.
4. Arrangements with other nations that impose an 18-month publication requirement to permit some summary, such as the 150-word abstract that is part of each patent application, but reveal no details of the creation.

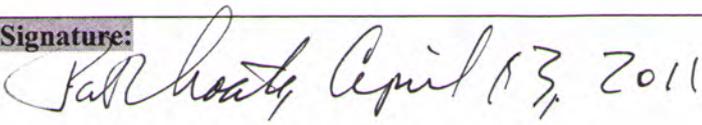
As events have repeatedly illustrated, America has enemies. In this hostile world, our economic security is as important as our national security, and increasingly the two are the same. The existing, unfocused publication policies are a fundamental threat to our security, national and economic, and this requires repair as quickly as possible.

Thank you, Mr. Chairman.

United States House of Representatives
Committee on Foreign Affairs

“TRUTH IN TESTIMONY” DISCLOSURE FORM

Clause 2(g) of rule XI of the Rules of the House of Representatives and the Rules of the Committee require the disclosure of the following information. A copy of this form should be attached to your written testimony and will be made publicly available in electronic format, per House Rules.

1. Name: Pat Choate	2. Organization or organizations you are representing: Mfg. Policy Project
3. Date of Committee hearing: April 15, 2011	
4. Have <u>you</u> received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?	5. Have any of the <u>organizations you are representing</u> received any Federal grants or contracts (including any subgrants and subcontracts) since October 1, 2008 related to the subject on which you have been invited to testify?
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
6. If you answered yes to either item 4 or 5, please list the source and amount of each grant or contract, and indicate whether the recipient of such grant was you or the organization(s) you are representing. You may list additional grants or contracts on additional sheets.	
7. Signature:  April 13, 2011	

Please attach a copy of this form to your written testimony.