How much of the British Army's next war will be digital?

Poppy Brown
The University of St Andrews

UK experiencing four 'nationally significant' cyber attacks every week -NCSC

Due to technological advancements, the army no longer faces threats just on the battlefield. There's constant cyber battles being fought that as civilians we would never see; it creates a grey space. The question is when does the cyber war become an actual war between two countries?

Literature Review

Cyberwarfare is a broad term, encompassing many ways adversaries can attack on the digital battlefield. This poster focus on: Deepfakes, Infrastructure, GPS, Communication systems, and Data Sovereignty. It is thought that the cyber space is the only domain contested by adversaries everyday; that there is a growing grey space as to when cyber war develops into war between two countries. However, it is hard to say what an actual cyber war will look like in the future, as technology is always developing. Therefore my findings are all theoretical and based off our current technologies.

Methods

I have used a lot of secondary data: news articles from a range of sources, some academic articles, as well as governmental documents about cyberwarfare.
I also gathered quantitative data from a survey I sent out to some civilians, to gain their opinions on cyber warfare

Deepfakes

Deepfakes can be used to spread disinformation which is dangerous in conflicts since it leads to fake news. For example, in the Russo-Ukraine war a cyber attack on Ukraine 24 which compromised its website to display a deepfake video of Zelensky issuing a surrender to the country's troops.

GPS

GPS allows for the closing of the kill chain using BAE systems technology as it can guide weapons to the pre-determined location of the target. If the precise timing signals from the GPS's multiple satellites are disrupted then this could cause supply chain issues as bank payments and power grids etc rely on them.
GPS jamming can also have a negative impact on the military since it makes it harder to guide drones, missiles, or surveillance tools

Infrastructure

Digitisation has connected systems that were once isolated, meaning that they can now be attacked in 2 ways. AI is making it easier to find and exploit weaknesses in legacy tech, via reverse engineering. CCTV and traffic cameras can also now be hacked by foreign actors, for example Israel was able to create a surveillance network, establishing Iran's leader's daily routine in preparation for the strike that killed him.

Communication Systems

Cellular networks are also under threat which means if mobile phone towers were disabled emergency dispatch communications could be blocked. For example, the US Secret Service disrupted a network of telecommunications devices that could have shut down cellular systems - this was >300 SIM servers and 100,000 SIM cards capable of shutting down the cellular network in NYC. This is relevant to the military, since it could block the UK's emergency messages in times of conflict.

Data Sovereignty

If the UK relies on cloud providers and network infrastructure under foreign jurisdictions, and a geopolitical crisis or trade dispute occurs then data and network operations could be compromised. For example, American companies have to allow American authorities access to data under applicable law and Palantir, a US based company, has a contract with the MOD and the NHS.

80% of those surveyed think there needs to be stricter definitions for the grey space

65% believe the army is not adequately prepared for cyber warfare

100% believe the rise in technology will change how the next major war will be fought by the British Army

How the Army is reacting

The army now has cyber exercises to test how we would react to big cyber attacks as they have now realised the importance of cyberwarfare. Because of this they have invested £1 billion into a new battlefield system and set up a new Cyber and Electromagnetic command.
The army has released their blueprint for the future soldier, where they are planning to embrace experimentation of trialling new technologies and integrating them into the way they fight. Over the next decade, the Army aims to modernise its deployable digital capabilities. They are also working on more algorithmic warfare, by trialling new artificial intelligence systems to compress decision cycles and speed target enagagement.

Conclusions

It is not solely the army's role to protect the UK from cyber attacks, we also have the NCSC, GCHQ, and MI5 for example. However, reliance on third party suppliers and foreign-owned technology providers may create additional strategic and legal risks. The army has too much bureaucracy surrounding technology and there is too much aversion to risk. However, the strategic defense review have recommended a 3 month deadline for bringing in the latest tech to keep up with the pace of modern warfare - meaning a certain level of risk will have to be taken.

References

To view my reference list I used to research and develop this poster, as well as my survey results please scan the QR code.

Contact Details

If you wish for a further discussion or to help develop this research further, you can reach me at:
pb236@st-andrews.ac.uk or
scan for my linkedin

University of St Andrews