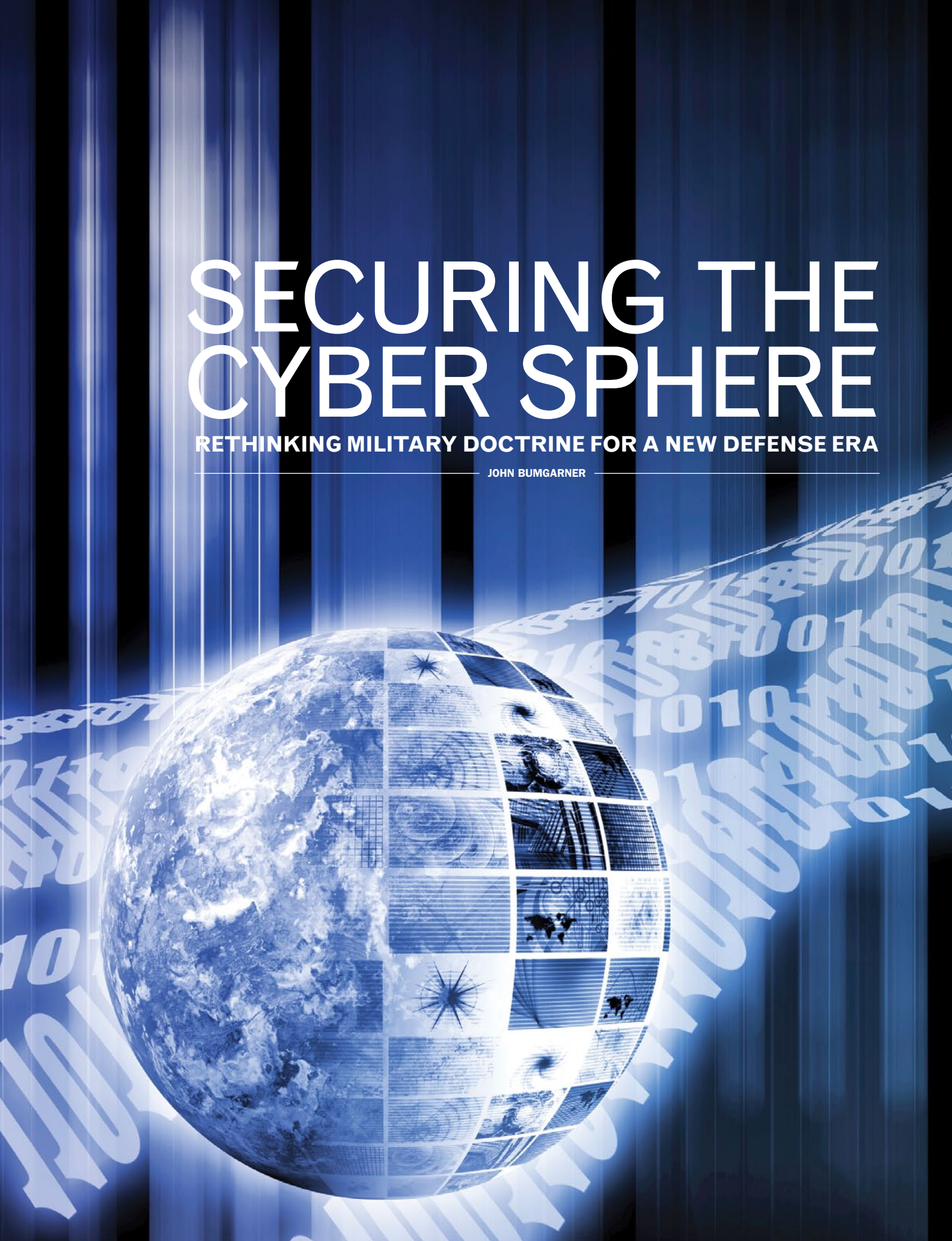


SECURING THE CYBER SPHERE

RETHINKING MILITARY DOCTRINE FOR A NEW DEFENSE ERA

JOHN BUMGARNER

"One must change one's tactics every 10 years if one wishes to maintain one's superiority."

Napoleon Bonaparte, 1769-1821

VEER IMAGES

Militaries have had to continually evolve over the past century to keep pace with advancements in weaponry and technology. Recent clamoring about the grave possibility of nations becoming entangled in cyber combat is once again forcing armed forces to rethink their battle plans for future conflicts. Operating in the cyber defense era, militaries will need to examine every aspect of their current doctrine to confront the challenges of the 21st century battlefield.

Many of the fundamental military strategies and tactics in use will need to be reshaped to take into consideration how technology can be applied in both conventional and asymmetric warfare. Additionally, nearly every military occupational specialty will require cyber-oriented training to meet the future challenges imposed by cyber warfare. Due to the anonymous nature, stealthiness and speed of cyber attacks, militaries will need to re-examine their decision processes linked to their customary response strategies.

Another essential part of these cyber defense era transformations will be the continual assessment of cyber threats against current weapon systems. All future weapon systems will need to be designed to limit their disruption or destruction from cyber attacks.

At a conference in February 2011, Sri Lankan Army chief Jagath Jayasuriya said the country still faces the threat of cyber war from sympathizers of the defeated Tamil Tiger rebels.

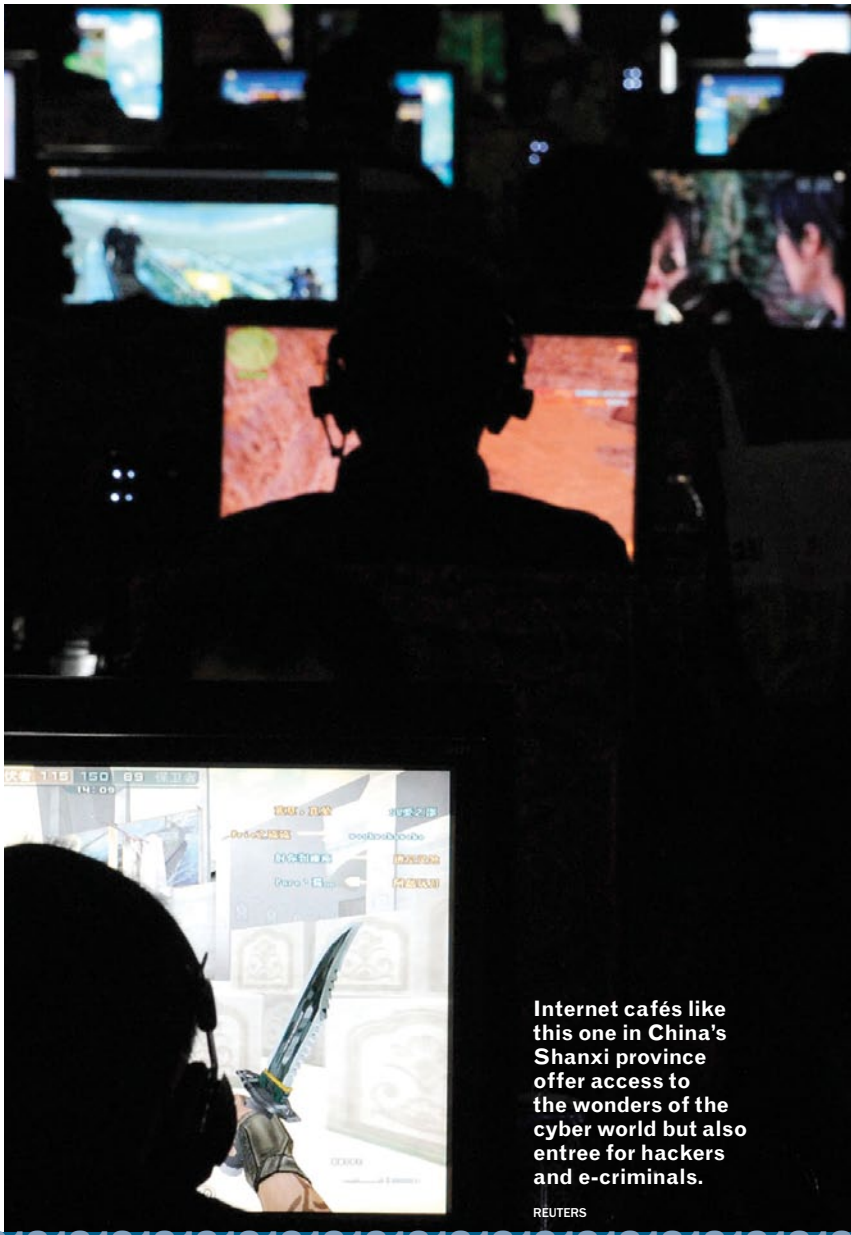
AGENCE FRANCE-PRESSE

BUILDING THE CYBER WARRIOR

During the industrial defense era, countries within the Asia-Pacific region developed their militaries to counter traditional threats in traditional spheres – air, land and sea domains. Over the past decade, several countries in this vitally important region have begun to develop capabilities to defend or advance their national interests in cyberspace, the newest domain of modern warfare. Some of the current groundwork under way in the region is the integration of cyber warfare units into existing military force structures.

For instance, the Republic of Korea established a cyber warfare unit within its military force structure in early 2010 to defend its military networks against cyber attacks and to provide offensive cyber capabilities. In 2011, the South Korean government announced its intention to establish and fund a Cyber War Department within a prestigious university. This new department will provide a technology-rich academic curriculum interwoven with courses in cyber war tactics and psychology. Its graduates will be required to serve seven years in the Republic of Korea Armed Forces as cyber war specialists. The military expects to have a fully operational cyber command by 2012.

Over the past decade, China has made remarkable progress in developing its military capabilities in all the domains of warfare including cyberspace. Historically, the Chinese military has not publicly acknowledged the existence of cyber warriors in its ranks, but the military recently confirmed the existence of an elite cyber warfare



Internet cafés like this one in China's Shanxi province offer access to the wonders of the cyber world but also entree for hackers and e-criminals.

REUTERS

Analysts at a U.S. cyber security center use a range of tools to identify and prevent potential cyber attacks.

REUTERS

unit called "Blue Team." The publicly declared mission of this cyber microforce is to assess the computer networks of the People's Liberation Army to uncover vulnerabilities that could potentially undermine military readiness. For many years, the People's Liberation Army has been developing cyber warriors through rigorous academic programs in important state-sponsored schools. Similar government-funded academic programs in the United States have proven effective in developing a cadre of talented cyber warriors.

Taiwan integrated cyber warfare capabilities with traditional military operations early on, as illustrated by the Han Kuang joint-forces exercise of 2000. During this exercise, thousands of computer viruses were unleashed by opposing elements in an attempt to paralyze the military command, control and communication networks. Since that exercise, Taiwan's military has continued to expand its cyber warfare capabilities through intense training and recruitment of cyber warriors into the armed forces.

Force structure changes are also occurring within the Indian Armed Forces. The current Singh government has directed the establishment of a national Cyber Command and Control Authority to assist the government of India with addressing the cyber challenges ahead.

ENHANCING SITUATIONAL AWARENESS

For these cyber warriors to be successful in real-world operations, they need to understand how a rapid decision cycle to counter cyber events can be applied to events when every nanosecond counts.

One of the key elements to accomplishing this is the development of in-depth situational awareness architecture in cyberspace. Developing a comprehensive framework is crucial for a military seeking to react quickly to unfolding incidents that could potentially provide an opponent with an advantage. The Japan Self Defense Forces recently held cyber warfare discussions with the countries of Australia and

Members of militaries from all over the world work together during the Cyber Endeavor exercise in September 2010 in Germany.

AIRMAN 1ST CLASS JEREMY BURNS/U.S. AIR FORCE

South Korea with the goal of developing regional cyberspace cooperation that could improve military situational awareness for all participants.

An integral component of any successful situational awareness program is the assessment of military weapon systems and other equipment (for example, tactical radios) for any known or unknown cyber-related vulnerabilities. The 21st century battlefield is littered with military equipment, such as main battle tanks, satellite communication architecture and unmanned autonomous vehicle battlefield surveillance systems that contain sophisticated electronic components that can be targeted by cyber warriors. The importance of these assessments is underscored by the discovery of various malicious computer programs in recent years. Some of these computer worms, or self-replicating malware, might have been discovered sooner if militaries had been performing regular cyber assessments. Militaries that fail to conduct these assessments throughout the lifecycle of any defense-related component could potentially overlook critical cyber sabotage vectors that enemy forces could utilize for an attack.

FUTURE SHOCK

The cyber defense era has the world in the midst of another revolution in military affairs. Future challenges will surely include: rethinking perimeter strategies to defend our ever-shifting cyber borders, revisiting counterinsurgency strategies to handle neo-combatants such as "technopatriots," re-evaluating intelligence collection in a rapidly expanding digital world, and re-examining the thorny problem of attribution in cyberspace.

The Asia-Pacific region will likely be the world's "proving ground" for much of the cyber warfare doctrine that will be developed and tested in the cyber defense era. □

John Bumgarner is chief technology officer for the U.S. Cyber Consequences Unit. He has served as an expert source for various publications, including *Businessweek*, BBC, CNN, *Jane's Defence Weekly*, Reuters, *The Guardian* and *The Wall Street Journal*.