CYBER WAR –
A HARDLY CONTESTABLE REALITY NOWADAYS

Major General (Ret.) Associated Professor Constantin MINCU, PhD*

Abstract: *This article is a follow-up of the material published in our journal no. 2 (42)/2016, entitled „*CYBER ATTACKS, MAJOR THREATS AND VULNERABILITIES AGAINST STATES, ORGANISATIONS AND CITIZENS*". We considered this follow-up necessary due to the recent events and, mainly, to the situations created in Great Britain and United States of America by the massive and diversified cyber attacks intended to influence the political process in these countries. We also consider that it is very interesting to study the attacks against certain institutions and companies in some EU and/or NATO countries and the need to take some firm and diversified measures of defence.*

Keywords: *cyber war, cyber attacks, UK, US, Russian Federation, Romania.*

The issue of cyber attacks that are increasingly aggressive and the clearer shaping of their transformation into real *cyber war*s has become a public topic of maximum importance and led to a more active and responsible approach of the states, organizations, individual users and, of course, IT professionals.

A brief history of these attacks shows that they have intensified after 2007 (when a state actor launched the *Red October* virus) and followed by other ample hostile actions that caused extensive damage to political, economic, financial and image fields of the targeted states and organizations.

There were also recent episodes illustrating the involvement of some state actors and organized groups supported financially and logistically by

* Entitled member of Romanian Scientists Academy, Member of the Honorific Council of the Romanian Scientists Academy, Scientific secretary of the Military Science Section. Phone: 0722.303.015, Email: mincu_constantin@yahoo.com.

state actors, as the case was in the political process of the Great Britain's exit from the European Union – BREXIT, and later, the involvement with potentially serious political effects by direct attacks, information theft and dissemination of false information within the target audience (already famous trolls) in a desperate attempt to influence the presidential elections in the US. All these have heightened the confrontation to another level, rendering us able to speak clearly, with arguments, about *cyber war.*

Evolvements of cyber attacks in-between 2014-2016

The Ukrainian-Russian conflict in 2014 followed by more or less firm reactions from EU and/or NATO Member States led to the worsening of political, diplomatic, economic and cultural relations between the Russian Federation and the democratic states mentioned. The annexation of Crimea and its involvement in the conflict in Eastern Ukraine have shown unequivocally the aggressive face of Russia, giving rise to concerns primarily among its neighbouring states.

This new situation with important geopolitical implications in the near future could not remain without effect in the cyber confrontation as well. That is why almost all European countries, EU members states, as well as NATO member states, found themselves with powerful and daily attacks on political, government, financial, industrial and media institutions, leading to serious security, economic, financial losses followed by harming citizens' morale through different methods including the introduction of false reports and diversions manufactured by old professionals in the field.

Let us try a short inventory:

a) The Russian-Ukrainian case shows the aggressive and unscrupulous manner of demonization by the Russians of their neighbour country and former part of the Soviet Empire. By media vectors controlled by Kremlin (from Russia and abroad) false news was spread to deny the involvement of Russian military forces in Crimea and in the Eastern Ukraine.

Cyber attacks were triggered on all major institutions of the Ukrainian state (parliament, government, armed forces, security services and economic infrastructure) along with the development of complex and sophisticated actions influencing public opinion in Western countries by

using, primarily, social networks and online media publications. In many cases these actions have produced the expected results.

b) BREXIT case

It is already famous that Moscow aims to weaken the European cohesion; it acts so as to separate some member states in the EU from the others and intends to weaken the EU-US relations and therefore to undermine NATO. By triggering a referendum in the UK whether to remain within or exit the European Union was a clear example in which forces controlled by the Kremlin, worldwide and in the target country in this scenario, put together a true school case by making use without economy of forces and means to influence British citizens by media vectors and cyber attacks on key institutions of the state.

Attack topics:

- EU is a profound bureaucratic institution similar to the former Soviet Union;
- UK lost part of its political and economic sovereignty;
- UK contributes far too large amounts of money to the community budget favouring poorer member countries in Central and Eastern Europe;
- The citizens of some EU member states are largely immigrating to the UK suffocating social services and "stealing" workplaces from British citizens;
- Some European leaders adopted a "disastrous" policy in the issue of admitting immigrants from the conflict areas (Syria, Iraq, North Africa, etc.).

As we already know the referendum was on the edge and the share of votes brought by the actions presented above could not be neglected.

c) The case of presidential elections in the United States of America

A former superpower called the Soviet Union and its main heir called the Russian Federation (that aspires to occupy the place previously held during the Cold War) could not miss the involvement in the most important political event of 2016 - the election of a new US president. After a long and thorough analysis using various sources of information, including

massive theft from the electronic systems of the competitors and those close to them, Moscow decided to go over to the candidate Donald Trump, considered by Russians more pragmatic and realistic and, according to his statements, willing to let NATO go, along with Article 5.

Attack themes on democrat candidate Hillary Clinton:

- The Democrat candidate is unpredictable and corrupt, receiving money by the means of Clinton foundation from the Arab countries;
- Theft and publication of thousands of emails of hers and her staff members with the clear goal of vilification and incitement of American investigative bodies;
- If she is elected, the confrontation between Russia and US will get closer to the level of danger (thesis also supported by her competitor Donald Trump)[1];
- Hillary Clinton may have been influenced by occult circles of power which will aim at achieving global dominance and the dismantling of Russian Federation;
- NATO is useless now as a political-military alliance in the recent circumstances (this idea coincided with the attack against NATO initiated by the republican candidate Donald Trump);
- Russia must „take back" its pieces detached from the Soviet Union and US have no right to intervene against it;
- Russia must defend without hesitation the Russians placed in the former USSR territory (about 25 millions) without caring about the criticism coming from USA and the European allies;
- Russia recovered politically, economically and military and can always be a deadly threat for US and NATO (it brings up the nuclear threat more and more often);

In this tensioned context of Russia – US and Russia – EU relations it is necessary to present some Western reactions to the latest cyber attacks and intrusions along the electoral process of the United States[2]:

- US government officially accused Russia on Friday, 11.10.2016, of a recent campaign of cyber attacks against some organizations of US Democrat Party, Reuters transmits;

[1] The article was written before the presidential elections from USA (06.11.2016).
[2] Site: antena3.ro/externe/sua-acuză-rusia-de-atacuri-cibernetice-380293.html.

• In the late months, many American officials stated the respective cyber attacks were performed by hackers supported by Moscow, perhaps to disturb the presidential elections where the democrat Hillary Clinton confronted the republican Donald Trump. Russia rejected these accusations (a. n. – in its usual behaviour when it comes to its aggressive actions);

• **Department of Homeland Security (DHS) and the Office of the Director of National Intelligence** transmitted on Friday (11.10.2016) to the mass-media a joint declaration quoted as a whole by Reuters:

• „The US intelligence community (USIC) is convinced that the Russian Government has directed the recent compromise of e-mails of US individuals and institutions, including those of some American political organizations. The recent revelations of alleged emails hacked on websites such as DCLeaks.com and WikiLeaks and the online character Guccifer 2.0 are consistent with the methods and motivations routed by Russia. These storms and disclosures are made with the intention of interfering in the electoral process in the US. Such activities are not new to Moscow - the Russians have used such tactics and techniques across Europe and Eurasia, for example, to influence public opinion. We believe, given the scale and sensitivity of these efforts, that only the highest Russian officials could have authorized such activities";

• „Also some states have recently observed scanning and testing their election-related systems which in most cases have originated in servers managed by a Russian company. However, we are now in a position to assign these activities to the Russian Government. USIC and Department of Homeland Security (DHS) appreciate that it would be extremely difficult for anyone, including for a non-state actor, to modify the actual count of votes or election results by cyber attacks or intrusions. This assessment is based on the decentralized nature of our electoral system in this country and the number of protection means implemented by state and local election authorities. The states ensure that voting equipment is not connected to the internet and there are multiple control mechanisms and an extensive surveillance on multiple levels inherent in our electoral process";

• After the last attacks on 11 November the White House reacted[3]:

• The response will be „proportional", press secretary of the White House Josh Eamest said, without elaborating. He said a "register" of possible responses is on the table. By Friday's announcement it was the first time the US government had publicly blamed another country on cyber attacks in order to influence US elections. The Joint Declaration of the Department of Homeland Security and the Office of the Director of National Intelligence said not only that officials are confident that the attacks on political democratic groups and campaign' officials came from high levels of the Russian government, and that the online publication of these e-mails it was part of the effort;

• National security counsellor Lisa Monaco mentioned for Washington Post, last week (12.10.2016), what the government could generally do in response to these attacks. *„We will meet at a time, place and method of our choosing, and when we do this we will consider a full range of instruments: economic, diplomatic, criminal law, military, and some of these reactions may be public, but some of them may not be"*.

d) The case of massive cyber attacks over some IT services:

• Friday, 21.10.2016, some attacks over Twitter, Spotify and eBay some attacks were produced against the networks;

• Their goal was to discourage and confuse American users and not only around the presidential elections in 8 November;

• Concomitantly, the authors of the attacks wanted to prove that they do not care about the positions expressed by some American officials on 11 and 12 October this year.

Cyber attacks over European Union countries

No EU country has escaped in recent years the cyber attacks orchestrated by state actors or organized groups supported by them.

Of all European countries, Germany emerges as a main target, as many attacks were triggered against it targeting political organizations, ministries, industrial infrastructure, financial and media organizations. Some

[3] http://adevărul.ro/continut/ştiri/casa-albă.

German officials accused Russia of these attacks. But there are indications that attacks were orchestrated also by other centres of power.

Surprisingly, some European countries were spared and suffered only marginal attacks. For understandable reasons it would not be a good idea to nominate them, especially since some of these states are undergoing electoral processes.

Cyber attacks against organizations in Romania

RIS official as well as other institutions recognize that the recrudescence of the cyber attacks came from different sources, aiming to damage political institutions, national defence and security, financial organizations, multinational companies operating in Romania but also small local enterprises.

Also, the attacks came from terrorist groups intensified against some high education and public administration institutions as well against a website of Romanian Patriarchy.

Romanian officials rightly consider that *„this complex context highlights the need to implement minimum standards for cyber security in the computer systems owned by public and private entities, as well as regular verification of the compliance with the norms and policies in this area"*[4]

For Romania, a subject of analysis could also be the unusual intense activism of the so-called troll posting to the topics launched on news sites and social networks.

We watched particularly the posts on the topics concerning the armed forces and defence and we could see that regarding the most harmless and usual topics inaccurate and unfair attacks were launched against the institution and the active, reserve and retired military. We promise we will try to come back with a more comprehensive analysis on this subject.

Regarding Romania we believe that the strengthening of the legal and regulatory framework followed by practical action for implementation are both urgent and necessary.

[4] www.sri.ro/romania-a-fost-ținta-unor-atacuri-cibernetice.html

Note (09.11.2016)

Unfortunately, the cyber attacks and the other types of attacks involved in the political process of US elections have had the effects aimed by the initiators.

BIBLIOGRAPHY

*** *National Defence Strategy,* Bucharest, 2010 (in Romanian: Strategia Națională de Apărare, *Bucureşti, 2010);*

*** Cyber Security Strategy of Romania, approved by the SCCD, in February 2013 (in Romanian: Strategia de Securitate Cibernetică a României, aprobată de CSAT, în luna februarie 2013);

*** *Draft Law on Cyber Security of Romania launched in public debate by the MRYI*, in January 2016 (in Romanian: Proiect de Lege privind Securitatea Cibemetică a României, lansat în dezbatere publică de către MCTI, în luna Ianuarie 2016);

*** *National Defence Strategy Guide for the years 2015-2019*, approved by SCCD no. 128, on December 10, 2015 (in Romanian: Ghidul Strategiei Naționale de Apărare a țării pentru perioada 2015-2019, aprobat prin Hotărârea CSAT nr. 128, din 10 decembrie 2015);

Durmigan F. James, *Noua amenințare mondială - Cyber-Terorismul,* Editura Curtea Veche, Bucureşti, 2010;

Raiu Costin, *Laboratoarele Kaspersky,* Interviu acordat Ziarului Adevărul, 19 februarie 2013;

www.internetworldstats.com/stats.html

http://www.nato.int/dom/review/2011111-september/Cyber-ThreadsIRO/index.htm http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/

Other profile sites by searching “cyber attacks”.