ieee.es
Instituto Español de Estudios Estratégicos

Informative
Document

56/2012 August 28th 2012

*María José Caro Bejarano*

DYLEMA: TRAINING AND RECRUITING HACKERS?



*This document has been translated by a Translation and Interpreting Degree student doing work experience, VIRGINIA RUIZ, under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute of Strategic Studies.*

# DYLEMA: TRAINING AND RECRUITING HACKERS?

## Abstract:

Many countries have approved or are in process of approving national cyber security strategies aimed at protecting their networks and computer systems, as well as their critical infrastructure connected to the Internet. Some countries have chosen to train or hire hackers as software agents in order to prevent possible attacks on the Internet. North Korea has chosen the former option and a U.S. expert suggests the latter one.

## Keywords:

Hacker, cyber security strategy, cyber threats.

**DYLEMA: RECRUITING AND TRAINING HACKERS INSTEAD OF CHASING THEM**

Many countries have approved or are in process of approving national cyber security strategies aimed at protecting their networks and computer systems, as well as their critical infrastructure connected to the Internet. Some countries have chosen to train or hire hackers as software agents in order to prevent possible attacks on the Internet.

The Government of South Korea is an example of training hackers: it has implemented a program, known as *Best of the best,* which is aimed at training hackers in order to fight against possible attacks on the Internet.

The cyber security of South Korea has been called into question many times in the last few years due to the attacks that have blocked temporarily the websites of ministries, official organisms and even bank institutions.

The Government usually attributes these attacks to hackers from North Korea. They often launch Distributed Denial of Service (DDoS) attacks, which overload the connection points of the servers until they stop working.

The DDoS attack (Distributed Denial of Service attack) and the so-called APTs (Advanced Persistent Threats) are the two most frequently used attacks on the Internet. The APTs are a new type of organized attacks which are focused on international organizations, governments and security forces.

Last July, the Government of South Korea announced its plans of recruiting and training six hacker students as computer agents whose mission will be fighting threats to the cyber security of the country, as the Ministry of Knowledge Economy at Seoul has informed.

A group of experts will select six 'white hat' hackers, which in the computers jargon refers to a hacker ethics focused on assuring the protection of systems and is different from the 'black hat' technique, which involves illegal activities.

The Government of South Korea will allocate more than 1.3 million Euros to this project. Each of the selected students will cover one of the six areas that have been established, which range from protection against cybernetic attacks to institutions to the security of smartphones.

Last June, the officials of the Government of South Korea interviewed 238 highly qualified young hackers, all of them undergraduate and postgraduate students, and selected 60 of them; however, only six will get to the final phase.

The selected students will receive a scholarship of almost 14,000 Euros, as well as the opportunity to study abroad and be a part of the human resources database of the National Intelligence Agency and the Police of South Korea.

The director of the Korea Information Technology Research Institute, Yoo Jun-sang, told the local newspaper Dong-a Ilbo that the Government had started this initiative because the country "does not have enough human resources devoted to security" to prevent attacks on the Internet.

John Arquilla[1], professor of defense analysis at the Naval Postgraduate School of Monterrey, California, supports the second option, hiring hackers, as he declared in an interview for The Guardian.

According to Arquilla, the US Government, instead of chasing top hackers, should recruit them to launch cybernetic attacks against Islamic terrorists and other enemies.

This remarkable military analyst and Government counselor considers that the US have lagged behind in the cybernetic race and need to establish a "new Bletchley Park" of IT geniuses and code hackers in order to detect, track and dismantle enemy networks.

Bletchley Park is the name of a Victorian house located in Buckinghamshire, England, which was used as a military facility during the Second World War and where German codes were decrypted. The first Colossus computer, which allowed the decryption of the codes of the German machine Enigma, was designed and built in this facility. According to some experts, decoding those encrypted messages with this machine made it possible to end the war two years before.

Arquilla, who created the term cyberwar twenty years ago, declared that only a few expert hackers have been recruited, but more are needed. He mentioned a parallelism between the German scientists that were hired after the Second World War, such as Braun, the best scientist at Hitler's service, who became an American hero after working in the US rockets and special programs.

The cybernetic threaten is no longer an exaggeration, as some skeptical people used to think. In 2011, the Pentagon made public a new strategy to protect military networks from

[1] Arquilla was an advisor of General Schwarzkopf during the first Gulf War and an advisor of Donald Rumsfeld, Secretary of Defense, during the second Gulf War.

hackers and gave the cyberspace the status of “global common”, just like land, sea, air and space.

The Stuxnet worm that attacked Iran’s nuclear program showed the true potential of what Arquilla called “cybotage” (a term that combines the words “cyber” and “sabotage”).

According to Arquilla, cybernetic attacks are more effective when they are combined with military strategies. He declared that Russia was a pioneer using this type of strategy during the conflict with Georgia in August 2008.

Moscu denied to have directed these cyberoperations and the origin of them was never proved. Previously, in 2007, Estonian computer and communication networks had suffered a cybernetic attack that was considered by some experts as the first case of cyberwar. Arquilla thinks that “everything is still hidden, but Russian are the true leaders in this field”. “China and North Korea also understand the strategic uses of cybernetic attacks”.

Arquilla urged US state agencies and companies to use strong encryption and cloud computing.

Finally, he accused the Pentagon and its political leaders of wasting billions of dollars in aircraft carriers, tanks and planes instead of implementing a more agile and better adapted to reality strategy.

*Mª José Caro Bejarano*
Analyst at the IEEE