Why Cyber Does Not Make Military Sense

Van Hoeserlande Patrick

Information technology is part of our daily lives. Apart from some isolated communities, every household has some machine with a chip in it, and this evolution will continue. The Millenniums, however you define them, do not know a world without it. Working in an office means without a doubt spending some time on a computer. No writer should waste words on the obvious statement that cyber connects or will connect everything.

Less obvious is our role as military in this virtual world. There is lots of talk about the need to get rid of the limitation to Cyber Defence and to engage in a more offensive role. We should even consider cyber as a new domain next to space, air, land and sea. There are good arguments supporting this approach, as there are equally convincing ones against it. I think that the discussion on the cyber domain is useless, because others decided that already for us. However you approach the military side of cyber, it is there and we need to consider it seriously.

As a domain, cyber will for sure compete for resources. Being militarily prepared for battle in the cyber domain will not come cheap. If you think that cyber soldiers are highly intelligent hackers with some fancy DIY equipment, think again. This is like thinking that a land army is nothing more than a bunch of ill-trained, but highly motived, terrorists with an AK-47. Nope. A cyber army will require investments in training and material equal to those for air and space. But, that is not the main reason why cyber does not make sense.

Bunkers were magnificent defence measures against the lethality of arms like rifles and guns. If you want to protect people, you just encapsulate them in reinforced concrete and add a strict access control to it. Nobody gets in without you scrutinizing them. Great!

That is our model for Cyber Defence: you protect your network against intruders and with a firewall you control the in- and outward flow of data. Like in the old days of competition between the offense and the defence, you have to update your defences with the latest building material because the weapons are getting better. Anyhow, with the right – any idea where that threshold is? – amount of investments, you feel safe, protected.

But the comparison with a bunker is wrong. You're not safe at all. A bunker is worthless if you may not shoot at an approaching enemy, if your guard may not use force to prevent unauthorised entry. Outside a bunker, you have to patrol to see movements and to get timely warning of a pending attack. You cannot sit and wait until you're surprised by an attack.

But it does not stop there. Your cyber bunker is built with components and software potentially developed by your enemy. There may be malware imbedded in some components that can be activated by a simple command. You may think you control the gate, but the other side has the key to a backdoor, maybe even more than one back door. How safe do you feel in the kind of defensive work where the enemy can walk in whenever they wish, without you knowing it?

Of course you can cut all connections to the outer world, but what use will your network have then? A command and control system is worthless if it cannot order combat elements into action. And even in complete isolation there is no guarantee that an infected component part of the whole system will not disrupt the function of your network.

So a purely defensive posture is just a nice façade and gives you a false feeling of safety, but it will not stop a cunning enemy. If you think this is an argument pro cyber offensive, than you're mistaken. Why is shooting back not the solution for a failing defence?

A cyber warrior, i.e. a cyber terrorist or any group with an offensive strategy, picks the moment and the target of the attack. In this discussion I consider hackers a nuisance as they do not have the intention to do physical damage, they can disrupt or manipulate data, but their intention is not to kill people. Killing people with cyberattacks?

As the effects of cyberattacks are not limited to the network, so our reactions must not be either. The consequences of a cyberattack can leave the cyber domain and enter others. What would be the effect of taking over the cooling system of a nuclear plant? What could happen if the pumps and valves of pipelines were out of control? How about a ship entering a port at full speed? Some changes in the Air Traffic Control information maybe? Our cyber enemies can pick their targets, study defences and attack when ready. Just like a 'conventional' terrorist can select a target, recon it and hit it when ready.

But we do not have this advantage. We do not know who our enemies are. We certainly do not know where to hit them, and the luxury of deciding on the attack moment is not ours either. So we have to train and plan on some, possibly high tech, unknown other. We can try to penetrate some systems, but never 'theirs'. Cyber warriors can study targets and even build a similar system to test some approaches. They can even try to penetrate the live target and prepare for attacks. Plant cyber mines. We cannot. We are not allowed to infiltrate a network as part of prudent planning.

And remember we're working from a bunker made of components built by the other side. Our cyber weapons may be infected and telling more about us to them then we know. Soldiers do not go to war with weapons controlled by the ones they attack. Why do we accept this in cyber warfare?

And we have not considered questions in the legal or moral field when taking the initiative in the cyber domain. Or what about collateral damage? How about attacking civil nerve centres? How well could we live with a virus aimed at blocking the locks of a harbour that accidently sabotages the plant control software of the petrochemical industry? We have not mastered the art of cyber warfare enough to talk about surgical 'bombing' operations.

If we cannot defend ourselves and we're not able to take the offensive - unless your nation has the money and a clearly defined enemy - are we at the mercy of whoever wants to attack us?

The answer is 'no'. But, we cannot respond to the threat as military alone. We can stop air, land, naval and even space forces alone, but we cannot do this in cyber. In this aspect it is much like biochemical warfare. That is another reason why it should be labelled a domain. We have to join forces and go for a comprehensive approach.

It may be too early to list all measures to take in order to get a real defence against cyber warfare. But we should start thinking about constructing our proper building blocks for our 'bunker'. We should render the hidden keys useless by installing our own back doors. Our bunker may be less cosy and more expensive, but at least we can concentrate on real access control at the front door without unlocked back doors. We could start producing the digital bow and arrow, simple weapons not controlled by the other side. Planning for joined answers to cyberattacks (i.e. resilience) may be another thing to consider.

Of course, this approach needs further thinking or may even force some to attack us before we're successful in negating all possibilities. But without profound reflection, cyber warfare does not make sense.