Cyber war and Terrorism in Kosovo

Assoc. Prof. Dr. Halim Bajraktari
Dean of the Faculty of Law, University "Ukshin Hoti" of Prizren

Agon Kokaj
University "Ukshin Hoti" of Prizren

Abstract

The war on terror has been an ongoing phenomenon for the past two decades. It has been a great challenge for the world to be able to neutralize our enemies in different aspects of our society. As we continue to move further into the 21st century we have started to encounter different new possibilities into working together for the best of our children. The problem is that the unknown enemy is no longer located in a certain state or region. We are continuously facing so called IT battle grounds or Digital Wars. The Cyber war has changed our lives completely. It has had a recent dramatic effect in the economies of several different countries. It has also changed the personal political background of certain significant individuals around the globe. The way we think and believe has taken a different turn in our society. It would be very logical to argue that if we are now able to trust the media or would it be worth choosing whom to trust. Cyber war has also had a strong impact in the Balkans. An unstable region where for the past few years has continued to have different cyber attacks amongst neighboring enemy countries.

Keywords: *Impact, Cyber attacks, Cyber War, IT-battle ground, enemy countries, Kosovo.*

Introduction

Cyber war is a very important ongoing phenomena in today's society. It has had a strong impact in the way certain decisions are made and it has changed the so called ideal believability in our present time. As we continue to move on into the so called developing world of IT and Hi-Tech, our societies are coming closer together. This has allowed different traditions and people with different backgrounds to reach out to one another whether it maybe from the eastern countries of Asia to the North Atlantic. This format of globalisation with the IT world has left us with many ongoing problems that may lead to a catastrophic domino effect that may be uncontrollable in the near future. The data we provide to the databases and the private information that we present to certain intuitions online may be at risk. It has occurred in our last two decades that data was corrupted stolen or misused for unlawful purposes.

Significant individuals have decided that they could start a new battleground online where they could use information and data regarding their own personal enemy and at some point they are able to publish it online. The major problem that we are facing here is that if that information, is personal or it could even contain images, video clips that could easily destroy one's image to the public eye. This could be related to a privately owned company or even an institution where people are employed. The problems we're facing are still not clear because it continues to get worse and

one could argue that the worst is yet to come. Cyber war is also associated with the destruction of data and information in information systems. It also includes the capability to use the web in order
to change or perhaps twist the information in order to gain public support. Cyber war is not costly in comparison to a real out scale war as it does not require the deployment of physical soldiers and weapons.

1.1 Problem Evaluation

The effect of cyber war has also had economic effect to certain institutions that where victims of cyber crime. The idea of cyberwar can be based on the ideology or purpose alongside the profitable objective. The graph in figure 1 illustrates this in detail. This analysis was carried out cyber research centre in the Netherlands

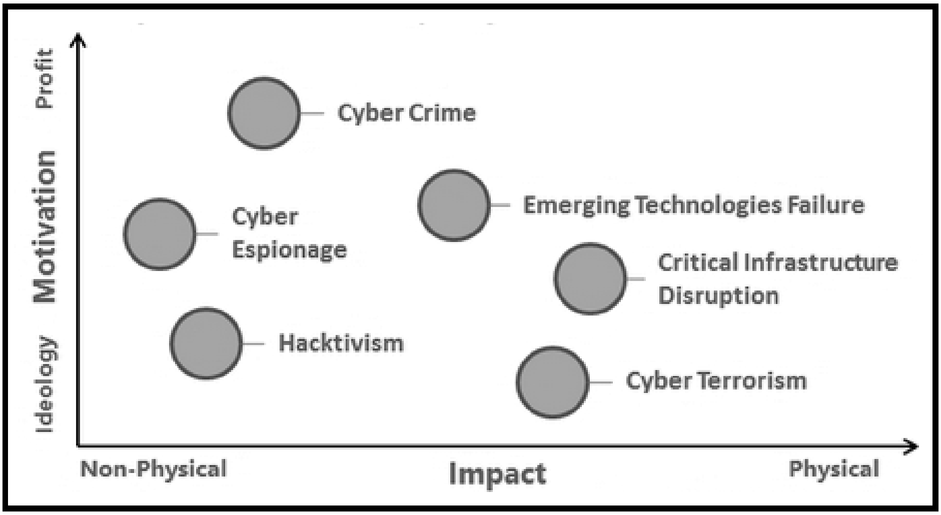

Fig. 1. Cyber Network Graph (Cyber Research Centre, 2019)

Figure 1. shows the significant relationship between motivation and impact. We can clearly agree that according to this graph cyber espionage is more profitable than critical infrasture disruption. Individual Experts are highly paid in order to perform the task required. The question that may arise is why critical disruption is more highly motivated and profitable than hacktivism. The logical understanding and explanation is that it could be in the interest of certain privately own institutions where they could try to send an unwanted program to its business competitor so that the firm itself would be able to catch with the competing online sales market whether it may be an online sales firm or a large scale production company that may be producing hardware electronics. Further analysis on the graphical representation on figure 1 is the break point of emerging technologies failure. It can be understood that it is the most crucial aspect out of all of them. Not only does it interconnect with the both the profitable objective but it also has a further future effect on the other sectors such as cyber terror and cyber espionage.

2. Future Analysis to Cyber War

In order to overcome our problem with cyber war it is crucial and essential that we analyse the certain institutions and times when they where effected and how. *Figure 2* shows the cyber attacks in 2018. This analysis was carried out by hackmagedon.

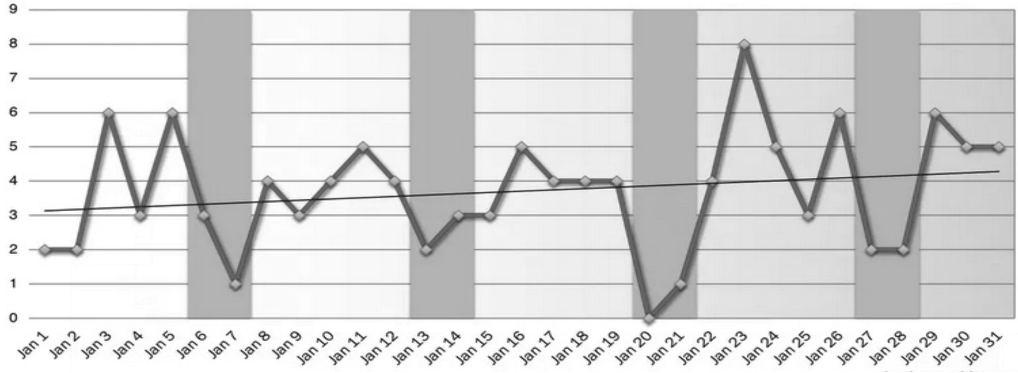

Fig. 2. Analysis of January

According to the graphical representation in figure 2 it is logical to say that attacks were mainly carried out in mid-end of January. We could argue here that there is also a psychological background that attacks are usually carried out after the winter vacation and the main explanation to this is to draw attention and warning as to how capable I am and this is carried out during the working time of the year when everyone is well aware and online of what is happening in the world. Further analysis was also carried out by the hackmagedon in order to dignify and point out what specific sectors have been mainly disrupted. Figure 3 shows the pie chart results for the motivational attacks in January 2018.

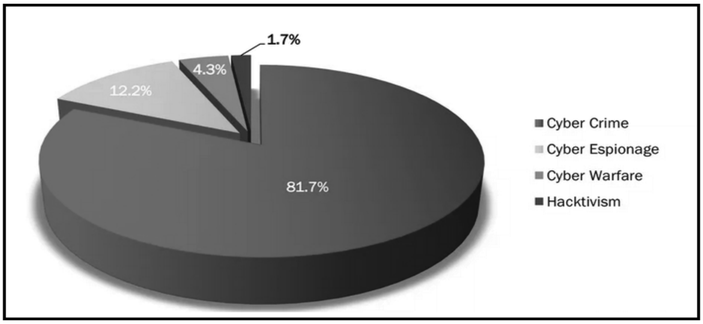

Fig.3. The Hackmagedon analysis*

In figure 3, we can clearly understand that cyber crime was the main attack of that month and the smallest number was in regular hacktivism. The Sector in cyber war was fairly small and this because in relation to cyber crime its significance is relatively less valuable as an overall outlook. Cyber espionage was also relatively high during the month of January and this is because during that time there were continuous ongoing attacks on different nations in the far east.

2.1 Future Analysis to Cyber War

Several Steps have been taken to try to overcome Cyber attacks or at least to minimize them as its consequences have had disastrous effect on its institutions. Figure 4 shows how a response to cyber security incident is carried out. Its stages are distinct and have been tested thoroughly before being implemented.

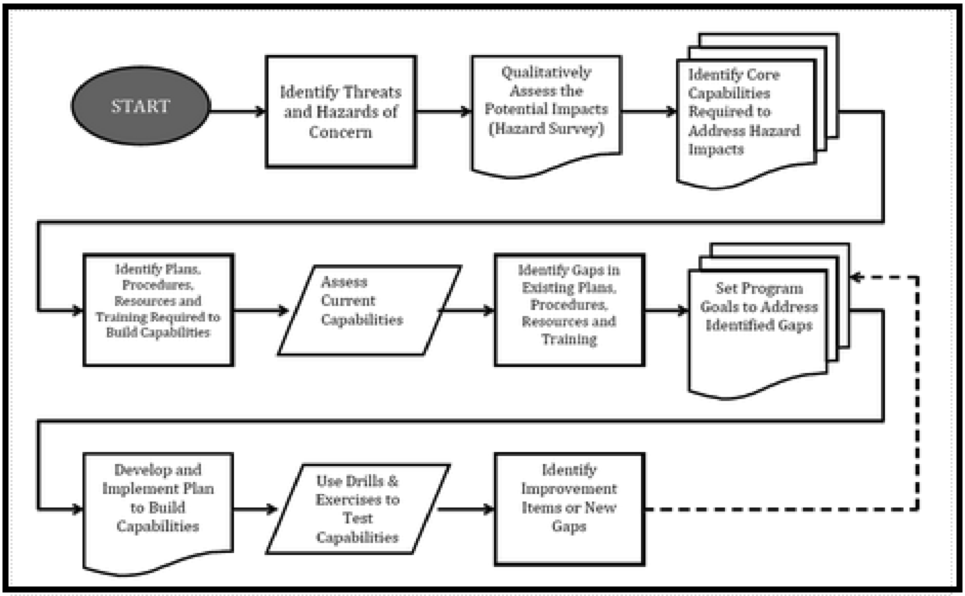
START
Identify Threats and Hazards of Concern
Qualitatively Assess the Potential Impacts (Hazard Survey)
Identify Core Capabilities Required to Address Hazard Impacts
Identify Plans, Procedures, Resources and Training Required to Build Capabilities
Assess Current Capabilities
Identify Gaps in Existing Plans, Procedures, Resources and Training
Set Program Goals to Address Identified Gaps
Develop and Implement Plan to Build Capabilities
Use Drills & Exercises to Test Capabilities
Identify Improvement Items or New Gaps

Fig. 4. Cyber Security Response Flow chart*

Tests have shown that this was very effective and it did help minimize the collateral damaged that might have been caused. We have also faced cyberwars between countries like Kosovo and Serbia where the outcome was a big deal. Certain unknown officials have used the net to spread propaganda, demonize certain political individuals. This ongoing political game has led to a very unwanted situations.

Conclusions

We have understood that as we develop new ideas and new capabilities in trying to overcome cyber crime and cyber war we are continuously being met with new problems. Globalization the new the changes in the economy and that political shift in balance in the superpowers is one whole interconnected concept. We do believe that more should be done in order to tackle organized cyber crime and new organizations should be set up to train and prepare our security institutions into overcoming our upcoming problems that may occur in the IT world.

References

https://www.crc-ics.net/research.html
https://www.hackmageddon.com/2018/02/22/january-2018-cyber-attacks-statistics/
http://www.efoza.com/post_response-flow-chart-procedures_625079/
https://www.talkingaboutterrorism.com/experts-talk/terrorism-as-a-threat-and-challenge-of-peace-and-security-in-21st-century-1