Inspiratron.org - Natural language processing, machine learning and cybersecurity

Case of the cyber war: Kosovo conflict

by Nikola Miloševi? - Tuesday, July 01, 2014

https://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/

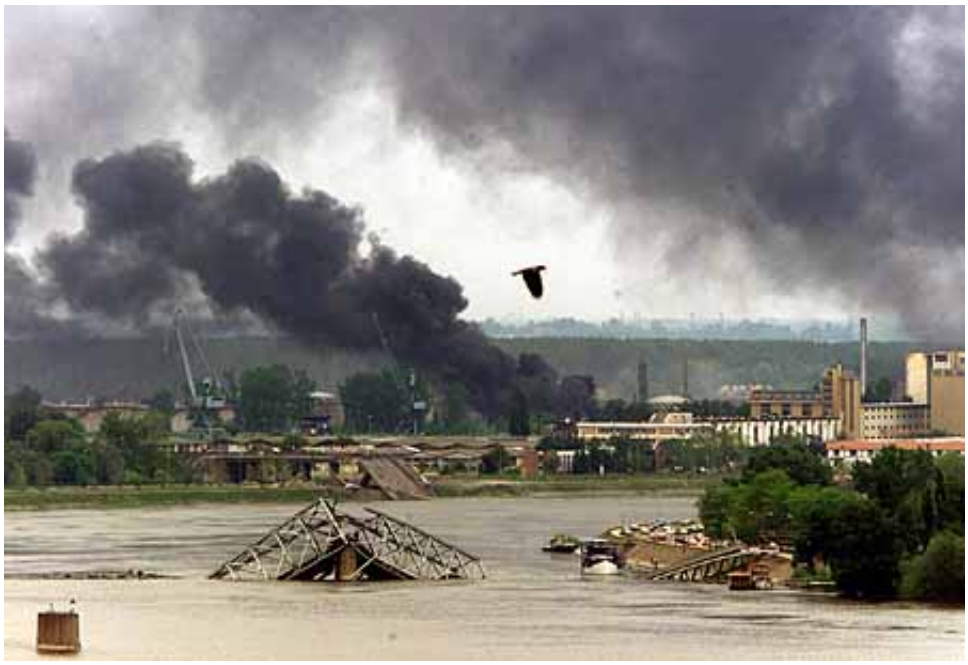
Introduction

Kosovo conflict was a conflict that started during the 1998 between FR Yugoslavia police and military forces and Albanian separatists in Kosovo. During the 1999. NATO launched air strike campaign against FR Yugoslavia. The air strikes lasted for 78 days, after which FR Yugoslavia agreed to withdraw forces out of Kosovo. This was the first war with quite extensive activity in cyber space or the internet. Many attacks happened during these 78 days. However, even thou the military conflict ended after the Kumanovo peace treaty, the conflict remained in diplomatic space and in cyber space. Since NATO proclaimed to be neutral (which it sometimes is, but sometimes is not), NATO facilities stopped to be targets, but we can say that conflict still rages between Serbian and Albanian hackers trying to disrupt internet websites and infrastructure of other side.

Since I have not seen anyone describing whole conflict I would try to do that in the following post. I would also try to be as objective as possible. However, some events I might miss, so I would welcome comments to fulfil the story. First I will describe political and military context of the war. If you are uninterested you may skip that part. Than I will talk about conflict in cyber space between Yugoslavian hackers and NATO. I will also describe some life-hacks Yugoslav army did to mislead NATO planes and bombs. Than I will talk about conflict that followed up between Serbian and Albanian hackers disrupting and defacing websites of the other's side governmental institutions and public figures.

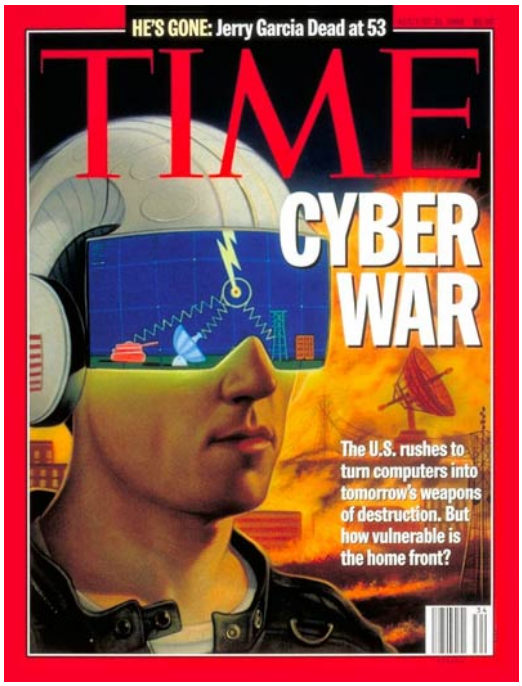
Context

Tensions on Kosovo started in 1980s. Started with discrimination of both ethnic groups where they were minority. In 1989. president of Serbia, Slobodan Milosevic, vastly reduced the autonomy of Kosovo. In response, Albanians in Kosovo organized referendum in 1991 and proclaimed independence. Independence was recognized only by Albania. However, Albanians started to ignore state and federal structures and started to create parallel institutions. In the mid 1990s, UCK was created, an Albanian militant force. There were no major conflicts until 1998. UCK by that time was building up, mainly trough organizing underground network in the western Europe. This network was using drug and human trafficking to fund UCK with equipment and weapons. In 1998. major attack on Yugoslav police and army started. As no state would stand still having a terrorist attacks on their police and soldiers, FR Yugoslavia fought back and as it was heavily equipped army and police of a country, they sometimes used their force too much. Because some of attacks had some consequences in civilians, international society started to get involved. At some point there should be peace negotiations in Rambouillet. It turned out to be NATO ultimatum on Yugoslavia requesting free movement of NATO troops over whole territory of Yugoslavia, which Yugoslavia refused. NATO used Yugoslav refusal as a justification for starting air strikes campaign called Operation Allied Force. Also it would be quite important to note that in was about month before NATO 50 years anniversary and that eastern block was gone and NATO was at that point redefining its point and mission. I could guess that redefinition was to play world's policeman. Also the attacks were launched without consent of UN Security council and this was the first international intervention done without consent of UN Security council in history. The power of NATO and FR Yugoslavia is quite incomparable. However, it is clear that NATO underestimated Yugoslav army and Yugoslav army did not suffer heavy loses during the war, but in 78 days NATO managed to exhaust countries economy and infrastructure, which consequences can be felt even today. According to the first NATO officials statements, they planned that the war will end in couple of days or maybe in one week. It ended after 78 days, which is quite a lot more than a week. But I would not talk anymore about military side of the conflict, but I will keep focus on war in cyber space, because this is also one of the reason why this conflict is interesting. This is the first war that took place also in the cyber space.



Phase I: Cyber war between FR Yugoslavia and NATO

After the NATO air campaign started, many people in Serbia felt duty to help defending country or somehow to disrupt or stop NATO operations. Among those people were also people involved in computing. Since the best they were able to do was trying to hack attacker's websites, they started organizing themselves into small groups that would attack NATO websites, servers or any infrastructure of NATO or countries that were part of NATO and are exposed on the internet. One famous group performing attacks during the bombing was group that called itself Black hand. These guys took their name by organization that existed in the Serbia at the beginning of 20th century. The group was formed among the Serbian officers who plotted a coup at the turn of the century and they also had a huge role in uniting southern Slavs in firstly Kingdom of Serbs, Croats and Slovenians, later renamed to Kingdom of Yugoslavia. However, modern Black Hand from 1999. was a hacker group that was quite successful in their attacks. Firstly they started with kosovo Albanian websites that spread propaganda. So they took down and defaced websites like kosova.com and Swiss based Albanian news portals zik.com [ref]. Zik was a news-portal of voice of Kosovo. Hosting company put down website after the attack and unregistered domain, because attacker who said he was from Poland threaten the company that he will delete all the content from the hard drives of the hosting company. Also website of UCK got defaced by Black Hand. They were claiming that each NATO tomahawk missile will destroy at least one server. By the beginning of the NATO aggression over Yugoslavia, Yugoslav hackers were aided with Russian hackers who performed attacks on US military websites and internet infrastructure. After NATO bombed China embassy in Belgrade, claiming it was a mistake, China hackers joined combined forces of Yugoslav and Russians hackers. Here the things became serious. NATO server was shot down because of denial of service attacks over it. US Navy website was hacked by the Russians. NATO mail servers were nonfunctional because they were daily they were receiving more than 20 000 emails with malware in attachment. It was reported that more than 25 different kind of malware were sent in these emails. After a denial-of-service attack based on "ping" saturations launched from Serbia brought down the NATO server, NATO personnel took evasive action. A ping attack is a malicious saturation of a server with messages that overwhelm the server's capacity to respond. To counter it, the NATO network crew swapped out a Sun SPARC 20 for the more powerful UltraSPARC for faster processing of the Serbian pings. And NATO switched from a 256K bit/sec access line to the European equivalent of a T-1 to keep the pings from eating up bandwidth [ref]. After these attacks. Group called itself Hong Kong Danger Duo completely deleted www.whitehouse.gov leaving the message *„Protest USA's Nazi action! Protest NATO's brutal action!*". Similar messages were seen in 100s more websites in US and other NATO countries. Some servers tried to defend themselves by blocking all the traffic from .cn and .yu domains. At one point US and NATO threatened that they will switch off .yu domain from the international network. However, that did not happened during the war. NATO also launched some quite minor attack trying to hack and steal money from foreign bank accounts of Yugoslav political leaders. Also several individuals, for example from Netherlands hacked and defaced some Yugoslav websites. However, these attacks were far less severe than ones did by the other side. US security people seemed to be caught unprepared for all these, since also they had ongoing conflict with their domestic crackers.UK claimed that they have lost some data from several quite sensitive databases. US claimed no damage was made, however, US is quite famous for claiming that they had no losses even when they have.



During the conflict FBI started operation that had a cause to hunt down US based hackers. These people saw it as call to war. Websites of FBI and US senate were inaccessible for more than a week. Hackers completely deleted content from the website of US senate. FBI claimed that the attacks on their servers were unsuccessful, however, they had to turn it off - for some reason. They also explained that sensitive information are not stored on website.

After these 78 intense days conflict ended. With it cyber war ended as well. Although, no army was officially involved in cyber attacks, it cannot be said that it was not real cyber war.

Phase Ia: Life-hacking during the war

There are two life-hacks I would like to mention that used during the war in Yugoslav army. During the conflict NATO used rackets that were tracking down radar signals and destroying radars. However, Yugoslav army realized that they can use radar for some amount of time (20 seconds) and if they turn it off after these amount of time, it would go undetected. Also, they realized that rocket navigation radar is emitting similar microwave frequency as home microwave. So they turned radar on, when NATO plain released rocket, they would switch off the radar and turn on microwave on some distant place. Rocket would get confused and start changing target for microwave. If the one turn off microwave, before rocket finishes its turn, rocket will hit some field, without causing any damage. These were quite advance rockets and quite expensive ones. So it was quite huge waste of money and resources if the rocket did not found target.

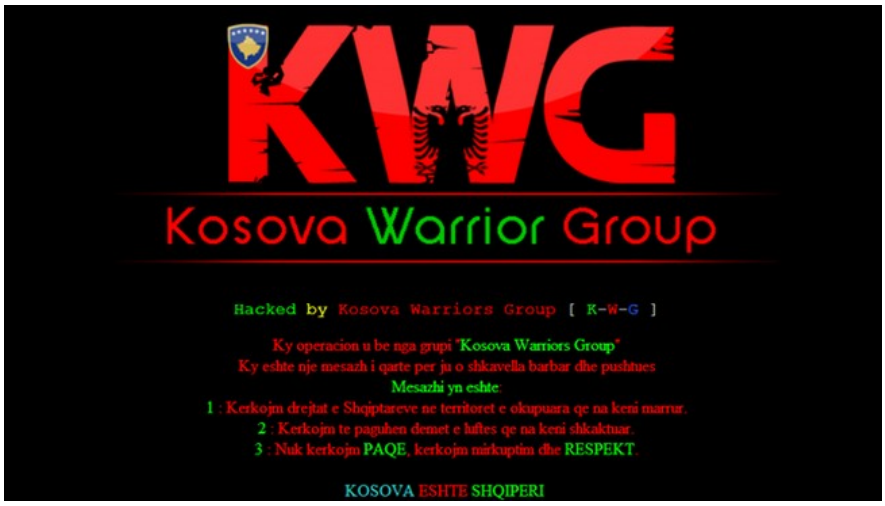
The second hack was made by Yugoslav officer Zoltan Dani, who modified radar system so that it would emit slightly changed frequencies. These frequencies were able to detect F-117 stealth plane, who was never damaged before. By doing this, his unit managed to shot down one F117 plane and damage one or two other.

End of the conflict with NATO

The ceasefire was signed on June 9th 1999. in Kumanovo in Macedonia. This ceasefire and following UN resolution ended conflict between NATO and FR Yugoslavia. NATO archived most of the goals in physical war, since it was stronger. However, in cyber space and on internet NATO was not good. US military leaders and NATO leaders said that they did not wanted to start any attacks on internet, because of undefined international regulations and similar excuses. However, it is more likely that NATO at that time was not prepared for the attacks in this domain, which led after number of incidents on the internet to the bigger funding of NSA and GCHQ teams trying to make cyber weapons. And they are doing now quite well with malwares like Stuxnet and Flame. In 2009. US formed US Cyber command whose mission is to coordinate US army in cyber space. Especially from 2009-2010. military security agencies of some countries are doing quite great work on preparing for another war in cyber domain. Conflict ended in military space, however, conflict between Serbia and Kosovo remained in diplomatic and cyber space. That is what I wanted to write about next. I'll try to make this one quite short.

Phase II: Cyber war between Serbian and Albanian hackers

After the war finished, Albanians in Kosovo thought it is over and that they will be able to make soon their independent country and maybe to annex Kosovo to Albania. In 2008. Kosovo again proclaimed independence and this time some (not so small) number of countries recognized it. Howeve, this number is still less than half of the world, and many international institution accept new members by consensus. So Kosovo, because of Serbia, and because of UN resolution 1244 which states that Kosovo is integral part of Serbia (FR Yugoslavia) under international protectorate, could not become real country and enter any international institution.



This could be quite frustrating, so Kosovo hackers launched number of attacks on Serbian websites. Number of Serbian government websites were defaces since 2008., including website of president of Serbia, several ministries. However, Serbian hackers replied with defacement of Kosovo government website defaced. Again number of ministries and public agencies websites were defaced.

This remained quite persistent conflict, with attacks from one side every couple of months and replies from the other side couple of days later. Most visible attacks are deface attacks, however, there are also DoS attacks and DDoS attacks going on.