UNCLASSIFIED//

ENVELOPE

RATUZYUW RUEIFBS9229 2211124-UUUU--RUZDTPW.
ZNR UUUUU ZUI RUEOMCG3444 2211125

HEADER

R
081124Z AUG 12
FM OSC RESTON VA

TO RUZFNEL/547IS NELLIS AFB NV
RAYWAP/ATTORNEY GENERAL D BRANCH
RUZDADA/BUREAU OF ALCOHOL TOBACCO FIREARMS WASHI
RUOIAAA/CDR USPACOM HONOLULU HI
RUZFMXI/CDR USTRANSCOM INTEL CELL SCOTT AFB IL
RUEPNGA/CDRNGIC CHARLOTTESVILLE VA
RHMFISS/CDRUSASOIC WASHINGTON DC
RUEPWDC/DA AMHS WASHINGTON DC
RHEBAAA/DEPT OF ENERGY WASHINGTON DC//IN-1//
RUEPTRS/DEPT OF TREASURY WASHINGTON DC
RHEFDIA/DIA WASHINGTON DC
RAYASAJ/DIO CANBERRA
[redacted] (b)(3)
RUOIAAA/DIRNAVCRIMINVSERV QUANTICO VA
RHMFISS/DIRNAVCRIMINVSERV QUANTICO VA
RUEPMAX/GISA FT BRAGG NC
RAYAIK/HQJOC WASP
RUZDJWC/JWAC DAHLGREN VA
RUZDQAN/MARCORINTACT QUANTICO VA
RUZDNAI/NASIC WRIGHT PATTERSON AFB OH
RUGIZZZ/NGA DISSEM WASHINGTON DC
RUETIAA/NSACSS FT GEORGE G MEADE MD
RAYWBFA/ONA CANBERRA
RUCXONI/ONI WASHINGTON DC//2140//
RHMFIUU/PACAF IDHS HICKAM AFB HI
RHHJJPI/PACOM IDHS HONOLULU HI
RUEKJCS/SECDEF WASHINGTON DC
RUEHC/SECSTATE WASHINGTON DC//INR//
RUZEADH/UDITDUSAREUR HEIDELBERG GE
RUMICED/USAFCENT INTEL SHAW AFB SC//A2//
RHHJRAP/USARPAC INTEL FT SHAFTER HI//APIN//
RUMICEA/USCENTCOM INTEL CEN MACDILL AFB FL
RUCQSAB/USSOCOM INTEL MACDILL AFB FL
BT

CONTROLS

UNCLASSIFIED//

UNCLAS
SECTION 1 OF 2
QQQQ
CITE OSC RESTON VA 982628

WARNING: TOPIC: DOMESTIC POLITICAL, INTERNATIONAL POLITICAL, LEADER, TECHNOLOGY

SERIAL: SAP20120808118004

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

BODY

COUNTRY: PAKISTAN, IRAN, ISRAEL, UNITED STATES

SUBJ: (U) PAKISTAN ARTICLE WARNS INTERNATIONAL COMMUNITY OF DANGERS OF CYBER WARFARE

SOURCE: ISLAMABAD THE NATION ONLINE IN ENGLISH 08 AUG 12 (U)

TEXT:

(U) Article by S M Hali: "Cyberwarfare - New Arms Race"

Internet

OSC Transcribed Text

Text disseminated as received without OSC editorial intervention

Cyberwarfare has been defined as politically-motivated hacking to conduct sabotage and espionage. It is a kind of information warfare that some pundits compare to conventional warfare, although this analogy is controversial and has dangerous implications meriting closer examination. Richard A. Clarke, US government security expert, in his book Cyber War (May 2010), defines: "Cyberwarfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes

of causing damage or disruption." The Economist describes cyberspace as "the fifth domain of warfare", while William J. Lynn, US Deputy Secretary of Defence, states that "as a doctrinal matter, the Pentagon has formally recognised cyberspace as a new domain in warfare.....which has become just as critical to military operations as land, sea, air and space."

These perilous trends are evident from the disclosure made by David E. Sanger, Chief Washington Correspondent for the New York Times, in his new book Confront and Conceal (June 2012). He discloses that in an effort to disrupt Iran's quest for developing nuclear weapons and desisting Israel from militarily attacking Iranian nuclear facilities, US President George W. Bush had authorised the joint US-Israeli development of cyber weapons to sabotage Iranian nuclear plants. According to Sanger, the operation codenamed "Olympic Games" instituted in 2006 aimed at creating a computer worm, which would penetrate and destroy Iran's nuclear facilities. Sanger's chilling narrative - based on interviews of current and former American, European and Israeli officials involved in the programme - reveals that the first stage involved inserting a "beacon" into the Iranian computers, with the help of a clandestine action through the German company Siemens and an Iranian manufacturer to map their operations. The goal was to gain access to the Natanz plant's industrial computer controls by leaping the electronic moat, which cut it (the plant) off from the Internet called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialised computers that command the centrifuges. This enabled the beacon to draw the equivalent of an electrical blueprint of the Natanz plant to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds, seize control of the centrifuges and facilitate their failure by electronically varying their speed of rotation, causing the rotors to destroy the centrifuge.

For years, the CIA had introduced faulty parts and designs into Iran's systems - even tinkering with imported power supplies so that they would blow up - but the sabotage had had relatively little effect. Under "Olympic Games", the US-Israeli nexus developed a complex worm that necessitated testing.

Sanger divulges that the US began building replicas of Iran's P-1 centrifuges, an aging, unreliable design. The US already owned some P-1s, which the Libyan strongman, Colonel Moammar Al-Qaddafi, had reportedly acquired from Pakistan and then surrendered to the US in 2003, which were placed in storage at a

weapons laboratory in Tennessee. The military and intelligence officials overseeing "Olympic Games" borrowed some for what they termed "destructive testing", essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department's national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Sanger reveals that President Barack Obama authorised the cyber attacks on Natanz and despite a 2010 hiccup, destroyed more than 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium, setting back the Iranian nuclear programme by 18 months. The US government only recently acknowledged developing cyber weapons, but has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al-Qaeda, and of contemplated attacks against the computers that run air defence systems, including during the Nato-led air attack on Libya last year. But "Olympic Games" was of an entirely different type and sophistication.

/****** BEGINNING OF SECTION 2 ******

Apparently, for the first time, the US has repeatedly used cyber weapons to cripple another country's infrastructure, achieving with computer code what until then could be accomplished only by bombing a country or sending in agents to plant explosives. In executing these attacks, the US has unleashed a new weapon, which can have lethal consequences. Imagine disrupting air traffic operations or the power sources of a hostile nation, which could cripple hospitals and banks. The demon unleashed through cyberwarfare can well target the US too and would know no bounds. To rein in this latest arms race, the rules of engagement must be redrawn to avoid an apocalypse.

Description of Source: Islamabad The Nation Online in English -- Website of a conservative daily, part of the Nawa-i-Waqt publishing group. Circulation around 20,000; URL: http://www.nation.com.pk

Source Metadata
Source Name: The Nation Online
Source Type(s): Internet

Source City: Islamabad
Source Country: Pakistan
Source Start Date: 08 Aug 12
Source End Date: 08 Aug 12
Language(s): English

Article Metadata
Document ID: SAP20120808118004
Content Type: Translation/Transcription
Processing Ind: OSC Transcribed Text
Precedence: Routine
Country(s): Pakistan, Iran, Israel, United States
Region(s): Asia, Middle East, Americas
Subregion(s): South Asia, Middle East, North Americas
Topic(s): DOMESTIC POLITICAL, INTERNATIONAL POLITICAL, LEADER, TECHNOLOGY

CABLETYPE: FBISEMS ACP 1.0.

ADMIN

BT
#9230

NNNN