CHRONICLE PUBLISHERS

Chronicle Journal of Engineering Science

Research

Cyber Hybrid Warfare: Asymmetric threat

Christos Beretas*[1]

[1]PhD Candidate (full scholarship) in Cyber Security at Innovative Knowledge Institute, Paris, France.

*Corresponding author : Christos Beretas. PhD Candidate (full scholarship) in Cyber Security at Innovative Knowledge Institute, Paris, France. (+30) 693-890-9477 | e-mail: cberetas@ikinstitute.org

Received: 17th April 2020
Accepted: 2nd May 2020
Published: 11th May 2020
Copyright: © 2020 Christos Beretas

ABSTRACT

Cyber hybrid warfare has been known since antiquity, it is not a new terminology nor a new practice. It can have an effect even more than a regular conventional war. The implementation of the cyber hybrid war aims to misinform, guide and manipulate citizens, disorganize the target state, create panic, overthrow governments, manipulate sensitive situations, intimidate groups, individuals and even shortened groups of the population, and finally to form an opinion according to the enemy's beliefs. Creating online events designed to stimulate citizens to align with the strategy of governments or the strategy of the enemy government is a form of cyber hybrid warfare. The cyber hybrid warfare falls under the category of asymmetric threats as it is not possible to determine how, and the duration of the cyber invasion. The success or not of a cyber hybrid war depends on the organization, the electronic equipment, and the groups of actions they decide according to the means at their disposal to create the necessary digital entities. Finally, the cyber hybrid warfare is often used to show online military equipment aimed at downplaying its moral opponent.

Key words: hybrid war; cyber war; online threat; cyber warfare; warfare

INTRODUCTION

The cyber hybrid warfare also includes DeepFake, a practice mentioned in Christos Beretas previous research. The cyber hybrid war aims to disrupt and hurt the adversarial state in an organized and targeted manner, mainly regarding the organizational structure of the target state and its functioning. Digital media are used to intimidate citizens, target specific groups of people, disseminate false news between political and military leadership in order to spread hatred and resentment on both sides, to divide the people, and finally the fall of the government, followed by the anger and indignation of the people. The cyber hybrid warfare is not only and exclusively applied during a period of natural war, it is a kind of war that can be waged for years and of course in times of peace. It is difficult for citizens in a cyber hybrid war to understand the truth and lies. A well-organized cyber hybrid war is difficult for people to recognize as the facts presented are so convincing that it is impossible to recognize them as false. The ways to avoid and protect against such a war are numerous and require knowledge, experience, alertness, high morale, courage and professionalism to deal with such a cyber threat from its birth. Sovereign states around the world are using the cyber hybrid warfare to blackmail, trap, mislead, both foreign governments and citizens, achieving remote results without the use of physical violence and natural disasters. The cyber hybrid war has come to stay, and it is an emerging form of war - the pressure of the strong against the weak or better of the organized states against the disorganized. As mentioned above, a great DeepFake video is capable of stirring up enormous panic and hatred in a society. It is an asymmetric threat that is increasing day by day.

Characteristics

The cyber hybrid war is an asymmetric threat that is defined when an entity uses electronic means to disturb the peace or spread panic in the target state and launch hostilities or uproot social groups residing in it. A fake video, for example, that will be sent to targeted social groups is capable of sparking riots in the crowd with demonstrations and violence. By reading this one can easily understand the reader that the cyber hybrid war is the result of an entity preceding its onset. This entity is the digital asymmetric threat which if not handled properly then evolves into a cyber hybrid war. The cyber hybrid war is not tantamount to an isolated practice, that is, it is not a common attack on the adversarial state; rather, it consists of organized methods that are often impossible to identify, such an attack may include social media, online press, videos and hostilities from different events, etc. The difference between a cyber hybrid war and conventional warfare is that except there are no killings and conflicts, there is a constant low-level influx of information affecting the target state. That is, it does not follow the logic that an event has occurred, a number of people have risen and then the digital invasion process has ended, on the contrary, the digital presence is continuous and stable at the same level as possible.

Advanced stages of a cyber hybrid war include practices such as misinformation aimed at the financial loss of the target state, intra-country turmoil from pro-country groups that launched the cyber hybrid war to compel its citizens to withdraw. for the purpose of financial loss or even the overthrow of the government. In a cyber hybrid war, the invaders' practical ways of attacking are not one-sided but two-sided, which means that in one field they can decrease and increase in another, for example a false bent can be seen in social media news and on the contrary the volume of fake videos is growing too. A cyber hybrid war is often won when combine electronic and physical attacks in the target state, which means that in the target state it requires the penetration of disturbing elements in order to revolt and destroy the target state's infrastructure and economy. This includes increasing crime, which will then be used in the media and social media by the adversary state as a means of corrupting the target country with the ultimate aim of reducing its reputation, spreading fear to other countries. aimed at restricting travelers, other countries' security reviews, further financial burden, withering and global isolation.

The success or not of a cyber hybrid war in addition to the proper organization, hardware, and staff, requires and sufficient funding for the whole venture, funding is a key success factor, with insufficient funding the result will be the opposite, as it will unprofessionalism has emerged, and it is easy for social groups to understand that this is fake news, which is equivalent to project failure and redesign. Funding can come exclusively from the state that organizes the cyber hybrid threat, it can come from friendly countries in it, as well as from organizations that are scattered around the world, usually when a cyber hybrid war is funded by organizations around the world, the communication takes place through social media or smart phone applications that offer anonymous messaging services. At this point it should be noted that there is no formal single practice or specificity in the form of steps that need to be taken to be considered a threat as a cyber hybrid threat, so there is no legal framework defining the steps that characterize that this is a threat to the target state to take legal actions, the legal framework is incomplete and that is something that countries that are waging such wars are very aware of and they are washed.

As technology evolves, asymmetric threats increase as states with sufficient funding and equipment are able to wage such wars on a large scale, which is why the cyber hybrid wars will intensify. That is why governments and security agencies around the world are trying to organize and shield themselves against the cyber hybrid war, now knowing that its impact is greater than even conventional warfare. Preparing, organizing, and preventing such attacks are the basic prerequisites for dealing with the threat. This entails writing and implementing a cyber security policy that outlines the conditions, steps to be taken, education, definitions, and how to handle such incidents. The security policy should be updated annually and adapted to the needs and the level of risk that exists per period. It must adequately specify how government agencies must act in a period of digital asymmetric threat. Allied countries need to formulate a common cyber policy so that dealing with a digital asymmetric threat is unified. It is of no use to allies and friendly countries not to implement a common strategy against digital asymmetric threats. Friendly organized countries can easily trap the enemy and destroy the plans.

Conclusion

The cyber hybrid war is made up of several entities that, depending on the smooth functioning of all entities, are judged to be successful or unsuccessful. It is an asymmetric threat, no one can know the length or the size of the area it will take place. It is a kind of war that with the development of technology will see significant development. An important factor in success is financial support and therefore the amount of money each state is willing to spend to design and implement a credit cyber hybrid war. A well-organized and implementable cyber hybrid warfare can cause severe damage to a conventional one. It is not necessary for a cyber hybrid war to be designed exclusively by wealthy and developed countries, such a war can be created by any state that has the knowledge, money, and organization to mount an asymmetric threat. In the cyber hybrid war, the chances of convicting states for war crimes are minimized, as in the cyber hybrid war there is no clear legal framework defining the methods of intruders. Identifying a digital threat is difficult due to the complexity of its actions; identifying and neutralizing a cyber hybrid threat requires knowledge

and experience of such threats. Some countries in the world have developed methods and teams to detect and manage such threats, but the measures they take to protect them are found to be incomplete and not fully effective and the reason is the rapid development of technology that new methods and techniques are constantly being discovered. Finally, as has been said above, the best defense is the organization of friendly states to provide a single aid and formulate a unified security policy that will lead to massive isolation of cyber hybrid threats. Unified repression by friendly countries against such attacks is the best organized defense against hybrid threats.

References

1. Christos Beretas, DeepFake - Another One Cyber Threat. 2020.

2. Andreas Krieg, Jean-Marc Rickli, Surrogate Warfare: The Transformation of War in the Twenty-First Century. 2019.

3. Andrew Fevery, Hybrid Warfare. 2018.