Can your armor withstand a cyberattack?

The birth of the Swedish Cyber Armor for embedded vehicle cyber defense

Historically there has been a constant race where thicker armor is followed by heavier guns. Today there is a parallel war ongoing in the cyber arena where more advanced cyberattacks are followed by more effective cybersecurity solutions. But is it really a parallel war? What if the armor is penetrated by a cyberattack? Could a cyberattack make a vehicle come to a halt?

There are a few examples where a cyberattack had an impact in a military ground operation.

During the Ukraine conflict conventional military operations were combined with cyber operations including infected android applications used by Ukraine forces for artillery targeting computations and disturbance of GPS positioning.

There are also examples where cyber-attacks have been met by kinetic counter attacks such as the 5th of May 2019 when Israel conducted an airstrike against a building from which Hamas orchestrated cyber-attacks.

When it comes to stopping armored vehicles there are also examples, but first, what would be required from such a cyberattack?

Penetrating the armor

The cyberattack would have to penetrate the vehicles armor. As in any attack the attacker would be looking for the weakest spot and vulnerabilities that can be exploited. I the case of a cyberattack, a weak spot which can transfer data to the internal systems of the vehicle.

Todays modern vehicles are often wirelessly connected, and data can be transmitted and received via antennas. This data is likely encrypted and maybe not be the firsthand choice of an attacker. A weaker spot can be physical data connections used for maintenance and software updates where a service engineer connects a laptop. If that laptop has been infected with a virus it can spread to the vehicle upon connection.

There could also be built in backdoors and vulnerabilities already from the factory. Not all sub suppliers delivering components to the vehicle manufacturer may have the same level of security in their production. This is referred to as Supply chain attacks and could be a real threat in this context as the attacker is likely to have an incentive, large resources and long-term planning.

Aiming for maximum effect

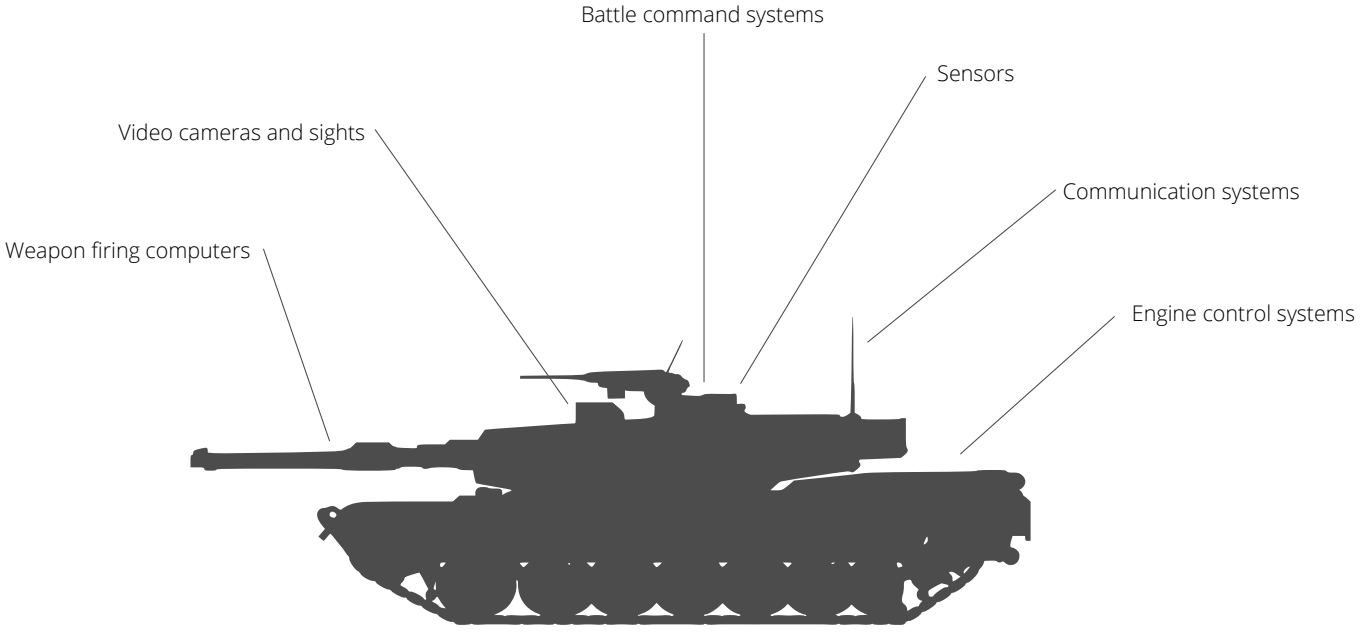
For the cyberattack to reach its target and get the desired impact such as making a vehicle come to a halt or heavily reducing its capabilities it is likely to be in the form of Weaponized malware.

One of the most well-known examples of weaponized malwares is Stuxnet which was used to sabotage Iranian nuclear centrifuges. Another example is BlackEnergy which is a Malware targeting powerplants. It caused a power outage in the Ivano-Frankivsk region of Ukraine in December 2015.

A Weaponized Malware can be a precision weapon which spreads from one system to another and detects when it has reached its target by checking usernames, domain names, IP-addresses and more. It covers it's tracks by deleting itself on the systems it passes on its way to the target. It can also "fly under the radar" of signature-based antivirus systems by being polymorphic i.e. dynamically changing itself to avoid detection.

The more digital and connected vehicles get, the more vulnerable to cyberattacks they become.

Vulnerable systems in a vehicle could be:



There are examples of vulnerabilities. 2018 Pentagon reported that they found several vulnerabilities in weapon systems in general;

> *"Vulnerabilities found within the systems included being able to turn a weapon on or off, affect missile targeting, adjust oxygen levels or manipulate what controllers see on their computer screens."*

More specifically for armored vehicles, 2018 the US Director, Operational Test and Evaluation reported vulnerabilities in the Stryker 30 mm Infantry Carrier Vehicle – Dragoon (ICV-D).

> *"Adversaries demonstrated the ability to degrade select capabilities of the ICV-D when operating in a contested cyber environment."*
>
> (Director of Operational Test and Evaluation 2019).

Finally, this is an example where main battle tanks were stopped by a cyberattack combined with electronic warfare.

> *"In a recent simulated exercise at the Army National Training Center at Fort Irwin, Calif., enemy tanks were stopped by cyber-attacks and electronic warfare. Army trainers successfully used cyber weapons and electronic warfare (EW) technology to thwart a simulated tank assault at a training exercise conducted at the Army National Training Center at Fort Irwin, Calif."*

Coordination of combined weapons

Coordination in time between ground operations and cyber-attack would be a challenge in the case of weaponized malware. For example, making a vehicle come to a halt at the time of a conventional attack. The malware would likely have to be spread months before an attack. Other effects may require less coordination such as making the vehicle consume more fuel than usual or make its weapon systems less accurate.

It's likely that this type of coordination will become better in the future. It could be compared with the coordination between ground and air operations which took many years before it became optimal.

Every vehicle needs embedded cyber defense

The defense industry is constantly working on improving the protection against cyber-attacks. To reduce the risk of being hit by a cyber-attack and reduce the effects if it still happens these are actions that should be considered:

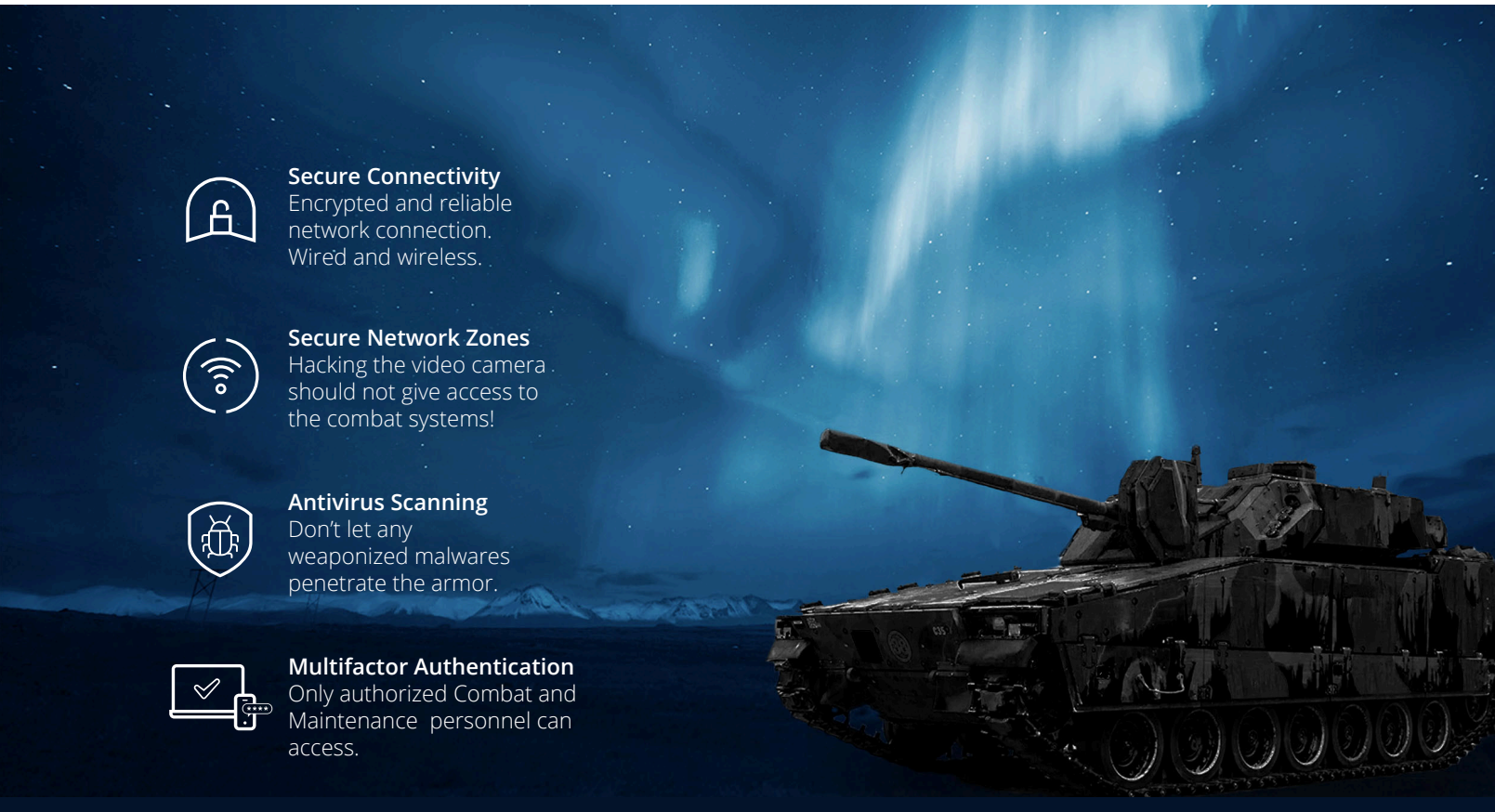
- Design and develop new vehicles with cybersecurity in mind from the beginning i.e. Security By Design. Use:
  - Protect and limit external access using built in firewalls only allowing certain protocols, systems or users to connect to the vehicle.
  - Segment internal networks to prevent malwares from spreading between internal systems.
  - Perform malware scanning of systems, laptops, USB memories.
  - Require authentication of crew and maintenance staff.
- Educate manufacturing staff and military units in cybersecurity to reduce risk.
- Make careful selections and validation of sub-suppliers to avoid supply chain attacks.

Swedish Cyber Armor that you can trust

Clavister is proud to be a trusted defense industry supplier of cyber security solutions. There are tough requirements for embedding cyber security solutions in vehicles, especially military vehicles. Rugged military grade hardware may be required. The software needs to be extremely reliable and fast while being as lean as possible in terms of hardware resource usage.

Clavister fulfill these requirements and can run on a range of different hardware including both Intel and ARM architectures as well as virtual environment. The software is also Common Criteria EAL 4+ certified.

Being a fully Swedish and European company Clavister stand out as the independent alternative. Clavisters Security By Sweden is unique.



SECURITY BY SWEDEN

clavister®
CONNECT . PROTECT

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 • **Web:** www.clavister.com