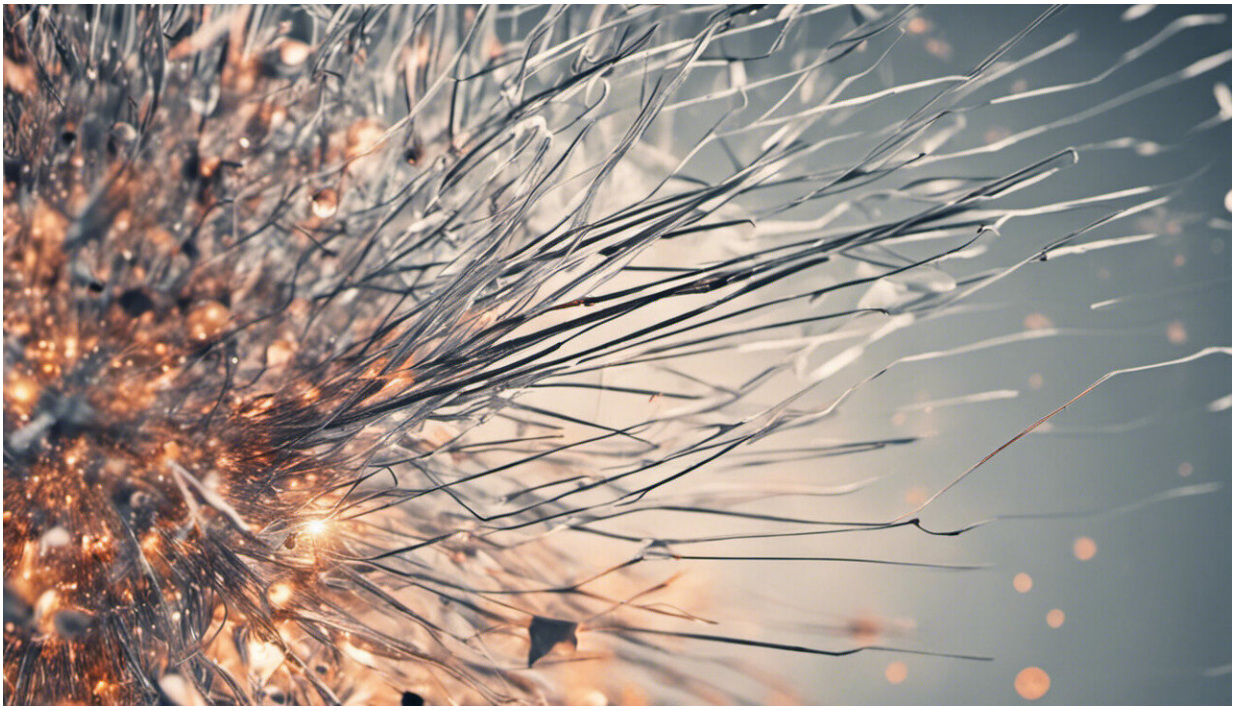
Why cyberattacks don't work as weapons

January 18 2018, by Dr. Myriam Dunn Cavelty



Credit: AI-generated image (disclaimer)

Digitalisation will fundamentally alter many aspects of our lives – in many cases for the better. However, our increasing dependence on computers and networks for data exchange and storage is creating new vulnerabilities for both individuals and society. The key word here is: cybersecurity. This encompasses more than just technical solutions: it involves not only security in cyberspace, but also security that is influenced by cyberspace.

Cyberattacks in political conflicts

It is only very recently that those of us conducting political science research have been in the position to systematically examine cyberattacks as a phenomenon of political violence – simply because the number of cases is increasing. We see that cyber operations are a "normal" side effect of political conflicts of all kinds. Both state and non-state actors use cyber activities to intervene in conflicts in various ways.

Testing the technical and political effects of cyber operations in various contexts is attractive to both state and non-state actors, as the costs are relatively low and mostly indirect. The targets have exploitable technical vulnerabilities and insufficient security measures, while victims often find it difficult to assign a clear attribution (specifying the perpetrator) and thus punish the attacker. This is why we are seeing more, and particularly more spectacular, cyberattacks. However, these attacks are often restrained: as rational actors, states are not interested in uncontrollable escalation.

Are cyberattacks a justification for war?

At the same time, efforts to develop rules of behaviour have intensified in order to reduce the remaining danger of escalation. An international consensus has developed that only cyberattacks that cause a high level of destruction equivalent to a kinetic military attack should be viewed as a reason for war. We can also see that the US seeks to regulate the cyber activities of states such as Russia (electoral manipulation) and China (industrial espionage) using the classic instruments of international politics, such as diplomatic negotiations, bilateral agreements and sanctions.

The most important point, however, is the awareness that cyberattacks

only have a limited use as instruments of destruction – as weapons. Only a short while ago, strategic "cyberwar" was considered as the central threat; a virtual attack out of nowhere (e.g. against a power supply) that would bring a state to its knees.

The reality looks a little different: the difficulties of achieving controllable effects and causing actual violence by means of cyberattacks mean that cyber methods are above all suited to protest actions of various kinds. They aim to cause confusion and influence a population's opinions. They are also well-suited for espionage, for (with a bit more effort) local sabotage and – much less frequently – as preparatory or disruptive measures in the course of "traditional" military operations.

What does this mean for the digital future?

Fears of a digital meltdown are unfounded. However, a wide range of actors are already using digital networks to achieve strategic goals against the will of other actors. This means that digitalised areas must guard against deliberate interference – because the more connected things become, the more potential targets there are.

In the future, an even better understanding of the motivations of political actors will be necessary. We must analyse how and on what basis they make their decisions and what role digitalisation plays. In this way, we can utilise technical solutions to influence political incentives through international standards, so that confidence in the technical opportunities of the future will be possible despite the strategic exploitation of cyberspace.

Provided by ETH Zurich