Opinion: What war in Ukraine means for cyber security in Europe

March 7 2022, by Greta Nasi

Credit: Pixabay/CC0 Public Domain

As bombs and missiles tragically rain on Ukrainian cities, so do another kind of armament: cyber weapons. This new generation of weaponry replaces explosives with destructive software (malware) and missile launchers with network vulnerabilities. Cyber weapons break into

adversary country's essential networks, establish remote control, and wreak havoc by erasing computers, leaking data and causing other dangerous disruptions to essential services and critical infrastructures.

But cyber weapons are different to traditional "kinetic" weapons in a key way: they are often less targetable. In other words, when a country releases a cyber weapon on another, it may hit other targets than its makers intend. As the malware moves inside a target's network, it can inadvertently spill into others. Researchers call this a "spillover' effect.

As Russia wages its war against Ukraine with cyber weapons, the risk of spillover to European countries and firms all over the world continues to increase. Microsoft has detected many Ukrainian computers affected by "wiper" malware that erases their contents in a difficult-to-recover way. In recent days, Microsoft also detected a new malware (named "FoxBlade") focused on stealing health, insurance, and transportation data from Ukrainian essential services. Ongoing technical analysis will determine how likely these malwares are to spillover from outside Ukraine. But given past examples of malware spillover from Ukraine to other countries, governments around the world are issuing warnings about possible spillover risk. There are also emerging suspiciously timed disruptions to European systems, that may turn out to be spillover. Isolating ourselves from kinetic warfare no longer means we are safe from the effects of the war itself.

What 'security' must mean for this moment in history

How should Europe prepare and respond to collateral damage of cyber war? Beyond technological defense and interventions, we must more broadly define our concept of "security" and our approaches to achieving it.

Traditionally, the concept of security developed along with the notions

of threat and force, primarily in the military. The related object and the existential threats have been related to physical domains, until the end of the last century.

In February 1998, while the US was preparing the bombing attack on Iraq, someone breached into military computer networks. It turned out it was not a state, but some teenagers out of California. This event, known as Solar Sunrise, shed light on the cyber domain. It raised the policy debate about the assets, vulnerabilities, and capabilities governments have to govern to protect their objects and their stakeholders in the cyberspace.

Drafting a national cybersecurity strategy requires:

- Defining the principles, priorities, and assets to govern (ranging from economic to social pillars)
- Understanding the technical security issues in terms of objects to govern (confidentiality, availability, and integrity of data) and how the attackers may compromise a computer system (by manipulating the threads of control, namely the instructions on what to run next on a computer);
- Identifying and developing capabilities to defend against specific threats to the state's principles and priorities;
- Deploying those capabilities as a projection of broader state power.

A national cybersecurity strategy requires an approach that cuts across agencies and sectors, defines goals, and plans actions designed to improve the security and resilience of national infrastructures and services.

Cybersecurity as a public good

Security in cyberspace must go from being a technical concern to a broader public good, developed by many societal actors. IT experts, lawmakers, regulators, social scientists, civil society groups and institutions need to cooperate. Governments must no longer be solely responsible for maintaining security and stability within their borders; other actors must become deeply involved.

Ukrainians and their allies have already begun to demonstrate this broader approach with:

Ongoing, deep information sharing between private companies and relevant governments about cyber weapons in use

Use of varied and changing information channels (not just official websites) to demonstrate the Ukrainian government's persistence and stability, despite attacks on their infrastructure
Twitter-based public diplomacy to bring a private organization's alternative infrastructure to Ukraine
Collaboration between civil and military groups to form cyber defense brigades and volunteer forces

Amid the ongoing catastrophe of war in Ukraine, European countries can and should prepare themselves for the cyber spillover by building a broader coalition of different stakeholders. The next cyber war will not just be a technology problem; it will be everyone's problem.

Provided by Bocconi University

https://techxplore.com/news/2022-03-opinion-war-ukraine-cyber-europe.html