CYBER ARMOUR

AI-based cyber security for military platforms

Defend the Defenders

clavister
CONNECT. PROTECT

Authors
Neena Sharma, Senior Product Marketing Manager, Clavister
Stefan Brodin, Head of Cyber Armour Solution, Clavister

A New Era in European Cyber Security

There is a war in Europe and Russia has threatened to take retaliatory measures on nations who support Ukraine, especially NATO's existing members and countries aiming to join the alliance such as Sweden and Finland. Europe is entering a new era and priorities have shifted from economic growth to defending our democratic values, freedom, and way of life. This war will have a long-term impact on Europe and its allied forces, not only in this year or next, but for years to come. There has been an unprecedented increase[1] in defence budgets across Europe, which has seen the global military spendings surpass $2trillion per year for the very first time. Russia has been hit hard with severe economic sanctions and there has been a huge global increase in energy and food prices.

What does it all mean for global peace? How will Russia retaliate? What would defer a potential conflict between Western Europe and Russia? Will it elevate the cyber risks in the region? These are some of the vital questions that every European nation need to consider. We haven't seen the kind of cyber-Armageddon in Ukraine that we were expecting to see from Russia's side but then Russia is already causing enough physical damage to destroy the country. But what about nations that don't share borders with Russia? A cyber warfare isn't confined with any geographical borders and could be the likely weapon of choice against highly digital weapon systems of NATO and allies. Risk of an escalation in hostile cyber exchanges between Russia and NATO states remains high. Cyber espionage activities have always been very difficult to attribute to specific countries or threat actors but in the recent years, especially now with the ongoing war, we have started to see more direct attributions of cyber-attacks and threats to Russia[2], which also means that in the long run we might see these threat actors retaliating more aggressively and openly.

> " Cyberattacks have become a theater for great-power conflict in which governments and militaries fight in the hybrid 'gray zone,' where the boundaries between peace and war are blurred " [3]
>
> \- Dmitri Alperovitch,
> cyber expert and Chairman of Silverado Policy Accelerator think tank

NATO Requires a New Cyber Defence Policy

Europe is entering a new era and digital Europe needs to strengthen its cyber security locks and build up its wall of digital defense, military platforms included. NATO is set to release strategic documents that will guide the next decade of its military planning. We can expect cyber security and cyber defence to be an integral part of it[4].

Military platforms, weapon systems and armoured vehicles are increasingly digital and software-dependent. Today, complex technology stacks and computer networks drive major weapon systems. There is also more interconnectivity between information technology (IT) and previously isolated operational technology (OT) than ever before, which powers the most critical and sensitive functions of major defence systems and weaponry including fighter aircrafts, combat vehicles, sea vessels and artillery.

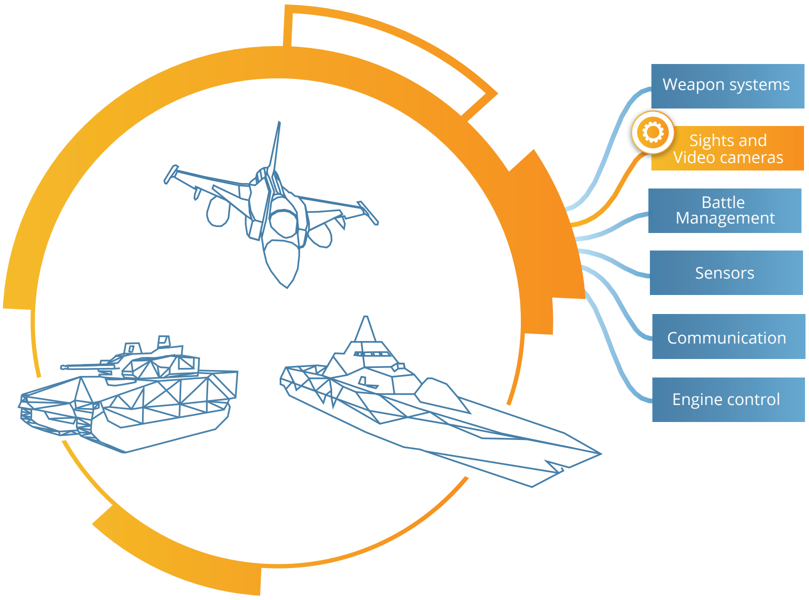
While IT security has improved tremendously, OT cyber security is still at nascent stage and therefore cyber security solutions capable of defending the entire system have not kept pace. A few reports have highlighted the vulnerabilities in military platforms and urgency of focusing on cyber security aspects .

What's needed is the 'cyber hardening' of networks, sensors, and systems against cyberattacks. This includes real-time operational systems such as military tanks, aircrafts, unmanned aerial vehicles (UAVs), and ships, which all must undergo cyber hardening to enhance mission resiliency against system manipulation, hijacking, or destruction. Different defence forces are at different maturity levels in terms of executing cyber hardening programmes but changing geo-political climate in Europe warrants all member states to understand its importance and need.

> " There is a technical aspect to hardening defenses and building redundancy in data and services, but the core of resilience lies in leadership that does not ignore the problem "
>
> \- Merle Maigre, member of International Advisory Board of NATO CCDCOE

Consider the example of an armoured vehicle and look at the vulnerable interfaces and attack vectors where the enemy could penetrate the armour and cause damage:

- The air interface, through wireless communication over digital radio or satellite.
- Physical connection, through a cable when a platform is connected for communication or maintenance.
- Supply chain attacks, when the enemy infiltrate a sub supplier and introduce malicious code in a component which ends up in a platform when delivered from the factory.



Invest in bespoke, fit-for-purpose cyber security solutions to build resilience

Cyber security solutions required for military platforms are definitely very different from the off-the-shelf commoditised products. 'One size fits all' won't work here. Defense domain expertise, including how different platforms and weaponry systems work, a deep understanding of cyber vulnerabilities, and knowledge of interfaces between IT and OT systems are all vital to build bespoke, fit-for purpose cyber security solutions that can then enhance the cyber security of an entire system.

Military platforms and weapons take years to build and need to be protected for the whole of their lifespan, lasting 10-20 years in most case. In the cyber security space, enemy can upgrade their (cyber) weapons every day and we need our solutions to be longer lasting and relevant. Artificial Intelligence (AI) provides us the answer here, and it needs to be an integral part of a solution. We need purpose-built algorithms specifically developed to identify new threats and new types of attacks to be able to future-proof cyber security for tomorrow. Implementing this level of advanced AI requires deep domain expertise and cyber security skills; and can take years to perfect.

Don't wait for lengthy upgrade plans

Cyber security needs to be embedded as an integral part of the development of new military systems or platforms, but there is also a great need to retrofit cyber security solutions to existing infrastructure. This can be done as part of upgrades and modernisation programs as the hardware can be tailored and optimised for each military platform. Developing new, cyber-secure military platforms such as ships and armoured vehicles takes time.

> **Fleets of existing platforms are to a large extent vulnerable today. Urgent action is required!**

Almost every existing military platform has internal components connected in networks using IP or CAN bus protocol communication, whether they be cameras, sights, weapon systems, battle management systems, navigation, or propulsion. Their cyber protection can be improved today, without waiting for large mid-life upgrades. For example, existing ethernet switches can be replaced by intelligent cyber security gateways, tailored to the same form factor and connectors for cost-efficient replacement while keeping the existing cabling.

Cyber security and cyber hardening initiatives require close coordination across national governments and the private sector, and NATO and the European Union must therefore continue to work very closely on this vital issue. Regional militaries should include cyber security as part of their immediate procurement activities and work with OEMs and defence contractors like BAE Systems.

The most important armed race of our times is the digital one and the side that controls the data will control the battlefield. It doesn't matter how thick the armour is or how big the guns are, if the enemy can hack into a military platform's software, it could shut it down. Invest in effect cyber solutions to protect your assets, data, platform, and personnel.

Defend the defenders!

About Clavister

Clavister is a Swedish cyber security company and we have developed Cyber Armour, an AI-based cyber security solution for military platforms. Cyber Armour is an advanced and flexible military grade Security Gateway with individual AI engine that integrated directly into existing platforms or vehicles and significantly increases protection against cyber-attacks. Cyber Armour collects data and provides complete visibility to commanders to continuously monitor mechanical and cyber health of the system and take preventative action when something wrong happens. We are using innovative AI algorithms specifically developed for this purpose. It is also one of the world's most efficient when it comes to hardware resource needs.

> **Clavister Cyber Armour protects NATO military platforms across Europe, such as BAE Systems CV90 Infantry Fighting Vehicle.**

Contact us today for more details.

[1] World Military Expenditure Passes $2trillion first time

[2] Russia Was Behind Cyberattack in Run-Up to Ukraine War, Five Eyes and US Governments Confirm

[3] How Russia Has Turned Ukraine Into a Cyber Battlefield

[4] NATO's Role in Global Cyber Security

clavister
CONNECT. PROTECT

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