Assessing what state institutions can do to combat cyberattacks

June 15 2018, by Dr. Myriam Dunn Cavelty

During the Cold War, the focus was on classical military threats and their defence of national territory. Credit: Keystone/Steffen Schmidt

When a cyberattack has been orchestrated by a state actor, people may be tempted to call it "war". After all, it's an attack waged on national infrastructures by a foreign power. But the term "cyber war" has been used so often for dramatic effect that I don't just want to warn against hype. It's also time to dampen expectations regarding the scope of governmental intervention.

Defined during the Cold War as protection against classical military threats and the defence of national territory, the term "security" is now widely understood to include non-military dimensions. Switzerland's 2016 Security Policy Report, for instance, lists not only armed attacks but also terrorism, crime, manipulation of information space, supply disruptions and disasters and emergencies as threats. This has led to security policy instruments being adapted for the prevention, defence and management of these threats. And although the military is still important here, it is no longer the only instrument.

A matter for the military?

If cyberattacks really were a form of "war", then it would be primarily up to the military to deal with this danger. But the assumption reflects neither the true nature of the threat, nor the legal and operational capacity of the military as a security policy instrument to counter it.

The vast majority of cyberattacks are criminal in nature, and target private networks and company assets. State bodies have no access to these networks. The few attacks on government or government-related networks in recent years – for example, the RUAG incident in 2016 in Switzerland – were espionage. They leave us with an unpleasant feeling and concern national security, but foreign intelligence activities are commonplace. We're therefore far from being at war. And although we know that both state and non-state actors are increasingly using cyber media to achieve strategic goals, all these incidents have so far fallen considerably – and no doubt consciously – short of warfare.

If not the military, then which government institution should be responsible for cyber security policy? It's a question that many countries are currently debating – including Switzerland. Because politically motivated incidents are on the rise, cyber security has been recognised as a national security concern at least since 2010 and has been integrated

into the larger security political framework. That the problem is too great to be addressed with only technical and operational measures has been acknowledged too. As a result, there's now a trend towards centralisation: previously disparate cyber-security competencies are grouped together and politically strengthened under (civilian) leadership by assigning them to specifically responsible units, sometimes located at the highest governmental level.

As with other present-day dangers, the role that the state wants to (and can) play in this area is remarkably small. All known cyber security policies rely mainly on businesses and citizens taking personal responsibility: it's a question of self-defence. This means that the state should intervene only when public interests are at stake or, in Switzerland specifically , when it's acting in accordance with the principle of subsidiarity. The armed forces are primarily responsible for protecting their own systems. To this end, the development of offensive and defensive operational capabilities is being driven forward within the existing legal framework.

And that's a good thing.

Cyber security is a security policy issue – but everyone has to pull together in a national effort. Security can only be strengthened if businesses, universities and various authorities work together and if we collaborate constructively with other countries. Discursive militarisation – rooted in constructions of the national enemy and assumptions about our nation state and its resources – merely creates unrest and arouses false expectations.

Provided by ETH Zurich

Citation: Assessing what state institutions can do to combat cyberattacks (2018, June 15)