Cyberattacks, Russia, and the changing face of war in the 21st century

March 9 2022, by Erica K. Brockmeier

Credit: Pixabay/CC0 Public Domain

Amidst the severe destruction, staggering humanitarian crisis, and worldwide economic impacts that Russia's invasion of Ukraine has elicited in less than two weeks, officials around the globe have also raised concerns about the potential for cyberattacks. Examples of Russia's previous actions in this realm have included attacks against the websites of Estonian organizations in 2007 and the hacking of Ukraine's power grid in 2015.

To learn more about how cyberattacks have shaped modern warfare and how countries are adapting their strategies, Penn Today spoke with Heli Tiirmaa-Klaar, a Perry World House visiting fellow and director of the Digital Society Institute at the European School of Management and Technology. During the past 15 years, Tiirmaa-Klaar has led efforts to coordinate, prepare, and implement cybersecurity strategies across the European Union and also helped prepare the NATO Cyber Defense Policy.

How did you get involved in the field of cybersecurity?

In 2007, Estonia received a large-scale coordinated cyberattack. After that attack, the Estonian Ministry of Defense was in charge of putting together the national cyber strategy to make sure that our critical assets would be protected in the future.

I was previously working as a defense policy planner, and I ended up leading the process of putting together the first Estonian national cyber strategy after the 2007 attack. Ever since then, I have been working on cybersecurity issues.

Generally speaking, what does cyber warfare and cybersecurity look like?

So far, we have not seen cyber means causing destruction during wars. What we have seen during conflicts is cyberattacks used to disrupt communications and disrupt the functioning of information systems. Fighting parties often use this method to disrupt their adversary's strategic communication and disrupt information systems or messaging to their own people.

In terms of cybersecurity, what countries usually do is prevent attacks from happening in the first place by implementing best practices and following prevention steps. This includes updating security requirements and making sure they have a layered cyber defense system.

One common misconception about cyberattacks during politically motivated campaigns or conflicts is that they have their own logic and happen outside the broader strategic context. Instead, they are actually used by warring parties to either aid or facilitate other goals, be they political or on the battlefield. Overall, cyberattacks happen because there is a point of using these attacks in the broader, systematic approach of the battlefield, and, if countries have a political motivation to attack another country, a cyberattack might certainly be a part of it.

Are there other types of cyberattacks beyond those targeting digital infrastructure, communications, or other national assets?

Most Westerners understand cyberattacks as a technology-based attack method that disables some IT system. But for the Russians, it is mostly information warfare. For Russia, the most important part of cyber or information warfare would be to spread disinformation that serves their interests in the conflict.

Currently, we see how the Russians use disinformation to make sure that their own population does not get truth from the outside about what happens in Ukraine. They also have used tactics of spreading disinformation in the battlefield so that soldiers don't lose morale.

It's also possible to use disinformation against the Ukrainian population, but the Ukrainians are very resilient to disinformation. They have their own excellent information campaign as a counter campaign, and they strike back with professional information campaigns and tools.

Information warfare also happened during the Russian invasion of Georgia in 2008. A major disinformation campaign spread about how Georgian troops were starting hostilities, and cyberattacks were used during the first days of conflict to disable the Georgian government's ability to put up a message with their version of events. During the current Ukraine invasion, there were attempted defacements and other cyberattacks against the Ukrainian ministries a few days before the war began, but they were mitigated quite professionally.

There haven't been many cyberattacks in Ukraine during this current invasion. Why do you think this might be the case?

I think the Ukrainians were prepared this time because they experienced and learned from some serious cyberattacks during the 2014 Russian invasion. And, while we have seen this information war happening in the background, most of the experts are surprised that they do not see major cyber elements happening.

My argument for this is that if the Russians can actually destroy electrical power plants or other infrastructure, why would they need to do a cyberattack? Countries tend to use cyberattacks if they need to do some disruption below the threshold of armed conflict, in this kind of gray zone between peace and war. But now, the conflict is full on, so they don't need to conceal it.

What has been the role so far of cyberattacks during this war?

Every time we have a war, we learn something. In this current war, we are seeing how the less conventional methods of cyberattacks have been used and how large of a part the information operation has been. While there have been some real cyber disablements happening, such as against satellite communications, it's another question as to how successful they were.

Given the impacts of information warfare, how are countries protecting themselves from these types of cyberattacks?

Western nations don't want to embark on the line of controlling content, and this is why I think Western countries have had difficult adaptation barriers around how to take care of these information operation aspects.

But, if we want to prepare ourselves, we have to because this is part of the Russian strategy since the very beginning. For the Russians, it's all part of a continuum of the tools that they can use: disinformation on one end, nuclear weapons on the other.

Provided by University of Pennsylvania

Citation: Cyberattacks, Russia, and the changing face of war in the 21st century (2022, March 9) retrieved 23 April 2024 from https://techxplore.com/news/2022-03-cyberattacks-russia-war-21st-century.html