Leo Zhang

6/11/2022

IDC 6601

Assignment I

Daniel Muller’s discussion

Abstract

The recent Russia-Ukraine war has paved the way for many cyber-attacks in the Russian webspace. It’s hard to imagine that a country that was well known for its massive cyber superiority now houses a free-for-all cyberspace filled with many users vulnerable to attacks. In this paper, I will discuss some behavioral imperatives that may lead to this issue.

Discussion

From some of the twitter post snippets shown on the website [1], many individual hackers are dissatisfied with the Russian government and its president Putin. Some are part of the Anonymous hacktivist movement and they are stealing private data in order to punish the government for their war crimes. In the beginning of the war, DdoSecrets published 200 gigs of emails from the Belarus weapons manufacturer Tetraedr. One important message was published with the dataset announcement “#OpCyberBullyPutin”. The group of hacktivists are definitely not on Russia’s side and they are very committed in attacking Russia and trumping them in this cyber-warfare. The hackers’ interests are to blackmail the Russian government and to threaten them if they don’t do what the hackers say. It’s clear that the hackers want to gain power thru this.

It is a dangerous territory to blend military and civilians for the very reason that Muller stated, militaries are subjected to specific rules and civilians would likely be treated more like outlaws and are doing so at their own risk and subjected to any laws they are breaking in their own country and the country they are attacking. One of the responses to Daniel Muller’s discussion stated if the civilian wants to help those who are in trouble, they should do so in a way that is not hurting other civilians. This is very true but unfortunately in this digital age, it is very difficult to stop every civilian from hacking into a state war. It is certainly unfortunate that the citizens of Russia have fallen victim to these growing cyber attacks since the war started. I think Russia has fewer dependencies since many of them cut off ties with Russia since the war started and they support Ukraine. I'm sure some of those dependencies include companies who offer great cyber security protection. And with them not on Russia's side anymore, Russia is more on its own now. As for the rhetorical question at the end of Muller’s post, I think the saying goes "all is fair in love and war", so in the most desperate times we as human beings will take desperate measures to protect ourselves and achieve our goals.

As mentioned in Muller’s discussion, several Russian TV channels, and social media accounts such as those on Twitter have been hacked. Many have been claimed to be done by a group called Anonymous. The group is certainly treading on some gray areas of politics even they mentioned “We are involved in the biggest Anonymous op ever seen. That being said, we are worried that some governments will indeed see us as a threat and create some scenarios to make us look bad (false flag). We only want peace, not war. [2]” It is important to note that what they do may potentially expose the privacy of innocent Russian civilians as well. Putin knows about these issues and signed a new law that puts those who distribute fake news about the Russian Army up to 15 years in prison [2], which makes the Anonymous have to always be on their feet when doing their hacking job.

The Anonymous hacktivist collective has been bombarding Russia with cyber-attacks since declaring "cyber war" on President Vladimir Putin in retaliation for the invasion of Ukraine [3]. According to this article [3], these hackers want to expose to the world what is happening in Ukraine during the war. What is shown in the video depicted bombs exploding and soldiers talking about the horrors of the conflict. The hackers were trying to convey that innocent Ukrainians were being massacred and said that they will keep attacking until the Kremlin in Russia stops the war. Just as mentioned in this article [3], the attacks instigated by Anonymous hackers have caused disruption and embarrassment, but cyber-experts have become increasingly concerned by the explosion of hacktivism for reasons such as having a hacker accidentally knock out a hospital’s computer network or interrupt communication links. This brings back to Muller’s discussion towards the end when he asked that question of the boundaries between civilians crossing into military affairs. It is imperative that the benefits and drawbacks be analyzed when civilians hack the military, for example, and cause accidental damage on other civilian property such as hospitals, which could potentially affect the patients at victimized hospitals and their lives in the worst case.

This article [3] also provides an example of what I mentioned in my response to Muller’s question about civilian hackers. A hacker named Roman, who is coordinating his IT resistance for Ukraine, states that what he is doing is illegal and wrong until there is a threat to you or your relative [3]. The fact of the matter is that whether it is truly right or wrong for civilians to interfere with military business, when it comes to times of war, people will take any measures they can to ensure victory and survival. In our digital age almost everyone owns a phone and/or computer, and once information is leaked, it is pretty impossible to delete it completely from the cyberspace.

RuTube, which is Russia’s equivalent of YouTube, was also hacked and so Russian citizens are able to see the anti-war messages displayed. As the truth unfolds throughout the Russian citizens, some decide to take digital action to protest the war, even within their own country [4]. As the war entered the third month (May 2022), Russia is struggling under an unprecedented hacking wave that entwines government activity, political voluntarism, and criminal action [4]. Digital assailants have plundered the country’s personal financial data, defaced websites and handed decades of government emails to anti-secrecy activists abroad. One recent survey showed more passwords and other sensitive data from Russia were dumped onto the open Web in March than information from any other country [5]. Ever since the Ukraine war has started, hacking Russia has been made a free-for-all, and the sense that Russia is off-limits is somewhat expired, and hacktivism is one of the most accessible forms of striking at an unjust regime or its supporting infrastructure, as mentioned by Emma Best, co-founder of Distributed Denial of Secrets [5].

Groups like Network Battalion 65 have even gone so far as to threaten and ask for ransomware payments from Russia. Many other groups have the objective of stealing state-secrets, government software (in the form of source codes), private documents and such [5]. These actions certainly can make it easier for these civilian hackers to be treated as military soldiers rather than civilians because of how involved they are at stealing government data.

Conclusion

It certainly is astonishing to see the tables turn as a once superior country in the cyberspace world falls victim in a free-for-all zone to being attacked and exposed by not only outsiders, but also insiders as well. It really goes to show how united people can be across the globe with the power of technology. It is clear that the gap between civilian and military matters have shrunk as a result of this kind of cyber-warfare.

[1] https://theintercept.com/2022/04/22/russia-hackers-leaked-data-ukraine-war/

[2] https://www.rferl.org/a/russian-tv-hacked-ukraine-anonymous/31740663.html

[3] https://www.bbc.com/news/technology-60784526

[4] https://www.washingtonpost.com/world/2022/05/09/russia-tv-hack-victory-day-ukraine-war/

[5] https://www.washingtonpost.com/technology/2022/05/01/russia-cyber-attacks-hacking/