A man uses his laptop in Beijing in January 2010. Cyber attacks are part of a shadowy campaign being waged from computers in China and other nations. Many of the attacks go undetected, according to Web security experts.

AGENCE FRANCE-PRESSE

Keeping the CYBER PEACE

THE EMERGING IMPORTANCE OF CYBER ALLIANCES IN THE ASIA PACIFIC

JOHN BUMGARNER

Cyber attacks are increasingly becoming a weapon of choice for extremists. Many of these incidents have affected countries in the Asia-Pacific region or their trading partners. In July 2009, a wave of Internet-launched strikes disrupted websites in the United States and the Republic of Korea. The following year, Japan's Defense Ministry and National Police Agency experienced similar assaults. In 2010, the government of Taiwan revealed that it is the target of about half a million cyber attacks every month, the majority of which originate outside the country.

Attacks on government computers were also reported in Australia, the Philippines and Vietnam in 2010. Furthermore, in December 2010, more than 200 websites, including that of the Central Bureau of Investigation of India, were attacked by so-called hacktivists.

These recent, high-profile cyber incidents have prompted many nations to re-examine their national security strategies for cyberspace. Compromises to cyber security in the Asia-Pacific region could have serious consequences not only for nations in this region but also for the rest of the world.

The increasingly global nature of the world economy makes the Asia-Pacific region more vulnerable to cyber attacks.

Several of the economies in the Asia-Pacific region, such as China and Japan, are some of the largest in the world, and many of the region's economies, such as Malaysia and Thailand, are growing exponentially. Many economies in the region are extremely vital to international trade. The volume of trade is significant, but so is the composition. Many of these nations produce intermediate goods as part of a global supply chain. In such a supply scenario, a disruption to production in one country can rapidly increase the scarcity of goods in other countries. The relative importance of countries in the Asia Pacific for international trade underscores the importance of preventing devastating cyber attacks against nations in this part of the world.

NEW VULNERABILITIES EXPOSED

The increasingly global nature of the world economy makes the Asia-Pacific region more vulnerable to cyber attacks. Many nations in this region supply the world with materials and equipment that are essential to critical infrastructure industries. A cyber attack in the Asia-Pacific region could interrupt the supply of these materials to the rest of the world or, perhaps worse, corrupt them. For example, the region is a large producer of electronic components that could be corrupted with malicious firmware during the manufacturing process. In this type of attack, the supply chain would be used to distribute the malicious programs or data structures throughout the world. The firmware could be designed to lie

Conservative activists in South Korea shout slogans as they hold anti-North Korea placards during a rally in Seoul in July 2009. The activists were denouncing cyber attacks from the North.

AGENCE FRANCE-PRESSE

dormant for years before disabling critical computer systems and other vital equipment without warning.

Financial markets are also vulnerable to cyber attacks, and financial markets in the Asia-Pacific region have been growing in significance. A disruption in these markets could adversely impact financial markets worldwide as investors react to a crisis. In theory, it is possible to launch a coordinated cyber attack against the computerized financial systems used by most countries. A properly planned and executed cyber campaign against these critical systems could cause significant monetary disruptions and possibly irreparable damage to the affected country's economy.

An international effort could help to prevent these kinds of disruptions. Firms in critical infrastructure industries must implement security measures to protect themselves and their trading partners from harm. But such measures will be effective only if contracts and standards can be enforced across national boundaries, which will require international agreements that are not yet in place.

Recovering from cyber attacks on critical infrastructure industries will also require international cooperation. No single country manufactures all of the components, supplies and know-how that would be required to remediate these industries after a major cyber attack. For example, the bulk electric power generators used in the United States are manufactured abroad, in France, Germany, Japan or Mexico. Some of the manufacturers of generators in these countries

depend on China for key manufacturing components. In addition, production facilities worldwide are limited, and inventories of bulk power generators are low, which presents logistical and political problems during periods of national crisis.

South Korean computer hackers compete during an information security olympiad at the National Assembly in Seoul in July 2009. South Korea's spy agency told lawmakers that the cyber attacks in July 2009 were carried out by using 86 IP addresses in 16 countries.

THE ASSOCIATED PRESS

EMERGING CYBER ALLIANCES

Several countries in the Asia-Pacific region have begun to improve their national cyber defense capabilities. A central element of these cyber defense initiatives is the establishment of a national cyber security organization. Some notable examples include Cybersecurity Malaysia and the Singapore Infocomm Technology Security Authority.

International cyber alliances could further improve the effectiveness of these national organizations. Cyber alliances would require members to collaborate on transnational cyber defense issues, such as securing national critical infrastructures, protecting strategic supply chains from cyber threats and assisting member nations in the recovery efforts associated with a catastrophic cyber attack.

Mutual assistance agreements are crucial to cyber alliances, in part because of the difficulty of preventing attacks. Mutual assistance could include actions that are relatively simple, such as providing emergency hosting services for government websites that have been disabled by a distributed denial-of-service attack. Mutual assistance could also involve key resources, such as providing replacement components for the electrical grid or critical infrastructures destroyed by a cyber attack. In the event of a cyber attack, national Computer Emergency Response Teams, or CERT, could form a Joint Computer Emergency Response Team, or JCERT, to coordinate predetermined actions taken as part of a mutual assistance agreement. The international teams could not only aid in host nation recovery efforts but also assist in forensic evidence collection actions. Many nations in the Asia-Pacific region already have well-established national CERTs that could participate in JCERT operations tied to a mutual assistance agreement.

CYBER EXERCISE AND COUNTERMEASURES

Once a cyber alliance is established, cyber exercises could be conducted to test the effectiveness of the alliance and its components, such as the JCERTs. Cyber exercises would involve all of the entities that are likely to be affected by a cyber attack or called upon to act in response to a crisis, including government officials and departments, private-sector companies, and international organizations. Cyber exercises can be designed to test international collaboration and cooperation. For instance, a recent Estonian exercise centered on an escalating cyber conflict. Throughout the Estonian exercise, government agencies had to coordinate their response to the crisis and share information with other countries and international organizations.

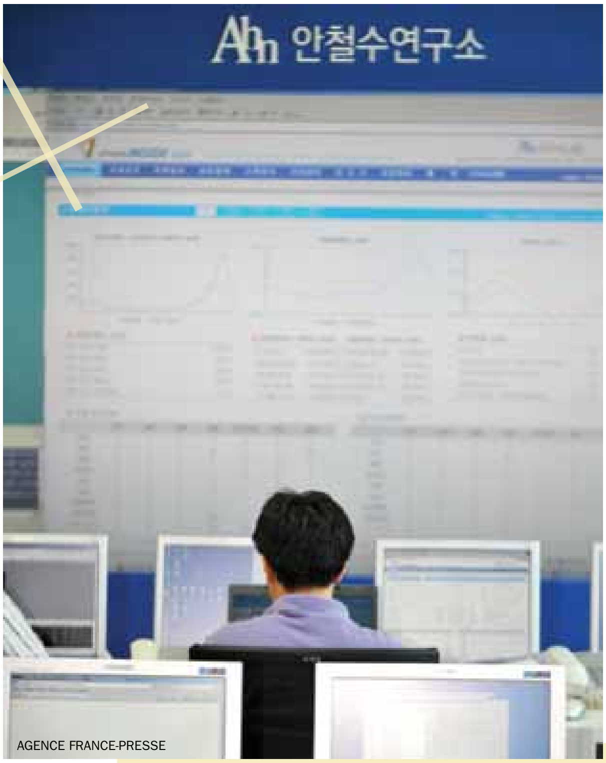
A cyber alliances would facilitate the sharing of cyber threat information among member nations in an expedited manner. Initially the more technologically advanced members of the alliance could establish an entity similar to NORAD, or the North American Aerospace Defense Command, that would be focused primarily on cyberspace threats. This collaborative threat matrix would allow individual alliance members to monitor their segments of cyberspace and provide advance warnings of impending cyber attacks to other members. Although warnings might not succeed in preventing attacks, they could potentially lessen the severity of attacks that do happen. In addition, these threat centers could provide ongoing international situational awareness to members, especially during heightened periods of cyber crisis.

As part of a cyber alliance, cyber peacekeepers could also be deployed to countries that experience ongoing cyber conflicts. Cyber peacekeepers could help to defuse cyber conflicts between disputing parties and aid in the peaceful resolution of the conflict. In the future, the United Nations will probably dispatch peacekeepers to monitor cyberspace peace agreements between disputing nations. Cyber alliances need to thoroughly explore the use of cyber peacekeepers within their sphere of influence and potentially in other nations when requested by the United Nations.

Establishing a framework for these cyber alliances in the Asia-Pacific region will require a thorough examination of existing regional and international agreements, pacts and treaties. The creation of cyber alliances raises new legal questions as well, especially for the mutual assistance agreements. One of the key legal questions that arose from the Georgian-Russian Crisis of 2008 was what action (for example, emergency Web hosting) by another nation (Estonia) constitutes material support for a foreign power engagement in war. Resolving such questions will require considerable foreign policy debate among alliance members and eventually at the United Nations. These obstacles are not insurmountable, however, and should not prevent the formation of cyber alliances.

In the 21st century, one nation's cyber security problems can become another country's concern almost instantaneously. This may be especially true in the Asia-Pacific region, which is a production hub for many critical infrastructure industries worldwide. Countries in this region can protect their national security interests by establishing cyber alliances with each other and with their trading partners. Several key elements needed to establish an effective cyber alliance already exist, but additional building blocks are needed to increase the resiliency of the Asia-Pacific region in the face of a cyber crisis. Several other features can be developed to increase the resilience of all nations in the face of a cyber attack. In the future, these cyber alliances will likely become just as important as other alliances have been in the past. □

John Bumgarner is chief technology officer for the U.S. Cyber Consequences Unit. He has served as an expert source for various publications, including *Business Week*, CNN, CBS, NBC, *Jane's Defence*, *The Wall Street Journal* and *The Guardian* in London.



AGENCE FRANCE-PRESSE

A South Korean security analyst for AhnLab Inc. conducts an investigation at the company's Security Operation Center in Seoul in July 2009. At the time, cyber attacks on South Korea were believed to have been mounted from 16 countries.