Suspension of pipeline geopolitics. Cyber-warfare in Balkan Peninsula?

By Selim Ibraimi,MA International Relations, Webster University at Scott Air Force Base,Il USA.

Abstract

Energy infrastructure is related to the cyber-warfare. Cyber- warfare is Internet-based conflict involving politically motivated attacks on information network systems.
Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal classified data, and cripple financial systems — among many other possibilities with unexpected consequences for national security. Government agencies spent billion of dollars to protect systems. In the Western Balkan, states are not aware of the threats.

Introduction

The way of future wars depend on how they will be conducted. The end of cyber-warfare attacks and which state is going to win the war on security is the strategic theme of all leaders and national security experts.
The aim of this papers consist on giving policymakers an idea of the potential threats that may come by Russia towards the states of the Western Balkans after the suspension of pipeline geopolitics in the Balkan Peninsula.
Cyber security has grown to be a preeminent concern for the national security institutions of the US, EU, China, Russia and other develop nations. In addition the US Intelligence in last report of the 2016, has raise the concerns on security threats against the US and European allies by the Russian Intelligence and Cyber Institutions.
The cyber attack may come from Russia and China, which puts the national security at stake and would destroy the energy infrastructure of EU.
In military incursions that Russia is playing around the Europe and Middle East this type of threat should be taken seriously by opponents' of Russia and China.

Traditional warfare

Sun Tzu in sixth century BC referred to the fact that the best form of warfare is to take down enemy without fighting with him. Over time as warfare has evolved, the notion has gained impetus, especially with genesis of the cyberspace and cyber warfare. It was for the first time that Sun Tzu notion of "Seizing the enemy without fighting the most skillful", could be imaged has happening in its entreaty, using this potent weapon, which in contemporary world politics has no limits, no boundaries, and to a surprise, no visible restriction or legistlation.[3]

Cyber indicate the topic of cyber-security. It has become an area of great interest in 21 century.

How big is the threat to the United States and to the world community? Cyber security practitioners and experts have some idea, but there is a degree of hyperbole surrounding the issue and some heads in the sand as well. [1]

How cyber security issues fit into energy to puts some boundaries on the problems faced, but it is important to consider what is meant by "energy security."

Energy security for the US is the capacity for US consumers, individuals, organizations, corporations, or government agencies—to gain access to the energy supplies they need or want.[6]

Foreign embargos, midstream plant disasters, and military action are all potential threats to energy security for the US and other states of international system.

Energy production in the US is changing, however, and affecting how the US meets its energy needs.

Moreover the US needs energy resources from other countries. In history of international relations, states or government go to war for resources. Is

---

[3] *The Virtual Battlefield: Perspectives on Cyber Warfare*
Christian Czosseck, Kenneth Geers

[1] *https://bakerinstitute.org/media/files/Research/e00e5348/Pub-IT-HacksonGas-020514.pdf*

[6] *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*
Jason Andress, Steve Winterfeld

the age of resources and wars will occurs because of lack of natural resources.
The U.S. government has budgeted $14 billion for cyber security for fiscal year 2016, so clearly, this threat is being taken seriously at the highest levels of government.4

The Balkans: Energy and Cyber security

The conflicts over the break-up of the former Yugoslavia damaged much of the energy infrastructure and compounded the challenge of providing reliable energy supply in long terms for the states. The Western Balkans composed of Albania, Bosnia and Herzegovina, Croatia, Macedonia Montenegro, Serbia and Kosovo – is a complex region facing significant energy challenges. Electricity systems in many parts of the region remain fragile and in need of investment. [2]
The Western Balkans has the most unstable energy sector. Even though the governments claims that this issue is in good path to be resolved, the reports of unfair competition in domestic market suggest that in future country can face a crisis as result of growing competition on regional scale of gas pipelines and oil production of World Powers. The distribution of power is based in old system and is vulnerable to the future attacks.

---

[4] *http://www.cnbc.com/2015/09/25/biggest-cyberthreats-to-watch-out-for-in-2016.html?slide=2*
[5]*The Evolution of Modern Land Warfare: Theory and Practice*
By Christopher Bellamy

[2] *https://www.iea.org/publications/freepublications/publication/energy-in-the-western-balkans.html*

In the coming decade by 2030, the Western Powers should not underestimate Russian role in the Balkans even though the economy of Russia is in decline. As we mentioned in our previous analyses, Moscow has ability to attack all major ports and energy infrastructure of the States with excellent ties to the US. In the coming years the US should watch particularly this type of threats' in Europe. Russia beside the traditional warfare may use other options to keep Western Balkan States out of the EU and NATO sphere of interests. Modern nations no longer accept war as relatively aspect of international relations. This brings us to the paradox of warfare and global trends of cyber threats.[5]
The non-state actors also are part of the cyber attacks, which the current world affairs, gives a space for future adventure.

Key points: Cyber-warfare, Balkans, Enemies and Regional Powers

Recommendation:

1.Take in consideration cyber threats by enemies. Intentions should not leave undetected.

2.Westeren Balkans on regional scale may face an attack by other regional powers.

3.The states of Balkan Peninsula must work on upgrading the systems with new technology.

4.Enemy potentially has interest on striking the old information systems.

5.In cyber-warfare, in age of competition, all goods and state resources during the first phase of attack do not have chance of surviving. Only protected systems have a chance of live.

References:

Cyber Warfare: Techniques, Tactics and Tools for Security. Jason Andress & Steve Winterfeld.Syngrees, 2011.

https://bakerinstitute.org/media/files/Research/e00e5348/Pub-IT-HacksonGas-020514.pdf.Retreived on February 13, 2016.

The Evolution of Modern Land Warfare: Theory and Practice. Christopher Bellamy.Taylor&Francis, 1990.

The Virtual Battlefield: Perspectives on Cyber Warfare
Christian Czosseck & Kenneth Geers.IOS Press, 2009.

http://www.cnbc.com/2015/09/25/biggest-cyberthreats-to-watch-out-for-in-2016.html?slide=2.Retreived on February 13,2016.

https://www.iea.org/publications/freepublications/publication/energy-in-the-western-balkans.html.Retreived on February 13, 2016.