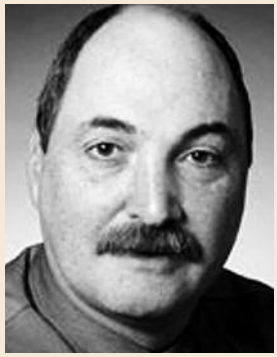
THE INTERNATIONAL ECONOMY
THE MAGAZINE OF INTERNATIONAL ECONOMIC POLICY
220 I Street, N.E.
Suite 200
Washington, D.C. 20002
Phone: 202-861-0791
Fax: 202-861-0790
www.international-economy.com
editor@international-economy.com

A SYMPOSIUM OF VIEWS

The New Cold War?

>>Is cyber security rapidly becoming the new cold war? As computer hackers, both state-sponsored and independent, seek illegal access to vital industrialized world networks for finance, utilities, and national security, to what extent could this new cold war disrupt the flow of global trade and finance? Do industrialized world governments need to rapidly transform their military capabilities, spending less on boots on the ground and more on fingers on the keyboard?

Seven experts offer their views.



The digital revolution created a golden age for espionage.

JAMES LEWIS
Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies

Cybersecurity's problems are not new. Every wave of innovation—steam, electricity, internal combustion—transformed business and warfare, created new risks, and, in their early incarnations, was remarkably unsafe for most users. The same is true for the networked digital devices that make up "cyberspace," the latest transformational technology.

Unfortunately, securing cyberspace faces more obstacles than did earlier innovations. These obstacles are political and conceptual, not technological. More than any earlier invention, digital technologies affect business and politics in direct ways that complicate and slow the process of building security. Many more participants assert expertise and claim a voice in any decision on cybersecurity. This is a confusing debate, marred by a reluctance to be bound by fact and by strident ideologies and self-interest.

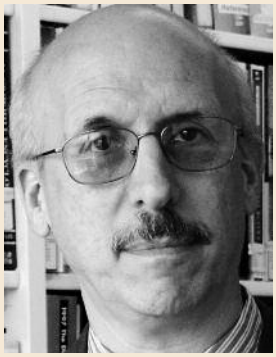
Old ideas—the internet is a "global commons" that must be open and free to empower innovation—do not withstand scrutiny and now resemble incantations more than analysis. Think about it: a place with no borders where governments have no role is an ungoverned space, making the internet a kind of digital Somalia. Another obstacle is the reluctance of the "internet community" to admit that global networks have become a mature infrastructure, critical for business and security, and require more than amateurish "governance" by technicians.

All technological revolutions arrive with hype, but this one is more afflicted than others. Cyberwar epitomizes this. Cyberattacks will not cause existential destruction like nuclear war. Cyber is a fast, long-range weapon, but with a limited destructive payload. Cyber can provide military advantage, but by itself, it is insufficient to defeat a determined opponent. The real challenge for cyberwar is deciding how to incorporate cyberattack into existing military doctrine and into the framework of international laws that govern conflict.

There have been remarkably few real cyberattacks. Most of what we see is espionage, directed by states, often using proxies. The digital revolution created a golden age for espionage. China is a leading beneficiary. Since the decision to open its economy, its policy has been to illicitly acquire technology to catch up with or surpass the west. Cyber espionage is slowly shifting the terms of trade in China's favor, but it is not death by a thousand cuts nor more costly than the drug trade. China's reluctance to change its behavior is troubling, but the current approach, which is to wring hands without taking action, will not persuade China or others to change.

Iran's recent behavior is more disturbing. Iran has basic cyberattack capabilities and used them against Aramco, RasGas, and several large U.S. banks. Data was erased from thirty thousand Aramco computers. The banks suffered less, but Iran's actions led the Secretary of Defense to announce a new U.S. doctrine that would preemptively intervene against truly damaging cyber attacks.

So the world has a new infrastructure upon which it now depends. Countries, groups, and individuals can acquire the means to attack it. The technology is still primitive and governance still undeveloped. This is not a new challenge. Nations found ways to make earlier technologies safer and more secure. To do the same for cyberspace means abandoning old ideas and giving states their normal role in law enforcement, trade, and defense. It has been a slow start but the way ahead is becoming clear.



Cyber operations can supplement a war, but they cannot be the war.

MARTIN LIBICKI
Senior Management Scientist, RAND Corporation, and author,* Cyberdeterrence and Cyberwar *(RAND, 2009)

The Cold War was, in large part, about weapons of mass destruction. Today's hand-wringing over the villainies certain to visit us in cyberspace is primarily about weapons of mass distraction.

Despite nearly twenty years of predictions, the total physical damage from cyberattacks so far has been low compared even to the smallest of real wars. No one has

died. Very little machinery has been broken. One exception, Stuxnet, was a concentrated effort by first-rate cyber powers focused on a nuclear enrichment facility managed by a third-rate industrial power (Iran) with scant mastery of the process, a jerry-rigged collection of black- and gray-market parts, and very little help from the outside world. Extrapolating such limited success (80 percent of the centrifuges survived the attack) into a Cold War II is more than a bit of a stretch. What appear to have been revenge attacks against U.S. banks in September deprived bank customers of online access—an annoyance, to be sure—but the perpetrators have not managed to penetrate banking systems or challenge the integrity of the financial system. This kind of war we can survive easily.

Granted, a great deal of espionage is carried out in cyberspace. It seems safe to say that if your internet-connected systems have something of interest to a state intelligence agency, it's probably not a secret anymore. But espionage is not war—and claims that China's cyber espionage constitutes the most serious threat to the U.S. economy are grossly exaggerated. After all, the theft of information does not necessarily deprive its owner of the information's use, and it would be easy enough to exaggerate the value it affords to the thieves. Technology transfer is hard enough when the exchange is mutually agreed upon; it is significantly harder when the primary means of exchange is theft of files with no context.

As for cyberspace, as a medium of war, if you have no networks you cannot play, either as an attacker or (not to put too fine a point on it) as a victim. By contrast, lacking an army, navy, air force, or satellite constellation hardly keeps one from being victimized by someone else's army, navy, air force, or space assets. Thus, there are real limits to how much damage U.S. cyberwarriors can inflict against low-tech countries (or at least those who do not acquire systems before they understand how to protect them).

The U.S. military, with its high-tech systems, must protect itself from cyber threats with much the same careful management that protects it against vulnerabilities associated with, say, explosives. But there can be no choice between boots on the ground and fingers on a keyboard. A military that scrimps on firepower will have no way to exploit the temporary confusion that its hackers can cause to the other side. In other words, cyber operations can supplement a war, but they cannot be the war.

Our cyber-insecurities are nothing like the Cold War.

JIM HARPER
Director, Information Policy Studies, Cato Institute

It's easy to forget what the Cold War was like. Generations of children thought that a silent, blinding flash of light would signal their annihilation. In this most important respect, our cyber-insecurities are nothing like the Cold War.

There are parallels between cybersecurity and the twentieth-century rivalry between the United States and Soviet Union. We have a military gunning to protect us. Our political class has only one frame of reference: geopolitics. And, like the cold war, this one won't ever turn hot—unless we let our leaders use "cyber" as a pretense for dropping real bombs.

Let's assess the risk of cyberattack, not by going saucer-eyed about vulnerabilities, of which there are many, but by focusing on threats: Who plans to attack global trade and finance or nation-states? And what do they stand to gain?

A minor power's cyberattack on a major one would be a losing proposition. The upside is modest, strategically insignificant, damage to the victim. Cyber assets are easily restored and kinetic damage is hard to produce with computers. The downside is retaliation—disproportionate retaliation.

When you strike at a king, you must kill him. No small state is going to (literal) war against a major power using the internet.

What about non-state-sponsored cyberattacks? Any response would simply produce collateral damage and new enemies. We can't use cyberwarfare to punish or dissuade these actors. Why develop the capability?

Happily, non-state actors can't pull it off. The head of the National Security Agency, General Keith Alexander, said at an American Enterprise Institute event in July that al Qaeda doesn't pose a cyberthreat.

The actors that are both sophisticated enough to produce serious cyberattacks and strategically positioned to use them are the industrialized world's governments—our governments. The Stuxnet virus, which interrupted Iran's weapons program for a time, is a rare example of a cyberattack that caused physical damage. It is widely cred-

ited to the United States and Israel. Cyberwar is something we're doing to them. It's not the other way around.

Successful though it was at exploiting interlocking and previously unknown vulnerabilities, Stuxnet and more recent successors may have propagated knowledge about attack techniques, making the world less safe for the time being. The U.S. government and other large powers may be hoarding vulnerabilities and cultivating new attacks rather than contributing to worldwide security by helping to close gaps in vulnerable technologies.

The true pro-security policies are quite a bit different than what we've seen—and less interesting. The world's powers could be less cyber-bellicose. The bulk of the security gains to be had are achieved simply, and boringly, by patching software.

The threats that remain are serious, but nothing like the threat of war: graffiti-like denial-of-service attacks; corporate and governmental espionage; crime; and insider attacks, whether cultivated by competitors or just the product of disgruntlement.

American founder Elbridge Gerry called a standing army "the bane of liberty." We needn't have one on the internet.

The rising importance of cyberspace changes rather than eclipses traditional elements of national security.

PATRICK M. CRONIN
Senior Advisor and Senior Director of the Asia-Pacific Security Program, Center for a New American Security

Cyberspace distinguishes security in the twenty-first century from security in all previous centuries. But the rising importance of cyberspace changes rather than eclipses traditional elements of national security.

Cyberspace is one of four domains (along with maritime, air, and outer space) that define the global commons. Computers are ubiquitous and help connect the world through a finite and vulnerable network of satellites, thin fiber optic cables, and other physical infrastructure. The ability to rapidly move massive amounts of information around the globe simultaneously spurs productivity and wealth, and introduces huge opportunities from crime, espionage, sabotage, and acts of war.

Consider how cyberspace is transforming security in the dynamic Asia-Pacific region. Among the major threats that could upset general prosperity in the region are nuclear North Korea's provocations and rising tensions in the South and East China Seas. There is no doubt that cyberspace adds levels of complexity and danger across both of these challenges.

North Korea, which practices brinkmanship and likes to exploit gray areas, sees cyber warfare as giving it the kind of asymmetric capability it needs to deal with a more powerful outside world. North Korea seeks to exfiltrate South Korean and other electronic secrets, and it apparently interfered with the vital Global Positioning System used by commercial flights in Seoul. U.S. Army General J.D. Thurman, commander of the Combined Forces Command in Korea, is rightly concerned that Pyongyang might resort to a spectacular cyberattack for a future provocation. After all, the 2010 sinking of the South Korean naval ship *Cheonan* required a weeks-long international investigation to demonstrate that North Korea instigated the attack, and even then some were not completely convinced. The attribution of who is behind any given cyberattack is difficult to prove.

Mounting territorial tensions in the South China Sea and East China Sea could well escalate into outright war. These threats would exist regardless of the rapid rise of cyberspace, but it is significant that leading claimant states (including China, Taiwan, Japan, the Philippines, Vietnam, and others) and major actors such as the United States are investing an increasing percent of defense budgets in C4ISR technologies for command and control and intelligence. They are also expanding training for amphibious operations, and it is noteworthy that the U.S. Marine Corps is spending more to buy cheap, lightweight, off-the-shelf equipment for both cyber and electronic warfare. While these investments are only partly related to maritime tensions in and near these seas, they are related.

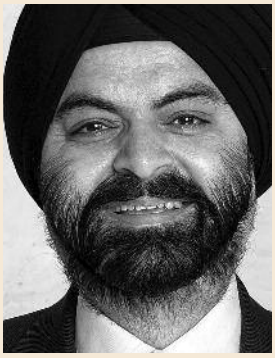
China's integration with the global economy means that virtually all countries wish to trade with China. But it also means that the United States and its major allies want to ring-fence off certain areas vital to national security, especially those related to cyber space. Australia stopped Chinese telecom Huawei from bidding on its national broadband system, and recently a committee report out of the U.S. House of Representatives accused Chinese telecoms as potential conduits for spying.

At the same time, militarily China's People's Liberation Army is rapidly modernizing its traditional arsenal, adding its first aircraft carrier, expanding its submarine fleet, and building fifth-generation aircraft. It is also perfecting longer-range anti-ship ballistic missiles as part of an anti-access and area denial capability aimed at the U.S. armed forces. U.S. Secretary of Defense Leon Panetta's admonition that we could one day face a "cyber Pearl Har-

bor" suggested how China (as well as less capable states or even non-state actors) could seek to hurt the United States in myriad ways through a cyberattack.

That's one reason why the United States set up a U.S. Cyber Command to help protect our armed forces operating in cyberspace. But if some future foreign leadership were to contemplate a crippling cyberattack, it would be more likely to be deterred by traditional defense systems and diplomacy, and not through some nonsensical notion of cyber deterrence.

Cyber warfare tools—both defensive and offensive—alter how traditional military systems are used, but they are no substitute for ships, planes, and soldiers.



Cybercrime is becoming increasingly complex and international in nature.

AJAY BANGA

President and Chief Executive Officer, MasterCard Worldwide, and Chairman, Information and Technology Committee, Business Roundtable

There was a time in the recent past when the average citizen of an industrialized nation thought little about the mechanics or infrastructure of information systems—how and why things like the internet, payment card networks, and the electrical grid work, and who makes them run.

In the twenty-first century, the global economy is coded in zeroes and ones. Sophisticated information systems are now embedded in every facet of our daily lives. Whether an electronic payment card transaction or a smartphone search for a restaurant, nearly everything we do depends on the secure operation of information systems.

Our global interconnectedness has made the world smaller and more accessible, but it has also paved the way for new types of criminal activity. Cybercrime today is becoming increasingly complex and international in nature, exposing us to attacks from hackers, industrial spies, terrorists, and criminals.

The variety, scope, and scale of cyberattacks is increasing monthly, imposing staggering costs. According to a recent study, the annual cost of global cybercrime is $114 billion.

Global businesses, which own and operate many of the most valuable information systems, are the first line of defense against cyber security threats. Chief executive officers take this responsibility seriously. We have integrated cyber security into the way we manage our companies and conduct our operations. But we need to coordinate with governments to access the resources that only they can provide.

Here in the United States, business leaders have called upon Congress and the Obama Administration to enact smart cyber security policies that facilitate new levels of domestic and international collaboration—especially for cyber events that target critical services supporting the world's economy and security. These policies include technical support essential for protecting global corporate assets against cyber threats and greater international cooperation in bringing cyber criminals to justice.

Prescriptive government mandates will not work, nor will a response driven only by private industry. Threats change so rapidly that solutions are often obsolete before they can be implemented. Inflexible mandates and unilateral programs don't fit the reality of privately owned information systems and rapidly evolving threats.

Cyber security is a critical component of economic and national security around the world. It is also a necessary foundation of future prosperity and opportunity. Governments need to make effective cyber security—based on flexible, collaborative, and responsive public-private information sharing partnerships—an urgent national priority.

Our collective future depends on it.

China has erected a formidable cyber warfare capability over the past decade.

ILAN BERMAN

Vice President, American Foreign Policy Council

In late October, speaking at the Intrepid Museum in New York, U.S. Secretary of Defense Leon Panetta delivered a stark warning. The United States, Panetta said, could soon face a mass disruption event of catastrophic proportions, a "cyber Pearl Harbor" of sorts.

"An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches," cautioned the Defense secretary. "They could derail passenger trains, or even more dangerous, derail trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country."

Such a scenario is grim, but it is entirely feasible. The past quarter-century has seen a profound transformation of virtually every aspect of American society as a result of the internet. But with the popularity of the worldwide web has come the proliferation of new threats to U.S. security emanating from it.

Of these, the most prominent is China. The People's Republic has erected a formidable cyber warfare capability over the past decade—one that it has used to carry out espionage against the United States on a massive scale. And if Washington and Beijing ever come to blows (over Taiwan or some other issue), there's good reason to believe that cyberspace would be part of China's strategy of "unrestricted warfare."

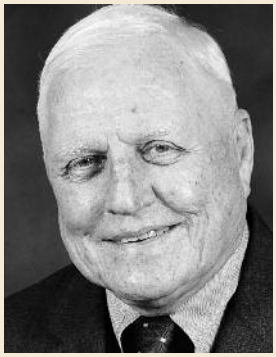
Russia is also a distinct cyber danger. In recent years, the Kremlin has exploited cyberspace to decisive effect in its dealings with both Estonia and Georgia, and government-linked cyber activists have helped suppress and silence the country's political opposition. Russian criminal enterprises, meanwhile, have moved online en masse, where they have begun targeting foreign marks—American financial institutions among them.

A newer, and more unpredictable, cyber foe is Iran. Recent attacks on U.S. financial institutions and Middle Eastern energy firms have served notice of the Islamic Republic's growing capabilities in cyberspace. They are also a foretaste of what could happen if the deepening international standoff over Iran's nuclear ambitions results in outright conflict.

Beyond Iran, a range of other actors—from North Korea to al Qaeda—all have demonstrated a growing desire to act, and act aggressively, in cyberspace.

America's response to these challenges is still a work in progress. Movement toward a comprehensive strategy for cyberspace has fallen victim to election-year politics in Congress, where several such plans now languish. U.S. military doctrine, meanwhile, remains ambiguous as to what exactly constitutes an act of war in cyberspace, and what America can and will do in response. U.S. cyber strategy, in the words of one expert, "is akin to where anti-terror efforts found themselves shortly after the attacks of 9/11."

That represents a dangerous deficiency. Warfare of the conventional variety is certainly not a thing of the past. But it's impossible to ignore the fact that cyberspace is emerging as a new domain of conflict—and that America's adversaries are increasingly active in it. Washington needs to be prepared to fight there as well.



Attempts to define the national interest in ICT are confused and contradictory.

CLAUDE BARFIELD
Resident Scholar, American Enterprise Institute

Certainly governments need to beef up their cybersecurity capabilities. As for the exact balance between this and boots on the ground, I leave those complicated decisions to defense experts. Rather, I'd like to put the spotlight on implications for U.S. trade and investment policy—and on our fraught relations with the People's Republic of China. Information and communications technology (ICT) occupies a no-man's-land between national security imperatives and international economic policy—and requires disparate and even conflicting calculations of U.S. national interest. At this point, attempts by U.S. government agencies to define the national interest in ICT are confused and contradictory.

Specifically, the United States vociferously espouses a policy of open inward investment, as programs such as Washington's USA Invest attest. According to an Asia Society report, the People's Republic of China will have upwards of a trillion dollars to invest abroad by the end of the decade, and a good portion may come here, boosting jobs and the economy.

Yet U.S. officials have on notable occasions rebuffed attempts by a major Chinese telecoms company—Huawei—to invest and/or obtain contracts in this country. In several instances, this has been done through *ex parte* interventions that belie the rule of law and due process we preach to the Chinese. Recently, the chairman and ranking members of the House Intelligence Committee, after a year-long investigation, issued a scathing indictment of the company, stating that Huawei (and its sister company ZTE) pose national security threats to the United States and warned U.S. companies not to do business with them if they valued U.S. national security. Though they referred vaguely to classified information, the report itself presented no evidence that either company had spied for China or secretly spiked their equipment with so-called Trojan horses. This led *The Economist* magazine bitingly to conclude that the investigation seemed "written for vegetarians. There is not much meat in it."

Then on October 17, a Reuters team broke the story that the White House had conducted a much more extensive investigation—enlisting U.S. intelligence agencies and interviewing a thousand telecoms buyers. The headline: "White House review finds no evidence of spying by Huawei." One investigator told Reuters: "We knew certain parts of the government really wanted" evidence for active spying. "We would have found it if it were there." The White House refused to confirm or deny the details of the story—which nevertheless is almost certainly true in most detail.

With the election over and fears of being "soft on China" less urgent, the Obama Administration should quickly move to bring some clarity to U.S. investment and security policy for telecommunications. It could declare the entire telecoms industry off-limits to foreign investors (a bad idea but an option). It could not, however, simply exclude Chinese companies alone without running foul of bedrock WTO rules for nondiscrimination. It could establish less draconian rules for telecoms investment and contracting by all foreign companies. On this course, it would admit that given the fact that the U.S. market cannot be sealed off—and that Huawei and ZTE operate in 150 other countries—the time has come to allow Chinese companies into the U.S. telecoms market, while mandating stepped-up cybersecurity operations by both the private sector and government agencies.