UNCLASSIFIED//

ENVELOPE

RAAUZYUW RUEIFBS9601 3450418-UUUU--RUZDTPW.
ZNR UUUUU

HEADER

R
110417Z DEC 15
FM OSC RESTON VA

TO RUQVOLA/35IS LACKLAND AFB TX
RHMCSII/ATTORNEY GENERAL D BRANCH
RUACFOF/CDR501STMIBDE INTEL SEOUL KOR//IADK-OP-O//
RHMCSII/COMJSOC FT BRAGG NC
RUEPWDC/DA AMHS WASHINGTON DC
RHEBAAA/DEPT OF ENERGY WASHINGTON DC//IN-1//
RUEPTRX/DEPT OF TREASURY WASHINGTON DC
RHEFDIA/DIA WASHINGTON DC
RHHJJAA/JICPAC HONOLULU HI
RHMCSII/JOINT STAFF WASHINGTON DC//J5//
RUZDJWC/JWAC DAHLGREN VA
RUHDNCK/NCR KOR SEOUL KOR
ZEN/NGA WASHINGTON DC
RHHJJPI/PACOM IDHS HONOLULU HI
RHMCSII/SECDEF WASHINGTON DC
RHMCSII/SECSTATE WASHINGTON DC//INR//
RUDWNCR/SUSLAK SONGNAM KOR
RUMICEA/USCENTCOM INTEL CEN MACDILL AFB FL
RHMCSII/USSOCOM INTEL MACDILL AFB FL
ZEN/CIA WASHINGTON DC
BT

CONTROLS

UNCLAS
QQQQ
CITE OSC RESTON VA 581460

WARNING: TOPIC: INTERNATIONAL POLITICAL, TECHNOLOGY
SERIAL:KPR2015121060229029

BODY

COUNTRY: NORTH KOREA, SOUTH KOREA, UNITED STATES

UNCLASSIFIED//

SUBJ: (U) DPRK PARTY DAILY BLAMES US FOR OPENING UP 'PRELUDE' TO 'Cyber War'

SOURCE: Pyongyang Rodong Sinmun (Electronic Edition) in Korean 19 Nov 15 (U)

TEXT:

[(U) "Analysis of the Situation" by Rim Wo'n: "The Great Criminal Power That Opened Up a Prelude to Cyber Warfare"]

[INTERNET]

[OSC Translated Text]

As science and technology develop at a rapid pace in the current era, the level of human civilization continues to advance further, and the world's countenance continues to change with each passing day.

The rapid development of science and technology tightens the bonds and exchanges between countries even more closely.

Mankind points its aspirations towards advancing scientific and technological development for the sake of common prosperity.

Running counter to this, however, there are forces running amok in an attempt to adopt even mankind's achievements in science and technology development as a means of warfare, in an attempt to realize their ambition for world domination. They are none other than the United States.

This is clearly demonstrated by the single fact that the United States has labeled cyberspace as the "fifth domain of warfare."

The United States is trying to turn not only the sky, land, sea,

and
space, but also cyberspace, into one of their battlefields, in order
to realize their ambition for world domination.

Recently, a Swedish newspaper, "Dagens Nyheter," exposed the fact that the United States executed an attack against Iran's nuclear facilities by developing a new malicious program called "Mask," which
is a reinforced version of "Stuxnet," a cyber attack program, in 2010.

"Stuxnet," detected in 2010, was co-developed by the United States and Israel, and it is known to be the most fatal means of cyber attack in history.

The United States, which was displeased with Iran's peaceful nuclear
development, has long been maneuvering directly and indirectly, in order to bring it to ruin.

Since 1996, under the objective of obstructing Iran's peaceful nuclear development, the United States has been pursuing a cyber-attack operation with the code name, "Olympic Games."

Having developed a cyber attack program called "Stuxnet" during 2005-2007, they delayed Iran's construction of nuclear facilities with attacks on the electrical systems of Iran's nuclear facilities.

Afterwards, Obama, who assumed the position of president, received a
briefing on a top-secret plan regarding cyber attacks against Iran's
nuclear facilities, that had been executed during the previous Bush administration, and gave the secret order to further expand [the plan]. Accordingly, by first infiltrating the computer systems of Iran's nuclear facilities with a program called "Beacon," the United
States stole the blueprints to interior operations at the nuclear facilities.

Meanwhile in 2010, they developed "Mask," a new malicious program that reinforced "Stuxnet," and executed another attack on Iran's nuclear facilities. As a result, in June of that year [2010], 1,000 centrifuges installed in Iran's Natanz nuclear facility were forced

to suspend operations temporarily.

Nevertheless, whenever there has been an opportunity in the past, the United States has clamored until it was blue in the face, that its actions in the cyber sector are thoroughly "defensive in nature."

However, there is no way to hide an awl in a sack.

In a publication concerning the world's cyber warfare, a US reporter argued that the United States' cyber attack on Iran's nuclear facilities has opened up the prelude to a new, international cyber war.

Snowden, who used to be an agent for the US National Security Agency [NSA], also revealed that "the era of cyber attack has arrived by means of the United States' execution of a malicious virus attack against Iran."

Although the malicious program "Mask" achieved its desired objective by infiltrating Iran's nuclear facilities, the secret leaked out through various channels, and it ultimately became open to the public.

On this occasion, the dark secret of the United States' cyber warfare against Iran was once again exposed to the entire world.

The United States' acts of cyber attack are not only limited to Iran.

The United States, with various countries in the world as its targets, is carrying out acts of cyber attack without hesitation.

Its major targets are anti-US, independent countries, including our country.

Only recently, the United States evoked public criticism after it was revealed that it had failed in an attempt to destroy our country's nuclear facilities by using the cyber attack program, "Stuxnet."

Allies also are not exempted from being targets of cyber attack by

the United States. The United States extensively carried out the act
of wire-tapping the phones of high-ranking French officials, by developing a program called "US-985D."

Regarding this [act], the French newspaper, "[Le] Monde," disclosed that the US NSA had secretly recorded more than 70 million phone conversations in France for one month starting in December 2012.

In this manner, the United States has carried out cyber attack operations all over the world and the number of [operations] cases reached no fewer than 230 cases in 2011 alone.

According to publicly available documents, the United States has invested 652 million US dollars to carry out operations infiltrating
the communications and computer networks of various countries in the
world, to hack into relevant data.

As all the facts show, the United States is the main culprit, who not
only started state-level cyber attacks before anyone else, but also turned cyberspace into a battlefield.

The world is raising its voice in denunciation of the United States,
which runs amok recklessly while abusing achievements in scientific and technological development -- which should contribute to human civilization and development -- as a means of its war of aggression against other countries and its infringement upon their sovereignty.

[Click here to view vernacular in its original format.]

[Click here to download the BiLingual file for this item.]
[Description of Source: Pyongyang Rodong Sinmun (Electronic Edition) in Korean -- Daily of the Central Committee of the Workers Party of Korea; posted on the Korean Press Media (KPM) website run by
the pro-Pyongyang General Association of Korean Residents in Japan; URL: http://dprkmedia.com]

only.
Any reproduction, dissemination, or use is subject to the OSC usage policy and the original copyright.
- BiLingRS20151119001.pdf - RS20151119001.pdf

CABLETYPE: FBISEMS ACP 1.0

The following attachments were removed from the message:
BiLingRS20151119001.pdf
RS20151119001.pdf

ADMIN

BT
#9601

NNNN