UNCLASSIFIED//

ENVELOPE

RAAUZYUW RUEIFBS2555 1270158-UUUU--RUZDZSE.
ZNR UUUUU ZUI RUEOMCG2742 1270159

HEADER

R
070158Z MAY 13
FM OSC RESTON VA

TO RUZFNEL/547IS NELLIS AFB NV
RUZDADA/AFIAA AMHS BOLLING AFB DC
RAYWAP/ATTORNEY GENERAL D BRANCH
RUZDADA/BUREAU OF ALCOHOL TOBACCO FIREARMS WASHI
RUEPPOG/CDR PSYOPGP FT BRAGG NC//ASOF-POG-SB//
RUOIAAA/CDR USPACOM HONOLULU HI
RUZFMXI/CDR USTRANSCOM INTEL CELL SCOTT AFB IL
RUEPNGA/CDRNGIC CHARLOTTESVILLE VA
RUEPWDC/DA AMHS WASHINGTON DC
RHEBAAA/DEPT OF ENERGY WASHINGTON DC//IN-1//
ZEN/DEPT OF TREASURY WASHINGTON DC
RHEFDIA/DIA WASHINGTON DC
RAYASAJ/DIO CANBERRA
[redacted] (b)(3)
RUEPMAX/GISA FT BRAGG NC
RAYAIK/HQJOC WASP
RUZDJWC/JWAC DAHLGREN VA
RUZDNAI/NASIC WRIGHT PATTERSON AFB OH
ZEN/NGA WASHINGTON DC
RUETIAA/NSACSS FT GEORGE G MEADE MD
RAYWBFA/ONA CANBERRA
RUCXONI/ONI WASHINGTON DC//2140//
RHHJJPI/PACOM IDHS HONOLULU HI
RUEKJCS/SECDEF WASHINGTON DC
RUEHC/SECSTATE WASHINGTON DC//INR//
RUDWNCR/SUSLAK SONGNAM KOR
RHHJRAP/USARPAC INTEL FT SHAFTER HI//APIN//
RUCQSAB/USSOCOM INTEL MACDILL AFB FL
BT

CONTROLS

UNCLAS
SECTION 1 OF 3
QQQQ
CITE OSC RESTON VA 985122

UNCLASSIFIED//

WARNING: TOPIC: INTERNATIONAL POLITICAL, MILITARY, TELECOM

SERIAL: CPP20130424787010

/******** THIS IS A COMBINED MESSAGE ********/

BODY

COUNTRY: CHINA, UNITED STATES

SUBJ: (U) PRC JOURNAL: CHINA, US SHOULD STRENGTHEN DIALOGUE, COOPERATION ON CYBER SECURITY

SOURCE: BEIJING LIAOWANG IN CHINESE 15 APR 13 NO. 15, P 52(U)

TEXT:

(U) Article by Shen Yamei: "The United States Sets Off a Cyberspace 'Supremacy Offensive'"

Publications

OSC Translated Text

The United States has always viewed the world with an intense hegemonic logic, and it has been difficult for them to scientifically acknowledge the new changes in their own environment and the international environment, to say nothing of objectively acknowledging China.

Recently, for no reason at all, US officials have denounced Chinese Internet secret-stealing activities as being a threat to US security, stirring up a "China Internet threat theory" and greatly elevating Internet problems as large problems in Sino-US relations. This is interfering with the hard work of China's current development of a new model major power relationship with the United States. China must expose the motives of the United States in this round of attacks, and at the same time, must also cleverly eliminate differences of opinion between China and the

United States in terms of Internet development and applications. China must work hard to transform cyberspace into a new domain for Sino-US dialogue and cooperation.

From the official speeches regarding the national situation since Obama's reelection, Assistant to the President for National Security Affairs the National Security Advisor Donilon's speech to the Asia Society, the remarks of Under Secretary of State Hormats on a recent visit to China, etc., it is apparent that the United States is putting every effort into using these trips to seize the high ground in cyberspace for the future. The United States has defamed China's Internet development from the economic, political, security, and other levels, and deduced from it a reproduction of the "China threat theory." In one aspect, this is also a manifestation of the fact that the United States has always viewed the world with an intense hegemonic logic, and it has been difficult for them to scientifically acknowledge the new changes in their own environment and the international environment, to say nothing of objectively acknowledging China.

The root origin of the various problems between China and the United States rests in the ebb and flow of the two sides' power and the obvious changes in attitudes. The United States has always held very deep strategic misgivings about China.

Economically, faced with the phenomenon of a large-scale shifting of wealth within the current international system ti xi, the United States has been unwilling to acknowledge the natural endowment of resources and system zhi du advantages that have brought about a rapid development of the Chinese economy, and at the same time, it has also been unwilling to squarely face the deep-level structural issue of a modest decline in its own competitive ability. Instead, it is blaming this on the outside world's activities of stealing via the Internet US intellectual property rights and commercial secrets, and it has illogically shifted "the majority of the blame" onto China. This aspect exposes the US sense of egotistic self-important stubbornness. It is even to the point that the United States has distorted the overall trend in the international situation of "the East rising and the West declining" since the financial crisis into the relevant nations pirating US developmental achievements. In another respect, this denouncement also completely overlooks the arduous hard work of the other nations of the world, including China, in search of development on the road to reform.

Politically, the United States is anxiously establishing

behavioral standards for cyberspace, and they have come out with this regulation formulation process with the intention of crowding out China. The techniques of the United States in vying for supremacy in the Internet domain share the same lineage with its usual tricks used in the handling of geopolitical issues in the Asia-Pacific, the Middle East, etc., namely, first building up and maintaining low intensity tension over the relevant issue, and then appearing to step in as an intermediary, a balancer, or mediator. Essentially, the United States is using the process of establishing rules and regulations, in which it is the leader, to constrain the other participants. Actually, back in August 2011, China, Russia, and other nations had already submitted a draft for an "international conduct standard for informati on security" to the United Nations, proposing that the international community formulate and implement international cyberspace standards. But the United States is now re-issuing a proposal of similar content, ignoring the contribution that China has already made to the international conversation on Internet security, and this exposes their global Internet strategy of a supremacy offensive.

/****** BEGINNING OF SECTION 2 ******
CITE OSC RESTON VA 985122

In terms of security, the United States needs to establish a target, and thereby drape its Internet attack activities in a veneer of legality and ethics. In recent years, the United States has strengthened its cyber warfare preparations, formulated cyber warfare regulations, and promoted a cyber command headquarters to increase and accelerate the intensity and speed of cyber military building. It has already incisively and thoroughly brought into play its advantages in network security technology and in policy and mechanism management. In the 2011 Strategy for Operating in Cyberspace, the US Department of Defense clearly listed the Internet as the fifth battlefield after sea, land, air, and space. It even stated that it would take military action against serious Internet attack activities. The US Government, Congress, military, media, and interest groups have coordinated with each other to contemptuously accused China of developing strategic Internet weapons, concoct lies about China carrying out Internet attacks against the US key infrastructure, and the like. They are using this to get their own piece of the pie in the national political agenda, the defense budget, and other actual interests.

In reality, it is the US' own actions in the domain of cyber

offense and defense that have put people in a state of high vigilance. In the example of the Iran nuclear issue, the United States kicked off a war of attrition early on in network, intelligence, and other secret action domains. In June of last year, The New York Times revealed that a network attack plan codenamed "Operation Olympic Games," that was aimed at Iran's nuclear facility, was formulated during the George W. Bush administration, and that after Obama took office, he accelerated the progression of this plan. Iran has frequently suffered computer virus attacks in recent years that have caused the Bushehr nuclear power plant, the Natanz uranium enrichment base, large petroleum corporations' internal networks, network operators, and other such industrial companies, as well as electronic government affairs and civilian networks, to be affected. It is publicly accepted that the main actors behind the scenes are the United States and Israel. US intelligence evaluations have also pointed out that the 2010 "Stuxnet" computer virus delayed Iran's possession of nuclear power by at least a year and a half. Some scholars in the United States have even recommended that Congress win US hackers over to its side, and that if they agree to only attack those nations and entities approved by Congress, then the government would give them immunity from prosecution, or even provide them with funding. It is obvious at a glance who is building a hacker empire.

In the Chinese view, the frequent occurrence of global Internet security incidents has really increased the urgency to protect Internet security. Still Internet attacks possess the characteristics of being transnational, anonymous, and deceptive. There is a great deal of uncertainty about the origin of the attacks, and this makes it difficult for any given nation fighting alone to achieve absolute Internet security. The issue of Internet security can completely become an excellent platform for creating international cooperation.

At this time, as the new content in international relations of the transition of authority between a rising power and the power holding onto its position is bestowed upon Sino-US relations, the differences of opinion and conflicts between China and the United States h ave seen a trend of being distributed over a wider area, running deeper, and being more closely connected. Scientifically acknowledging the differences of opinions is helpful to making the development of a new model major power relationship achieve possession of a definite object in view and pointedly putting an end to the drama of power politics. One could say that the conflicts and differences of opinions between China and the United

States in the aspect of Internet security are by no means fundamental or irreconcilable, but rather, that they contain the advantageous conditions for being transformed into conversation and cooperation, and they will not have a destructive effect on Sino-US relations by any means. Based on the considerations for building a new model major power relationship and promoting the establishment of international cyberspace regulations, the two nations of China and the United States should strengthen dialogue and actively promote cooperation in the areas of striking out against Internet crime and the administration of the Internet to reach more understanding and consensus on cyber sovereignty and military control of the Internet. The Chinese are steadfast advocates of Internet security cooperation, and they are optimistic about China and the United States holding more frequent direct conversations about this, and seeking to solve the problems through normal law enforcement cooperation and consultation while working hard to make the Internet become an active factor in spurring Sino-US relations.

Description of Source: Beijing Liaowang in Chinese -- weekly general affairs journal published by China's official news agency Xinhua, carrying articles on political, social, cultural, international, and economic issues

Source Metadata

Source Name:	Liaowang
Source Type(s):	Publications
Source City:	Beijing
Source Country:	China
Source Start Date:	15 Apr 13
Source End Date:	15 Apr 13
Language(s):	Chinese

Article Metadata

Document ID:	CPP20130424787010
Content Type:	Translation/Transcription

/****** BEGINNING OF SECTION 3 ******

Processing Ind:	OSC Translated Text
Precedence:	Routine
Country(s):	China, United States
Region(s):	Asia, Americas
Subregion(s):	East Asia, North Americas
Topic(s):	INTERNATIONAL POLITICAL, MILITARY, TELECOM

Attachments:

UNCLASSIFIED//

(Attachment not included: CPP20130424787010001.pdf) lw0415s.pdf

CABLETYPE: FBISEMS ACP 1.0.

ADMIN

BT
#2557

NNNN

UNCLASSIFIED//