Feb 27, 2015 5:13 PM

Package: General

Category: Science, Technology Politics

Priority: 5 Feature

Location: Ankara

Publisher: Mert Bezgin

Author: Andrew Jay Rosenbaum

Cyber warfare threat rapidly increasing: Experts

- Weaponized software becoming dangerous threat to governments and business, experts warn.

By Andrew Jay Rosenbaum

ANKARA (AA) - Cyber warfare is on the rise, experts warn.

"Cyber warfare is increasing in frequency, scale, and sophistication," the U.S. Director of National Intelligence James Clapper told Congress on Thursday.

Clapper said Russia is among the most sophisticated cyber warfare states.

"While I can't go into detail here, the Russian cyber threat is more severe than we've previously assessed," he added.

Chinese advanced cyber espionage is "a major threat" and is continuing despite U.S. pressure on Beijing, Clapper said.

But not only governments are threatened by cyber weapons. The financial industry, Clapper said, is facing increasing threats from cyber criminals. "Criminals were responsible for cyber intrusions in 2014 in JPMorgan, Home Depot, Target, Neiman Marcus, Anthem, and other U.S. companies," he said.

This year has seen a critical increase in the creation of cyber weapons, Oguz Yilmaz, chief technology officer of the Ankara-based Labris Networks, told The Anadolu

Agency on Friday.

"We can say cyber weaponization has started and will continually increase in 2015," Yilmaz said.

He also said that terrorists, too, are getting cyber weapon technology.

"The Syrian Electronic Army and ISIS groups are examples, they have claimed responsibility for such incidents," Yilmaz said, using an abbreviation for the militant Islamic State of Iraq and the Levant, also known as Daesh.

"At the moment, these incidents are at the level of getting control of some web pages and Twitter accounts; these and other non-governmental groups may increase the depth of attacks," he said.

"We see that specially crafted espionage malware and malware-based surveillance operations started to address countries other than the U.S., U.K., China, and Russia," Yilmaz warned. "We expect cyber espionage will be a standard method for non-war interstate espionage relations. The geopolitical landscape will interfere with cyberspace more."

- What is a cyber weapon

There have been a number of proposals at the United Nations and in international forums to control or regulate cyber weapons.

"A weapon is generally understood to be an instrument of offensive or defensive combat, and has been defined as a device that is designed to kill, injure, or disable people, or to damage or destroy property," explained Chatham House expert Louise Arimatsu in London.

“Although this definition might adequately encapsulate traditional weapons that have been designed, when utilized, to have a direct kinetic outcome, it fails to capture the essence of what are generally regarded as cyber weapons. This is because most of the malicious codes or malware that would fall within the parameters of a cyber weapon are not designed to kill, injure or disable people nor, necessarily, to damage or destroy tangible property," Arimatsu explained.

"A cyber weapon is malicious code that is intended to kill or injure people or to destroy property," Arimatsu said.

Since 2009, legal experts have been at work on a manual that defines the law governing cyber warfare. It is now referred to as the "Tallinn Manual," and is being refined by contributions from around the world.

The manual highlights many of the issues involving cyber warfare. When does a cyber war begin, and when does it end? How is a cyber attack defined (as opposed to hacking or just network penetration). When is a country attacked? For example, if a business in the country is attacked, is this war?

These kinds of questions still make controlling cyber warfare a challenge. But the U.S. Defense Department has, nonetheless, put together a classified list of cyber weapons which it considers clearly dangerous and threatening in the broadest sense.

A good example of a cyber weapon is the malware Duqu, a note from the Infosec Institute explained.

"It has a state-sponsored origin and mainly a cyber espionage purpose. Despite this characteristic, security firms have recognized that it has been developed using the same platform that created Stuxnet, the 'Tilded Platform.' The malware created the innovative platforms that are known to have a modular structure that specify their behavior. This means that Duqu equipped with proper components is also adoptable for offensive purposes," the note said.

- Responding to attacks

When Sony Pictures was attacked in November 2014, allegedly by North Korean cyber weapons, President Barack Obama said that the U.S., as a country, would respond to the attack.

In December, North Korea suffered a nine-hour Internet outage and the government blamed a U.S. cyber attack.

Without assuming that the attack on North Korea was a U.S. armed response, experts ask what kind of response would have been appropriate, and by whom?

In November, U.S. Cyber Command held war game exercises with the forces of the U.K., in an effort to nail down an answer to that question.

Navy Adm. Mike Rogers, who is also director of the National Security Agency -- said in a statement that the exercise "Cyber Flag" was "force-on-force" training, "fusing attack and defense across the full spectrum of military operations in a closed network environment."

This is a start from the point of view of national governments, but what should businesses do?

For now, cyber warfare theory dictates that attacks by sovereign states, even on private companies, should be responded to by sovereign states. Legal experts are still working this out, but the doctrine provides comfort for businesses who fear suffering the same fate as Sony Pictures.

"But businesses will also suffer attacks from gangs of cyber criminals who dispose of the same technology as countries," Yilmaz said. "This is the time for them to take the necessary measures for protection."

www.aa.com.tr/en

Cyber warfare computers viruses