CYBER DETENTE BETWEEN THE UNITED STATES AND CHINA

SHAPING THE AGENDA

EastWest Institute
Forging Collective Action for a Safer and Better World

Cover image by Dragan Stojanovski

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused solely on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, and Moscow. For more information about the EastWest Institute or this paper, please contact:

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
1-212-824-4100
communications@ewi.info

www.ewi.info

CYBER DETENTE BETWEEN THE UNITED STATES AND CHINA: SHAPING THE AGENDA

Greg Austin and Franz-Stefan Gady

EastWest Institute
Forging Collective Action for a Safer and Better World

EXECUTIVE SUMMARY

In May 2012, the United States and China agreed publicly for the first time to begin talks on military aspects of cybersecurity. The agenda and expectations for this process at the official level remain to be set. Through Track 2 processes some very useful preparatory work has taken place, but for now, as analysts on all sides agree, the diplomacy—both official and unofficial— needs to be more intense, to cover more concrete problems and to involve a larger number of people on both sides, especially from the military and private sector. Since this is a policy arena where both countries are at odds and where neither has fully formed definitive positions on all issues, a closer examination of some the key potential agenda items is appropriate. This paper looks briefly at two sets of issues that have, to date, received scant attention in bilateral conversations:

1. Clarifying the mix between offense, defense and preemption in the military cyber policies of the two countries;
2. Understanding the degree of interdependence between the United States and China in cyberspace and its impact on strategic deterrence.

The dialogues need to shift from discussion about cyber warfare as if it were a stand-alone set of operations to a discussion of the impact of advanced cyber capabilities on strategic capability and intent in the broad sweep of the relationship between China and the United States.

The challenge is to deepen the conversations and reduce mistrust through enhanced transparency and predictability. The two governments must play a leading role in these conversations, but the tempo of official engagement on these issues has been so slow that they should probably not be allowed to set the pace. The diplomatic costs have been too high due to the slow pace of bilateral conversations. Track 2 organizations need to continue to stimulate more robust and more frequent exchanges of opinion by officials on the military aspects of cyber strategies. Moreover, the potential economic impact of continued delay in addressing the divisive strategic issues may lead to a deeper and unsatisfactory co-mingling of private sector and military interests in cyberspace. We should have no illusions that the two countries will agree quickly to a set of military confidence building measures in cyberspace, but there is some room to lay the foundations to begin to bridge the bilateral divides by addressing issues that are closer to the civilian domain rather than exclusively military.

This paper has three specific proposals:

- The United States and China should agree on a joint public study on the interdependence of their respective critical information infrastructure in terms of likely economic effects of criminal attacks with strategic impacts.
- The United States should work to include China in the existing infrastructure of the 24/7 Network of Contacts for High-Tech Crime of the G-8. The aim is to strengthen cooperative mechanisms at the international level that distinguish acts by criminals from acts by states.
- The two countries need some common understanding of cyber espionage. Since the main problem is about blurred boundaries between national security espionage and theft of intellectual property for commercial gain, a sustained policy dialogue between officials should be possible.

Shaping the Agenda

For both sides, cyberspace encompasses the entire fabric of strategic command and control and intelligence dissemination on which the national military security depends.

Introduction

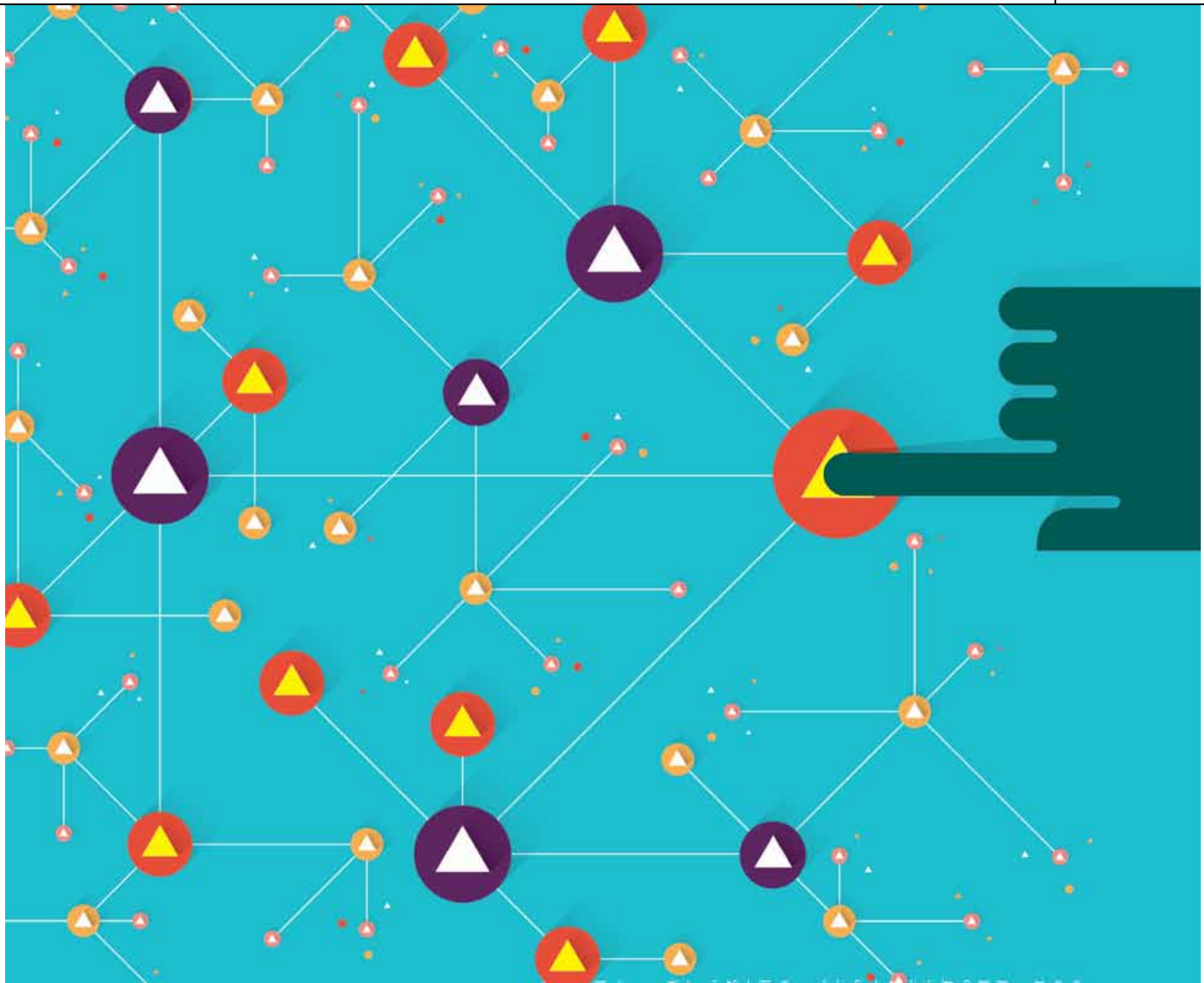
The United States and China are adversaries in cyberspace at a more serious level than in any other field. Some observers disagree, arguing that cyber weapons are only a tool, not the main source of divisions on a par with issues like Taiwan and Tibet. But the authors of this paper feel that the emotions for the cyber confrontation are newer and more raw. Moreover, the diplomacy for cyberspace is far less developed and less predictable than the diplomacy surrounding Taiwan and Tibet, which plays out in routine, predictable patterns.

For both sides, cyberspace encompasses the entire fabric of strategic command and control and intelligence dissemination on which national military security depends. It also encompasses all other digital systems in use that affect military preparedness, including those in critical civil infrastructure. Cyberspace is not a single domain of warfare like air, land, sea or space, but involves the entire fabric of command authority over all of these domains, including strategic nuclear weapons. United States cyber commands at national- and single-service levels are responsible for the full spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions, including in space. Since all military operations, except for the lowest level tactical operations, are now controlled by digital communications, the capacity of one side or the other to dominate in cyber warfare seriously exacerbates existing mistrust between the two sides.

Moreover, both countries appear to have preemptive aspects to their cyber war strategies or operational doctrines that may affect nuclear and conventional force deterrence. In addition to massive use of cyber-based espionage activity, each is engaged in cyber probes directed against network and data integrity of the other, across a wide range of military, scientific, political, economic and social targets.[1] These probes are seen by each as a direct threat to the economic or military security of the other.

U.S. intelligence officials maintain that their government's cyber espionage activities are conducted exclusively for national security purposes. They also claim that Chinese state-sponsored espionage includes commercial espionage, with the state directing large-scale economic spying that targets intellec-

1 For documentation of Chinese espionage against the United States, see United States, Office of the National Counter Intelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011", October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. There are no similar sources available in public that document United States cyber espionage against China. The authors' information on this is based on discussion with senior United States and Chinese officials and specialists.



This paper offers an assessment of where the two countries sit on the adversary/partner spectrum in cyberspace and where they are heading in this climate.

tual property, pricing positions and market data. Both sides feel they see enough of the other's activities in cyberspace to make them worry, but not enough to have a complete picture. In both instances, there is little appreciation of the politics of cyber military postures—largely because these are not fully formed in either country.

In January 2010, McAfee CEO Dave DeWalt noted that some 20 countries seemed to be involved in a cyber arms race.[2] He cited a survey commissioned by McAfee of approximately 600 IT executives worldwide, which showed that 60 percent believed that most attacks were government initiated, with roughly equal numbers (36 and 33 percent respectively) viewing the United States and China as the main perpetrators.

The U.S. government, legislators and private sector leaders have put China on notice, expecting a very different pattern of behavior from China.[3] An unclassified intelligence report argues that China is "the world's most active and persistent perpetrator of economic espionage."[4] By comparison, Beijing has not been as outspoken about its perceptions of Washington's offensive cyber posture.

In January 2011, the subject of cybersecurity appeared in a U.S.-China Head of State communiqué for the first time—a full 14 years after it first appeared at a similar level in U.S.-Russia relations. Even then, the reference was a passing one, mentioned among a number of global issues on which the two countries would work jointly. By early May 2012, the two countries had broached this topic seriously in the annual bilateral Strategic Security Dialogue, (under the Strategic and Economic Dialogue at the cabinet minister level). Not long after that meeting, Chinese Defense Minister General Liang Guanglie and U.S. Defense Secretary Leon Panetta struck a new tone during a joint press briefing in Washington.[5] Panetta backed up Liang's statement that the two sides had agreed to look for ways to cooperate on cybersecurity.[6] "It's extremely important that we work together to develop ways to avoid any miscalculation or misperception that could lead to crisis in this area," Panetta said. He added that he appreciated the "general's willingness to see if we can develop an approach to having exchanges in this arena in order to develop better cooperation when it comes to cyber."

This paper offers an assessment of where the two countries sit on the adversary/partner spectrum in cyberspace and where they are heading in this climate. It gives some further suggestions for an agenda for this official bilateral cybersecurity exchange and for the Track 2 diplomacy that must support it.

Cyber Detente Goals Are Clear, the Agenda and Expectations Are Not

The unresolved dilemma in relations between the United States and China on cyberspace issues flows from the tension between each country's needs to secure its military power relative to the other and the need for each to work together to protect high-level economic interests, especially from cyber crime. Since, as former Secretary of State Henry Kissinger has implied, neither the United States nor China is ready to view the other in less than adversarial terms in cyberspace, any moves toward cooperative activity have to be aimed more at detente (tension reduction and con-

2 See Hui Min Neo, "China, US, Russia in cyber arms race: net security chief", AFP, January 28, 2010, citing a speech by DeWalt at the World Economic Forum at Davos. See the associated report, "Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare", McAfee, Santa Clara CA, 2009.

3 See for example, the speech by former United States Ambassador to China John Huntsman, who in his presidential campaign observed on August 11. 2011: "This is also part of a dialogue that has not taken place with the Chinese. We need a strategic dialogue at the highest levels between the United States and China. That is not happening."

4 United States. Office of the National Counter Intelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011", October 2011, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

5 United States, Department of Defense. "Joint Press Briefing with Secretary Panetta and Gen. Liang from the Pentagon", May 7, 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5027.

6 The transcript of the press briefing by the two defense leaders contains references to other occasions when Liang had raised the issue. Transcript, Joint Press Briefing, The Pentagon, Washington DC, May 7, 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5027.

fidence building)[7] than at any more elaborate form of arms control. Neither China nor the United States is interested in the latter even though officials on both sides mention it from time to time.

Notwithstanding the U.S. government's measured official declarations on this issue, the mood in private is inflamed. The atmospherics were well captured in an article by Richard Clarke on April 15, 2011: "If we discovered Chinese explosives laid throughout our national electrical system, we'd consider it an act of war. China's digital bombs pose as grave a threat."[8] A similar tone was struck by two former senior officials in an article on cyber espionage, headlined "China's Cyber Thievery Is National Policy—and Must Be Challenged." They warned of "the catastrophic impact cyber espionage could have on the U.S. economy and global competitiveness over the next decade."[9]

Yet, as the statements of the defense ministers of the two countries in May this year indicate, the official position of both the United States and China is one of cyber detente. The case for this was put particularly forcefully in presentations by Kissinger and former U.S. Ambassador to China Jon Huntsman on June 14, 2011.[10] Huntsman said: "At some point, we are going to have to develop a context in which we can actually discuss this and, I would think, draw some red lines around areas that we don't want them into and they might not want us into."

The mutual commitment to cyber detente by both sides is clear. The agenda, however, is not so clear. There is not even basic agreement about the appropriate cooperative model for the process. Should it be informed by the detente and arms control models that were so prominent in the Cold War, or are other models appropriate? Do existing international conventions and customary norms govern cyber conflict, or do we need new legal arrangements for ensuring international peace? Has the traditional security relationship between states like China and the United States been fundamentally transformed by the cyber era? Has the control of key national security assets been partially transferred to the private sector as a result of the latter's dominance of cyber infrastructure?

China and the United States disagree on the practicalities of cyber policy at almost every level, notwithstanding their symbolic commitment to shared values on issues like cyber crime, especially the protection of children in cyberspace.[11] With respect to cyber crime, the two countries have a shared commitment to bring perpetrators to justice, and there are success stories in that cooperation. Nevertheless, there are even substantial policy differences between them in this area. For example, Chinese officials complain in private how difficult it is to get the United States to agree to extradition of people in the United States suspected of cyber crime under Chinese law. The United States has consistently criticized China, as would be expected, for its policies that constrain Internet freedom.

On the other hand, the growing integration of the Information and Communications Technologies (ICT) sectors of both countries, in circumstances of the globalization of supply chains, capital and labor, has meant that both governments are well behind the curve when it comes to developing new bilateral policies in cybersecurity. The two countries have been linked (beyond trial connections) to the Internet since 1995. Since 2002, when Microsoft became the first foreign company to be admitted to the Chinese Software Association, there has been a deep integration of the ICT sectors, with U.S. corporations now among the parties consulted in the drafting of China's regulations in the ICT sector. Yet by mid-2012, the two governments have only rudimentary frameworks for joint man-

China and the United States disagree on the practicalities of cyber policy at almost every level, notwithstanding their symbolic commitment to shared values on issues like cyber crime, especially the protection of children in cyberspace.

7 See Paul Eckert and Daniel Magnowski, "Kissinger, Huntsman: U.S., China need Cyber Detente", Reuters, 14 June 2011, http://www.reuters.com/article/2011/06/15/us-china-kissinger-cyber-idUSTRE75D62Q20110615.

8 Richard Clarke, China's Cyberassault on America", *Wall St Journal*, June 15, 2011, http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html?mod=googlenews_wsj.

9 Mike McConnell, Michael Chertoff and William Lynn, "China's Cyber Thievery Is National Policy—And Must Be Challenged," *Wall St Journal*, January 27, 2012, http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html.

10 See Paul Eckert and Daniel Magnowski, "Kissinger, Huntsman: U.S., China need Cyber Detente", Reuters, June 14, 2011, http://www.reuters.com/article/2011/06/15/us-china-kissinger-cyber-idUSTRE75D62Q20110615.

11 One of the best examples of shared values in cyber space between the United States and China is the Lima Declaration of APEC Telecommunications Ministers, See http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2005_tel.aspx.

Dan Page

agement of cybersecurity issues. They have only recently begun to develop comprehensive international policies in this field. In May 2011, the United States issued its first comprehensive "International Strategy for Cyberspace".[12] The paper identified the following policy priorities:

- Economy: Promoting International Standards and Innovative, Open Markets
- Protecting Networks: Enhancing Security, Reliability and Resiliency
- Law Enforcement: Extending Collaboration and the Rule of Law
- Military: Preparing for 21st Century Security Challenges
- Internet Governance: Promoting Effective and Inclusive Structures

12 United States, The White House, "International Strategy for Cyberspace", May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

- International Development: Building Capacity, Security and Prosperity
- Internet Freedom: Supporting Fundamental Freedoms and Privacy.

In the sections that addressed military policies, the United States did not canvas the idea of cyber detente, but rather the need to work with allies for maximum deterrence of potential adversaries. It did recognize the value of diplomacy in working towards mutual peace and prosperity in cyberspace. To the extent that unanimity exists in the U.S. government on key issues of international cybersecurity strategies, these are quite different from the Chinese position.

For example, in September 2011, China, Russia and two other countries tabled a proposal at the UN called an "International Code of Conduct for Information Security."[13] Later, a Russian newspaper reported that representatives of some 52 countries had worked on an associated draft convention, which was subsequently released. The content is wide ranging and seeks to prohibit non-peaceful uses of the Internet as well as to internationalize Internet governance. The United States has so far opposed such positions, arguing that existing international arrangements are adequate. Behind the American position on the military issues is the concern that countries like China will use any means possible, including international public opinion and new conventions, to limit U.S. military options.

Thus, in real terms, the scope for a cyber detente between the United States and China is from the outset quite significantly limited by larger geopolitical constraints.

Nevertheless, to execute this detente, both China and the United States have been quietly supportive of modest efforts in Track 2 diplomacy (and its variant Track 1.5)[14] to stimulate some progress. A number of Track 2 processes to address these issues have been underway. In 2009, the EastWest Institute (EWI) convened its first meetings between interested parties in the United States and China. Based on its consultations, it concluded then that the best way forward was to work on a number of civil (non-military) issues: after beginning with spam, it is tackling topics that are progressively more sensitive and difficult.[15] At the same time, in a number of its private meetings since 2009, EWI raised more sensitive military issues, most often in the context of possible new multilateral arrangements (codes of conduct) in cyberspace.

In February 2012, the Brookings Institution published an analysis of the results of its Track 2 work.[16] The meetings brought together public and private sector leaders from the two countries, with military officials included on the U.S. side. The report published as a result of the meetings is not an official record but rather reflections by its authors. They observed the political realities that determined the type of agenda that could be set:

- Both countries want to protect their prerogatives for developing cyber capabilities for espionage or military purposes.
- The two countries have "different views concerning freedom of information in cyberspace."
- Bureaucratic mechanisms for setting cyber policy in both countries are fragmented and weakly coordinated.
- Private sector actors are significant players in setting cyber policy in both countries.[17]

Private sector actors are significant players in setting cyber policy in both countries.

13 See http://www.fmprc.gov.cn/eng/zxxx/t858978.htm.

14 Track 1.5 is a variant of Track 2 where there is a declared official interest in the discussions and the participating officials are not afraid to speak in their official capacity, but where the setting is informal. Outcomes of Track 1.5 work usually have more impact, sooner.

15 The policy differences on non-military issues are quite large. One of the technologies used for controlling spam (spam filters) is also used by China for censoring Internet traffic for political reasons. China has been frustrated that for a number of years it could not convince U.S. authorities to take down botnets involved in spam by simply ordering ISP providers to block the relevant connections simply upon notification of the botnet linkup. The U.S. government is constrained from interfering in communications of its citizens by constitutional protections of free speech.

16 Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," John L. Thornton, China Center at Brookings, February 2012, http://www.brookings.edu/research/papers/2012/02/~/media/Research/Files/Papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.PDF.

17 P. viii.

"Create an international management body to ensure equitable distribution of Internet resources."

The authors concluded that the scale of Track 2 so far was simply inadequate relative to the scale of the challenge.[18] They called for expansion of the pool of people engaged in this work who could be trusted by both governments. They proposed a heavy initial focus on cyber crime; supported by an airing of different views on the norms governing cyberspace. They suggested a review of models of cooperation not limited to arms control; instead, it would also include public health, ecosystems, global financial regimes, crime-fighting and counter-terrorism.[19] They also called for bilateral discussion of the "red lines" for action in cyber activities that might provoke escalation and suggested that some effort be made to remove the riskier actions from the policy menu of the two states.[20]

A report released in April 2012 by two other U.S. organizations made a number of useful suggestions, based on two workshops involving Chinese and Western scholars, policy analysts, and scientists discussing the political, economic, and strategic dimensions of cybersecurity in China.[21] Noting that the Chinese military planning system had not systematically integrated a number of the ideas presented, the report included useful discussion of policy needs and options for a range of civil, military and espionage issues but addressed few military issues in detail.

The Center for Strategic and International Studies (CSIS) in Washington D.C. has also been conducting a Track 1.5 meeting with the China Institutes for Contemporary International Relations (CICIR) in Beijing.[22] This involved two "war games" in 2011 and another in 2012 with Chinese and American military officers and other officials participating. In a joint statement in June 2012, the two parties concluded that the level of mutual misperception is high even though agreement on some issues had "promoted cybersecurity cooperation between the two countries."[23] The statement noted that work remained to be done on a range of contentious issues, including even the supposedly less sensitive issues of cyber crime.[24] The parties acknowledged that cyber emergency channels of communication between the two countries had not been formalized. A CICIR participant advanced a proposal for a code of conduct in cyberspace with four main elements:

- "Restrict weaponization of cyberspace."
- "Respect rights of countries to manage relevant networks and oppose hegemony in cyberspace."
- "Increase mutual trust through pledges not to use cyber warfare and refrain from developing ... cyber weapons."
- "Create an international management body to ensure equitable distribution of Internet resources. This could be accompanied by a UN investigative body, modeled after the IAEA, to review and investigate cyber attacks and determine attribution. This UN body could also deal with proxies."

For their part, CSIS participants addressed the "importance of norms and confidence building to increase stability," including "ideas for greater transparency, such as direct dialogue between the two governments, stability and risk reduction measures, acceptance of the applicability of the existing laws of armed conflict, observance of existing commitments on the protection of intellectual property, adherence to the Budapest Convention

18 P. viii.

19 P. ix.

20 P. x.

21 University of California Institute on Global Conflict and Cooperation and the United States Naval War College, "China and Cybersecurity: Political, Economic, and Strategic Dimensions", Report from workshops held at the University of California, San Diego, April 2012, http://igcc.ucsd.edu/assets/001/503568.pdf.

22 For a press account of this, see Nick Hopkins, "U.S. and China turn to war games to build cyber detente", *Sydney Morning Herald*, April 18, 2012, http://www.smh.com.au/world/us-and-china-turn-to-war-games-to-build-cyber-detente-20120417-1x5mk.html#ixzz1wBPTnQcB. One of the organizers, Jim Lewis, was quoted as follows: ''China has come to the conclusion that the power relationship has changed, and it has changed in a way that favors them. ... The PLA [People's Liberation Army] is very hostile. They see the U.S. as a target. They feel they have justification for their actions. They think the U.S. is in decline.''

23 "Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR) – Center for Strategic and International Studies (CSIS)", June 16, 2012, http://www.cicir.ac.cn/chinese/newsView.aspx?nid=3878.

24 The joint statement observed: "While there is agreement on the benefits of cybercrime cooperation, implementation is difficult. Existing bodies for law enforcement cooperation meet infrequently and requests for investigative support are not always answered. This seems to reflect procedural difficulties as much as political obstacles."

on cybercrime, and state responsibility for actions in cyberspace by individuals resident in their territory." [25]

Of considerable interest, the two sides agreed that both governments had identical views of their vulnerabilities to supply chain interference by the other. This was seen as a high-priority issue for further discussion at a formal level.

A CICIR participant raised the issue of a "no-first-use" agreement among major cyber powers by referring to an American article on the subject, but a Chinese military source asserted later to the authors of this paper that such a position is not something that China would officially endorse. A CICIR participant also raised the "idea of civilian sanctuaries, and a prohibition of cyber attacks against purely civilian targets." In response, a CSIS participant reverted to the view that the existing laws of armed conflict, including the need for proportionate response and discrimination in targeting, already provided the necessary framework for protecting civilians, even though the "line between civilian and military infrastructure is blurred."

On the very important point of the threshold for actions in cyberspace that should be characterized as an act of war, the two sides agreed that the threshold "should be high—not everything bad that happens in cyberspace is an attack or the use of force." They also agreed that clarifications are needed on ambiguities about what constitutes an attack.

Thus, for cyber detente between China and the United States to be meaningful, especially in an environment where both countries are consistently at odds and where neither has fully formed long-standing positions, continued examination in multiple forums of some of the key potential agenda items is essential. The rest of this paper looks at two issues that have received scant attention in bilateral conversations to date:

1. Clarifying the mix between offense, defense and preemption in the military cyber policies of the two countries.
2. Understanding interdependence between the United States and China in cyberspace, and its impact on strategic deterrence.

Clarifying the mix between offense, defense and preemption

China sees information warfare as the primary determinant of military victory.[26] For China, information warfare includes cyber operations as part of an array of diverse instruments, including classic political propaganda as well as operations in all domains of the electromagnetic spectrum, including cyberspace. Chinese military leaders see their cyber warfare capabilities as a powerful asymmetrical tool in their deterrence strategy vis-à-vis the United States because they are seen as offering the potential to degrade the United States' advantages in conventional military power. China sees it as essential to put a very heavy reliance on its asymmetric military options, including cyber warfare, to deter its political adversaries from resorting to force—and if, armed conflict erupts, to limiting an adversary's options.

Chinese military leaders see their cyber warfare capabilities as a powerful asymmetrical tool in their deterrence strategy vis-à-vis the United States.

China's 2010 White Paper on National Defense gives insight into how good China thinks it is in terms of its information warfare capability.[27] It notes that China has obtained only a "preliminary level" of interoperability between different elements of its armed forces within this sphere. This reflects what Chinese sources say in private about the weakness of their cyber warfare capabilities relative to those of the United States. (The best informed American sources concur with this broad brush assessment.) China's armed forces are well short of where they want to be in cyber warfare capability. It would be

25 "Bilateral Discussions on Cooperation in Cybersecurity", op.cit.

26 This view has been aired in Chinese military circles beginning in 1995, but was endorsed as official doctrine of the PLA only in 2003. For an overview of PLA doctrinal writings, see Brian Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: *Chinese Capabilities for Computer Network Operations and Cyber Espionage,"* Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corporation, March 7, 2012, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

27 , "White Paper on National Defense, 2010" at "China's National Defense in 2010", http://news.xinhuanet.com/english2010/china/2011-03/31/c_13806851_3.htm.

The United States went on to develop information dominance of the battlefield as a fundamental part of its military strategy.

almost impossible for us to make any credible comparative statement in further detail about how much better U.S. capability is than Chinese capability, but in very broad terms, if we put U.S. capability at high, Chinese cyber war capability is probably very low in terms of sophisticated options. That said, in terms of intended effects, China's capabilities may be somewhat higher and would be largely confined to softer infrastructure targets.

China sees itself as lagging well behind in technology. It knows how difficult it is for a country to achieve a level of technological preparedness in its armed forces that is significantly different from the technological foundations of the society as a whole (talent base, research and development climate, investment levels). A number of Chinese and international studies have consistently given China fairly low grades in terms of advanced information technology.[28]

In the military sphere, there are grounds for Chinese concerns that it is lagging behind the U.S., but this is not simply a question of comparative national standings in cyber warfare capability. The imbalance in cyber warfare capability exacerbates Chinese insecurities stemming from U.S. superiority in military power and the strength of its global alliance system.

The U.S. has been the global leader in developing information dominance as a military strategy, with associated weaponry, dedicated units and dedicated planning elements in the Pentagon, the uniformed services and the intelligence agencies. As Professor Joseph Nye and Admiral William Owens observed in a 1996 article in *Foreign Affairs*, "The information technologies driving America's emerging military capabilities may change classic deterrence theory."

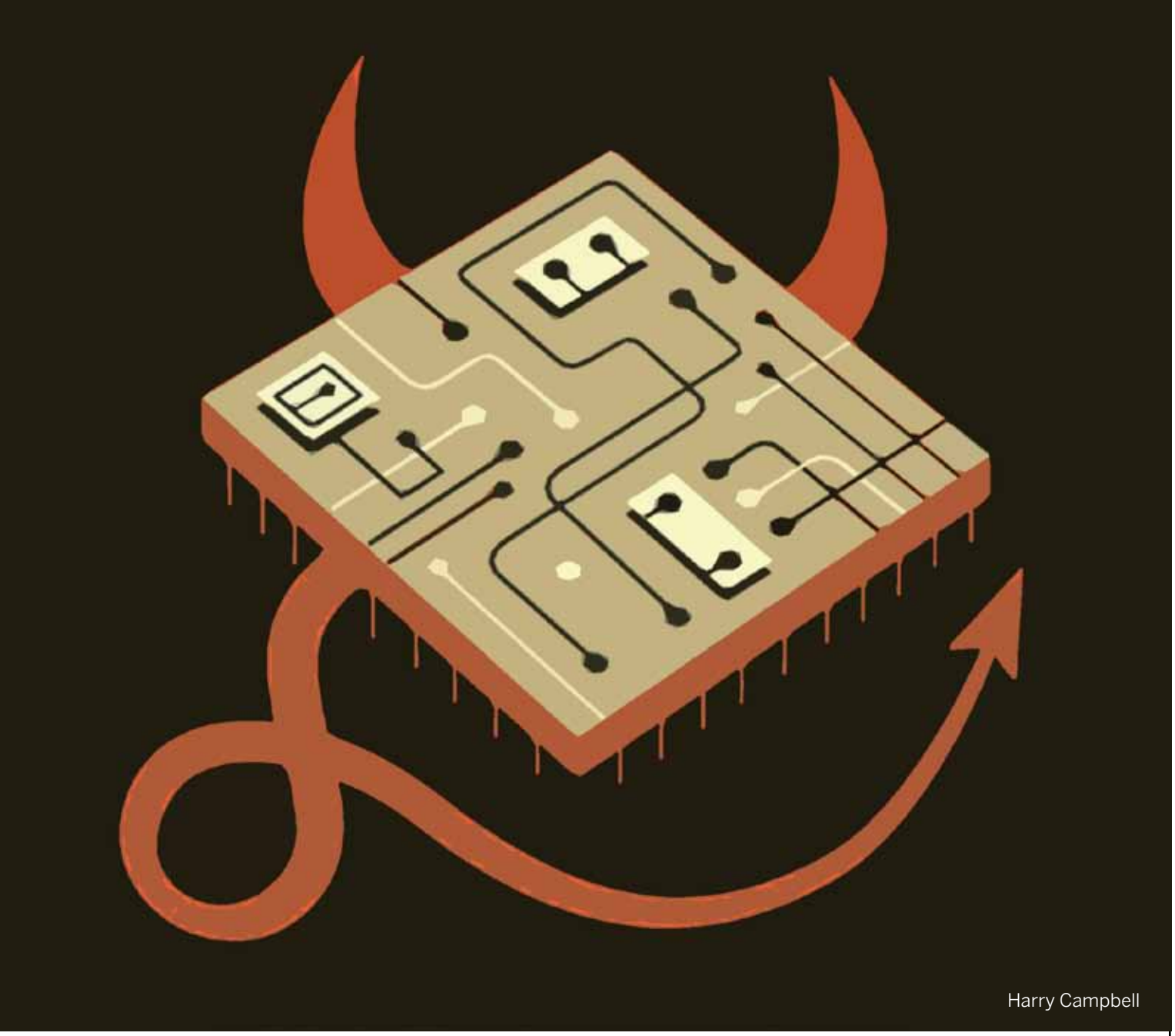
The United States went on to develop information dominance of the battlefield as a fundamental part of its military strategy. It was quite within its rights to do so. But events since 1996 have shown how profoundly this change of strategy shifted the calculus of deterrence between China and the United States. As enunciated by former United States Air Force Chief of Staff, General (ret.) T. Michael Moseley in 2011, the advances in cyber weapons and their impact on strategic nuclear stability represent an acceleration of a pre-existing trend where precision conventional weapons had already been destabilizing traditional concepts of deterrence[29]. One question that such assessments now prompt is how much does American cyber war doctrine—though defensive in character, but with a pre-emptive element of strategic strike in milliseconds[30]—contribute to China's concerns and shape its pattern of cyber military operations.

China's armed forces are actively seeking to overcome their backwardness in military development through massive cyber espionage activities. A decade ago, cyber espionage cases were dismissed as mere "brushfires," minor incidences that are bound to happen in a competitive international system. Western officials did not see this activity as a strategic threat. However, Western leaders have recently concluded that this is a problem too big to be ignored and have escalated their political rhetoric about it.

28 See for example, a 2011 study by the Chinese Academy of Sciences, *Information Science and Technology in China: A Roadmap to 2050*. The study also registered broad agreement, though in visible disappointment, with a set of IT competitiveness rankings by *The Economist* that placed China 50th in global terms, out of 66 countries surveyed. See Li Guojie (ed.), *Information Science and Technology in China: A Roadmap to 2050*, Chinese Academy of Social Sciences, Science Press, Beijing, Springer, 2011, pp. 20-21. A similar view can be found in the World Economic Forum's 2012 Network Readiness Index (NRI), which ranked China 51 for its use of information technologies to advance its national competitiveness and its citizens' lives. China had slipped from 36th in the 2011 rankings. The NRI gives only a partial picture of China in cyber world but it mirrors quite critical sentiment within the country about its weak position relative to others. The United States, Japan, Singapore, Taiwan, South Korea and Malaysia are all ahead of China in the 2012 NRI. See World Economic Forum, *The Global Information Technology Report 2012*, May 2012, http://www.weforum.org/issues/global-information-technology.

29 Remarks by General (ret.) T. Michael Moseley, USAF, October 24, 2011, United Nations Headquarters, New York. See : http://www.ewi.info/ban-ki-moon-calls-nuclear-disarmament-ewi-forum.

30 The concept of global (strategic) strike in milliseconds was canvassed in a speech by Gen. James E. Cartwright at the Center for International and Strategic Studies , Washington D.C., June 4, 2009, reported in Jim Garamone, "Deterrence Plays Into Overseas Basing Decisions, Vice Chairman Says." See http://www.defense.gov/news/newsarticle.aspx?id=54648.



Harry Campbell

China's Operational Use of Cyber Warfare

In Chinese military thinking, the armed forces need an offensive capability so that they can be prepared to pre-empt U.S. options in a Taiwan-related scenario and possibly in other regional scenarios. As mentioned above, the argument is that since China could not match the conventional military capabilities of the United States, it must find asymmetric means of attack.

In the minds of Chinese military planners, an offensive military cyber posture would probably include elements such as:

1. Wide-ranging cyber attacks on the critical civilian infrastructure of the United States, Japan and Taiwan that would degrade American military preparedness in the Western Pacific, including in the continental United States;
2. Opportunistic attacks on selected high value military targets that China has succeeded in penetrating;
3. Suspension of all Internet traffic into China to prevent a cyber attack.

But one very important qualification has to be made. There is a difference between the overall strategic posture of a state on the offense/defense spectrum and the disposition of different elements of its capability at an operational level.In our view, China's national

The two most urgent tasks for bilateral discussions would appear to be clarifying the relationship between offensive and defensive cyber operations at the strategic and operational levels of war.

strategic military posture is defensive in character. This is in part due to its weakness, but it is also due to the fact that China does not have hostile military intent, except in respect to defense of what it sees as its territory, most importantly Taiwan and at a lower level, the Diaoyu/Senkaku Islands and the Nansha/Spratly islands). China would only resort to offensive cyber operations with destructive effect against targets in the United States if it felt that the latter was embarking on a military intervention that could lead to the final separation of Taiwan from China.

The type of war that China would want to fight over Taiwan, if forced to, would not be an all-out massive attack on Taiwanese and United States forces. Instead, it would prefer a carefully designed strategy of political, economic and military gambits intended to weaken the capacity or will of the United States to deliver overwhelming military power in the Taiwan region and to weaken the capacity of the Taiwan government to control the civil affairs of the island. A partial economic blockade or sanctions are more likely tools of choice for China than heavy reliance on cyber weapons for strategic impact, though such weapons could be used for operational and tactical effects.

In sum, China is probably engaged in cyber warfare planning for operations against the United States on a very serious level, and possibly more so than for naval or air combat operations against it. At least in relative terms, China's cyber warfare capability is probably far more powerful but less lethal than its conventional military capabilities. That suits China enormously in both respects. China's military strategy is highly defensive, but to defend against U.S. operations against China over Taiwan, China has to rely mainly on unconventional operations, and these include cyber operations as well as psy-ops of the classic kind, including through fifth- column policies.

The scale and intensity of United States offensive cyber operations aimed at China on a day-to–day basis may be lower than vice versa, but without access to classified material it would be hard to characterize the difference between the potential disruptive effects of American and Chinese capabilities. This lack of clarity, in an environment of exceedingly low transparency peculiar to cyberspace compared with land, air, sea and space operations, aggravates insecurities on both sides.

The two most urgent tasks for bilateral discussions would therefore appear to be clarifying the relationship between offensive and defensive cyber operations at the strategic and operational levels of war (the thresholds of response), and clarifying the link between these thresholds and traditional notions of strategic nuclear and conventional force deterrence.

Understanding interdependence in cyberspace

China and the United States do have a complementary interest in cooperating on many aspects of cybersecurity. The most significant argument to support a claim for cooperation in China's international behavior in cyberspace is mutual dependence among the major economic powers (including China, the United States, Japan and the European Union) in the economic sphere, in a situation where trillions of dollars of transactions occur through networked digital communications each day. In speaking of the U.S.'s economic reliance on digital networks and systems, former Director of National Intelligence Mike McConnell observed in 2010: "The United States economy is $14 trillion a year. Two banks in New York City move $7 trillion a day. On a good day, they do eight trillion... All of those transactions are massive reconciliation and accounting. If those who wish us ill, if someone with a different world view was successful in attacking that information and destroying the data, it could have a devastating impact, not only on the nation, but the globe."[31]

The cost to global economic stability would likely be very high if there were a major confrontation between China and the United States. Sustained or repeated interruptions in connectivity, corruption of transaction data, or deletion of commercial records on a large scale could have major negative repercussions for the global economy. Whether confidence after such attacks could be restored remains an open question. These costs would

31 Intelligence Squared Debate, "The Cyber War Threat Has Been Grossly Exaggerated," June 8, 2010, Transcript, p. 7, http://intelligencesquaredus.org/wp-content/uploads/Cyber-War-060810.pdf.

be so high that they should at least dampen if not fully deter states from resorting to cyber war. Cyberspace only amplifies traditional interdependence in trade.

At a lower level of interdependence, China's high reliance on foreign manufacturing investors for its "advanced technology products" (ATP), which constituted 31 percent of total exports to the United States in 2009,[32] exposes another major vulnerability. Both countries are dependent on each other's markets access in the production of ATP, and any confrontational behavior in cyberspace will risk fragile economic growth. According to one study, as of 2010, foreign investors are responsible in some way for more than 96 percent of all Chinese ATP exports.[33] China is slowly moving from low skill-intensive to high skill-intensive manufacturing products, which will only increase the mutual dependencies in this sector. In the United States, the creeping dependence of its systems on Chinese-produced components is high. That said, as Moran observes, Chinese firms are losing in the export competition with foreign-invested multinationals in China.

Acute dependencies also exist in other sectors that are deemed to be part of the national critical infrastructure such as telecommunications and electricity. The United States, for example, is investing in Chinese nuclear energy construction and providing critical know-how especially when it comes to nuclear power plants. The case of Stuxnet—the worm specifically designed to target industrial control systems in Iran's nuclear enrichment facility—has shown both the vulnerability of such systems and the relative difficulty in containing cyber weapons once unleashed. During cyber conflict, weapons that are used could easily affect both sides, similar to gas warfare in the First World War; yet this time the entire country or region may be vulnerable, not just the field of battle.

In October 2011, the Commerce Department rebuffed the bid by Huawei, a Chinese telecommunication company, to build a wireless network for first responders in the United States. But this has not slowed the steady increase in investments of both Chinese and U.S. companies in each other's telecommunication markets. The unprecedented U.S. current account deficit and the country's consumption behavior has been financed, to a large extent, by China, substantially limiting Washington's policy options. In spite of occasional limitations on particular Chinese investments in the United States, Washington simply cannot threaten to cut off China's access to the U.S. domestic market.

China and the United States have already started cooperating in some other sensitive fields. For example, both countries have set up a military hotline to prevent misunderstandings from escalating into crises. This was a response to the deterioration of relations after various spying incidents, including the collision of a U.S. spy plane with a Chinese fighter jet in 2001.

In its 2010 White Paper on the Internet, China reaffirmed its earlier international commitments to collaborate with other countries on cybersecurity. China's strongest commitments on cybersecurity came in the 2003 UN General Assembly Resolution 57/239 on Creation of a Global Culture of Cybersecurity and in the 2003 Geneva Declaration of Principles of the World Summit on the Information Society. There were earlier resolutions beginning in 1999 on the implications for international security as well as in 2001 on combating criminal misuse of information technologies.

Examples of such commitments can also be found in the 2009 ASEAN-China framework agreement on network and information security emergency response and the 2009 agreement within the Shanghai Cooperation Organization on information security. In July 2006, the ASEAN Regional Forum (ARF), which included China, issued a statement that its members should implement cyber crime and cybersecurity laws "in accordance with their national conditions and by referring to relevant international instruments." The ARF has also called on its members to collaborate in addressing criminal, including terrorist, misuse of cyberspace.

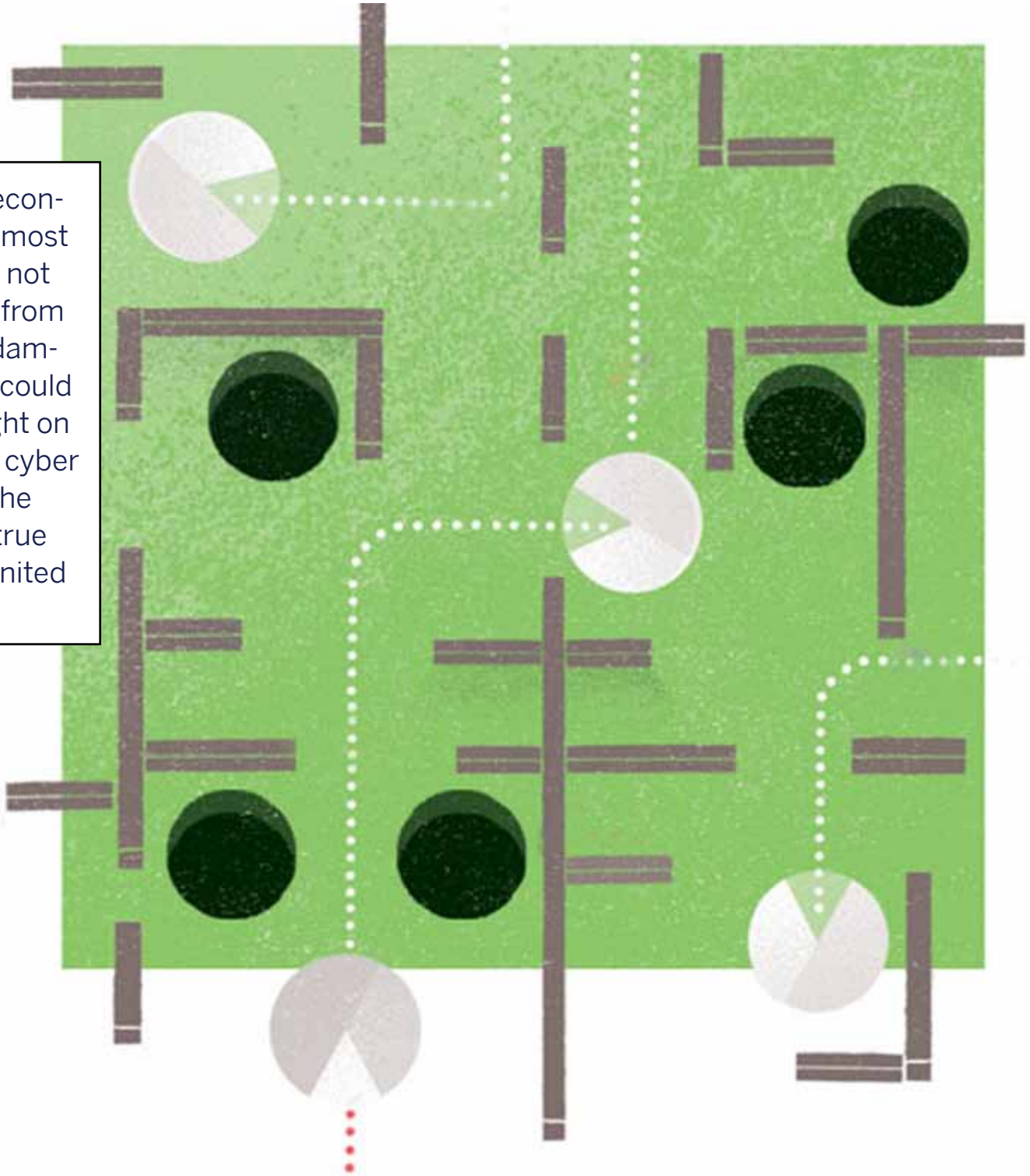
China, Japan and Korea have agreed on a work plan that "includes projects on network and information security policies and mechanisms, joint response to cyber attacks

China and the United States have already started cooperating in some sensitive fields. For example, both countries have set up a military hotline to prevent misunderstandings from escalating into crises.

32 Xing Yuping, "China's High-tech Exports: Myth and Reality," Working Paper, National Graduate Institute for Policy Studies (GRIPS), Tokyo, 2009, p. 1.

33 Theodore H. Moran, "Foreign Manufacturing Multinationals and the Transformation of the Chinese Economy: New Measurements, New Perspectives," Working Paper, Petersen Institute for International Economics, April 2011, p. 10.

China's economy is almost certainly not immune from serious damage that could be brought on by a U.S. cyber attack. The same is true for the United States.



(including hacking and viruses), information exchange on online privacy protection information and creation of a Working Group to promote this cooperation."[34]

The APEC Working Group on Telecommunications agreed on an action plan for 2010-2015 that included "fostering a safe and trusted ICT environment," the security of networked systems, sharing of best practice approaches, joint technical cooperation, and cybersecurity awareness initiatives.[35] The plan commits members to work within the industry.

34 The existence of this trilateral agreement was confirmed with Japanese officials. Public information on it is sketchy. See Imad Y. Hoballah, "Cybersecurity Organizations and Efforts," Presentation, February 8, 2010 in the first meeting of the "Regional Pan Arab Observatory for Cyber Security" at the Antonine University in Baabda, Lebanon.

35 APEC TEL Strategic Action Plan: 2010-2015, adopted by the 2010 APEC Telecommunications and Information Ministerial Meeting, October 31, 2010, http://www.apec.org/Meeting-Papers/Ministerial-Statements/Telecommunications-and-Information/2010_tel/ActionPlan.aspx

Recent annual threat assessments of the United States Director of National Intelligence have referenced signs of cooperative behavior by China in cyber policy, even if the record of U.S.-China diplomacy in this area is weak. Yet a senior U.S. official, Under Secretary of State Robert Hormats, told the United States China Internet Industry Forum in December 2011 that the relationship on key cyber issues was stalled or even going backwards.[36] The same tone of concern was reflected in remarks made by Secretary of State Hillary Clinton on September 5, 2012 in a visit to China.[37]

Is China's level of dependence on the security of the Internet and other international digital communications platforms so high that it is forced to pursue cooperative behavior rather than put at risk its international economic ties? Or is China's economy immune from serious damage that might be suffered by the United States if the latter were subject to a debilitating cyber attack for which many Americans believe China is preparing, if only on a contingency basis? The latter statement is probably farther from current reality than the former. China is most likely obliged to cooperate in cyberspace rather than risk the fabric of its economic ties. China's economy is almost certainly not immune from serious damage that could be brought on by a U.S. cyber attack. The same is true for the United States.

We are forced to a probability assessment because we don't know with a high degree of certainty the answer to either question. There are few studies available in the public domain and even fewer references in public to classified studies. We don't know how transformational the Internet may have been on geopolitics because we don't have clear data on just how intermingled the critical elements of economic life are. This is a subject worthy of significant and urgent study.

There have been various studies and tabletop exercises conducted on the subject of the interconnectivity of critical information infrastructure. For instance, the *Blue Cascades Exercise* series in the United States looks at the interconnectivity of critical information infrastructure on the regional level; *Livewire* simulates coordinated cyber attacks on multiple critical information systems and networks; and the *Cyber Storm* exercises conducted by the Department of Homeland Security modeled a credible national crisis scenario. The public conclusions of all these exercises are similar: there is an urgent need to develop ways to share accurate, real-time information to understand interdependencies and how to respond and recover from cyber attacks. The People's Liberation Army has also conducted various table-top exercises primarily in the offensive realm, simulating cyber attacks on the telecommunications, electricity and finance sectors of Taiwan, India, Japan, South Korea and the United States over the years. The Chinese are acutely aware of their intrinsic vulnerability to sophisticated Western cyber weaponry and cyber attacks in general. In 2010, more than 4,000 Chinese government websites were hacked, a 68 percent increase from 2009. The Chinese government repeatedly claims to be the "biggest victim country of hacking."

In 2010, more than 4,000 Chinese government websites were hacked, a 68 percent increase from 2009. The Chinese government repeatedly claims to be the "biggest victim country of hacking."

We can be more certain about the shared interests when we look at the potential impact of cyber crime. This is an increasingly dangerous threat to the macro-economy of major states. As the U.S. Director of National Intelligence Lt. Gen, (ret.) James Clapper observed in February 2011, the United States is facing "new security challenges across a swath of our economy" because new technologies intended to underpin prosperity "are enabling those who would steal, corrupt, harm, or destroy public and private assets vital to our national interest." This is linked to international organized crime which, he said, was penetrating governments, degrading the rule of law and enhancing the ability of states to manipulate key commodities markets such as oil.

At the enterprise level, the risk has gone from accounting loss in cyber theft to one of a threat to the long term survival of companies. Too many cyber criminals appear for now to be outside the reach of law enforcement, and global businesses now face attacks on such a scale and frequency that they are being forced to re-evaluate enterprise security

36 United States. Department of State. Remarks by Robert D. Hormats, Under Secretary for Economic, Energy and Agricultural Affairs, Keynote Address, U.S.-China Internet Industry Forum, Washington, DC, December 7, 2011, http://www.state.gov/e/rls/rmk/2011/178423.htm.

37 United States Department of State, Remarks by Secretary of State Hillary Rodham Clinton with Chinese Foreign Minister Yang Jiechi, Beijing, September 5, 2012, http://www.state.gov/secretary/rm/2012/09/197343.htm.

The United States and China should agree on a joint public study on the interdependence of their respective critical information infrastructures in terms of likely economic effects of criminal attacks with strategic impacts.

strategies and come to terms with new risk management techniques. For major businesses, the risks, vulnerabilities and threats are now as multinational and complex as their corporate footprint; in addition, those threats are difficult to anticipate. This is as true for Chinese enterprises operating globally, as it is for similar American corporations. The reported contamination of Huawei products by Chinese intelligence agencies is thwarting its otherwise normal corporate ambitions in the United States.[38]

Policy Options

There has been an almost automatic assumption in some circles in the United States that international cooperation with China on sensitive issues of cyber espionage or cyber warfare, or even on Internet governance, would be almost impossible because of differences between its domestic political arrangements and those of other leading cyber powers.

That said, the two countries' economies, though very different in many respects, are each highly dependent on a global Internet and shared communications platforms and hardware. While the Chinese economy is not as dependent on the Internet as the U.S., economy is, the difference between the two is fast shrinking. China's export-driven economy and its trade in financial services make it as vulnerable to cyber attack as the United States. This interdependence—despite occasional outbursts of confrontational rhetoric coming from both Beijing and Washington—can be leveraged to promote stability in bilateral relations. In fact, this is already happening.

We can think of this interdependency as a balance of cyber power. If one accepts that both governments make rational calculations, than this new interconnectedness can be exploited to make conflict less likely. In today's interconnected, digitalized world, the "opportunity cost" associated with embarking on a confrontational course will deter both parties from engaging in open hostile actions. This of course does not preclude cyber espionage, intellectual property theft, or even what some analysts have called the "long game," i.e. the slow and gradual infiltration of strategically significant economic ICT systems by hackers on both sides.

Due to the unequal distribution of cyber power between the two countries, there will continue to be sharp limits on cooperation. What are the mechanisms available to reduce tensions and promote cooperation? For example, could China and the United States agree to set up a formal dialogue on confidence building measures, perhaps leading to the establishment of standing cyber risk reduction centers in each country, permanently staffed and linked with each other to reduce misunderstanding and tensions in times of crisis? That is probably too ambitious in the foreseeable future, yet talks on this subject have already started with Russia.[39] Some cyber risk reduction is indeed possible.

There are three proposals that the authors feel warrant immediate attention and may produce benefits in a reasonable time frame.

38 This challenge was addressed in a White Paper released by Huawei on Sept. 5, 2012 under the title "Cyber Security Perspectives." It goes into some detail on the lack of consistency in United States concerns about Huawei. These center on the notion that "foreign developed" cyber technologies may not be fully reliable from a security point of view. To counter that concern, the paper outlines the heavy involvement of *Fortune* 500 companies in China and asks rhetorically if their production is now to be regarded by the United States regulators as "foreign developed." It asserts the general rule, "No longer is technology designed, developed and deployed only in one country; no longer can any country or large company claim to rely on a single sourcing model."

39 Washington Post, April 4, 2012, http://www.washingtonpost.com/world/national-security/in-us-russia-deal-nuclear-communication-system-may-be-used-for-cybersecurity/2012/04/26/gIQAT521iT_story.html.

The United States should work to include China in the existing infrastructure of the 24/7 Network of Contacts for High-Tech Crime of the G8.

First, the United States and China should agree on a joint public study on the interdependence of their respective critical information infrastructures in terms of likely economic effects of criminal attacks with strategic impacts. This could be done under the framework of the United States- China Strategic and Economic Dialogue. This may not be welcome by some private operators. Yet the need for such a study exists on a political level. It is a consequence of the strategic impact of private ownership of critical infrastructure. As much as such a study might intrude on narrowly defined private sector interests, leading ICT businesses need a deeper understanding of the military implications of the intermingled, even tangled, character of U.S. and Chinese operations in cyberspace.

Second, the United States should work to include China in the existing infrastructure of the 24/7 Network of Contacts for High-Tech Crime of the G8. This might be accompanied by an effort to set up bilateral cooperation between the two countries on emergency response that go beyond the current capacity of the Computer Emergency Response Teams (CERT) of the two countries.

Third, cyber espionage, especially against intellectual property and critical infrastructure, is now too big a problem to ignore or to dismiss as a necessary evil. The U.S. and China need to take stock of the negative impacts and establish some limits. Both countries need some common understanding of the limits of cyber espionage.

There are two main problems to be dealt with on that third point. The first is the blurred boundaries between national security espionage and theft of intellectually property for commercial gain. The second involves the often equally blurred distinctions between critical infrastructure of an exclusively civilian or humanitarian character and that of a military or strategic one. But to deal with such issues officials from each side would require more information-sharing than their government has so far been willing to permit. Quite understandably, both sides feel that they can't discuss anything that is secret without breaking their own laws.

A first step may be to create a new domestic legal foundation to allow authorities in both countries to share information and to conduct joint assessments of that part of the problem that lies clearly in the intellectual property domain or civil domain.[40] Most Western governments underestimate China's stakes in international collaboration that derive from its vulnerability to large-scale disruptions and crime in cyberspace.

Speaking about the United States, Admiral Mike McCullen observed in 2010: "We now need a dialogue among business, civil society and government on the challenges we face in cyberspace—spanning international law, privacy and civil liberties, security and the architecture of the Internet. The results should shape our cybersecurity strategy."[41] This approach is now also needed at the international level. So far, in U.S.-China relations, the conversations are still in their infancy and are characterized as strongly adversarial. The challenge is to deepen the conversations and reduce mistrust through enhanced transparency and predictability.

40 In the joint article referenced above by McConnell, Chertoff and Lynn in January 2011, the authors observed that national secrecy laws would have prevented them from airing the very serious challenges they faced three months earlier, had the government not released an unclassified study of the subject.

41 Mike McConnell, "Mike McConnell on How to Win the Cyber War We're Losing", *Washington Post*, 28 February 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493_2.html?sid=ST2010031901063.

The Authors

Greg Austin is a professorial fellow at the EastWest Institute, who earlier served for five years as a vice president there. He is also a senior visiting fellow in the department of War Studies at King's College London. Prior to joining EWI, Austin served as director of research at the Foreign Policy Center in London (2004-2006) and as a consultant to the UK Cabinet Office and four other government departments (2003-2004). He was the Asia program director, then director of research at the International Crisis Group (2000-2002). He is the author, co-author and editor of several books on China's strategic policy. He has a doctorate in International Relations and master's degree in International Law. He co-authored with Franz-Stefan Gady the 2010 EWI Policy Paper, "Russia, the United States, and Cyber Diplomacy: Opening the Doors." He is currently writing a book on China's cyber policies for publication in 2013.

Franz-Stefan Gady is an associate and foreign policy analyst at the EastWest Institute. He has previously worked as an adjunct research assistant at the Institute for National Strategies Studies of the National Defense University in Washington, D.C., focusing on regional security issues. He was also an analyst for the Project on National Security Reform, a congressionally funded nonprofit organization founded to reform the national security structure of the United States. Gady has written for the *Christian Science Monitor, Foreign Policy Magazine, Foreign Policy Journal, American Diplomacy Quarterly, The National Interest, Small Wars Journal,* and *New Europe*, among other publications. He has a master's degree in Strategic Studies / International Economics from the School of Advanced International Studies, Johns Hopkins University.

EWI Board of Directors

OFFICE OF THE CHAIRMEN

Ross Perot, Jr. (U.S.)
Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC
Board of Directors
Dell Inc.

Armen Sarkissian (Armenia)
Vice Chairman
EastWest Institute
President
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President, Co-Founder & CEO
EastWest Institute

Mark Maletz (U.S.)
Chair of the Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

R. William Ide III (U.S.)
Counsel & Secretary
EastWest Institute
Partner
McKenna Long & Aldridge LLP

Leo Schenker (U.S.)
Treasurer
EastWest Institute
Senior Executive Vice President
Central National-Gottesman Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former Chairman
EastWest Institute
2008 Nobel Peace Prize Laureate
Former President of Finland

Tewodros Ashenafi (Ethiopia)
Chairman & CEO
Southwest Energy (HK) Ltd.

Jerald T. Baldridge (U.S.)
Chairman
Republic Energy Inc.

Sir Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Matt Bross (U.S.)
CEO
WBE Hong Kong

Robert N. Campbell III (U.S.)
Vice Chairman (Retired)
Deloitte LLP

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Mark Chandler (U.S.)
Chairman & CEO
Biophysical

George F. Russell, Jr. (U.S.)
Former Chairman
EastWest Institute
Chairman Emeritus
Russell Investment Group
Founder
Russell 20-20

Ramzi H. Sanbar (U.K.)
Chairman
SDC Group Inc.

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Kanwal Sibal (India)
Former Foreign Secretary of India

Henry J. Smith (U.S.)
CEO
Bud Smith Organization Inc.

Pierre Vimont (France)
Executive Secretary General
European External Action Service
Former Ambassador
Embassy of the Republic of France in Washington, D.C.

Alexander Voloshin (Russia)
Chairman of the Board
OJSC Uralkali

Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Mangement, LLC

Hilton Smith, Jr. (U.S.)
President & CEO
East Bay Co., LTD

CO-FOUNDER

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.
Co-Founder
EastWest Institute

CHAIRMEN EMERITI

Berthold Beitz (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Francis Finlay (U.K.)
Former Chairman
Clay Finlay LLC

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor & Minister of Foreign Affairs

Donald M. Kendall (U.S.)
Former Chairman & CEO
PepsiCo. Inc.

Whitney MacMillan (U.S.)
Former Chairman & CEO
Cargill Inc.

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, OSCE and the UN in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

EastWest Institute
Forging Collective Action for a Safer and Better World

Founded in 1980, the EastWest Institute is a global, action-oriented think-and-do tank. EWI tackles the toughest international problems by:

Convening for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel "Track 2" diplomacy, and also organizes public forums to address peace and security issues.

Reframing issues to look for win-win solutions. Based on our special relations with Russia, China, the United States, Europe and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

Mobilizing networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) nonprofit organization with offices in New York, Brussels and Moscow. Our fiercely guarded independence is ensured by the diversity of our international board of directors and our supporters.

EWI New York Center
11 East 26th St.
20th Floor
New York, NY 10010
1-212-824-4100

EWI Brussels Center
Rue de Trèves, 59-61
Brussels 1040
32-2-743-4610

EWI Moscow Center
Bolshaya Dmitrovka St. 7/5,
Building 1, 6th Floor
Moscow 125009
7-495-2347797

EWI Washington Office
1069 Thomas Jefferson St. NW
Washington, DC 20007
1-202-492-0181

www.ewi.info