NATO: Could cyber attack be the best form of defence?

Tom Ball

5 days ago



NATO is in the process of hammering out clear guidelines on the use of cyber attacks for engaging the enemy, while considering the possibility of taking a more robust approach.

The old adage of 'attack is the best form of defence' might be getting dusted off during the NATO discussions on cyber attacks, with ideas of a more offensive set of tactics being floated. A decision is set to be made by 2019.

Britain, the United States, Germany and Spain are among the nations involved in deciding how cyber weapons should be utilised, all of whom have taken a defensive approach while nations such as North Korea play a much more aggressive role.



As reported by Reuters, U.S. Navy Commander Michael Widmann at the NATO Cooperative Cyber Defence Centre of Excellence, said: "There's a change in the (NATO) mindset to accept that computers, just like aircraft and ships, have an offensive capability."

While it may seem like an obvious approach to do more than just repel incoming nation-state cyber attacks, there are a plethora of factors that must be considered.

Bill Evans, Senior Director at One Identity: "Recently, it was announced that NATO is considering a more muscular response to state-sponsored computer hackers that could involve using cyber attacks to bring down enemy networks. Moreover, in 2014, NATO declared cyber as a domain of warfare putting it on equal footing with land, air and sea. However, NATO has not yet defined the details behind cyberwarfare."

The principal of cyber warfare may not yet register with some, but cyber attacks have the potential to completely shut down elements of critical infrastructure, and in turn neutralising the threat of the enemy there, and also potentially impacting innocents as collateral damage.

"On the one hand, it's likely high time that NATO begin considering how cyber can be weaponized and integrated into both defensive, which is already occurring, and offensive battle plans. To be sure, NATO adversaries are already doing this. However, there are risks. Unlike "smart bombs" that can pinpoint the damage to an air strip or enemy fortress, cyber attacks are far less specific. Consider an attack at an enemy's power station. Surely this will cut off power to the enemy's ground forces, but it might also pull the power from a local hospital or senior citizen's facility – certainly not the moral high ground that NATO prefers," Evans said.