THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Taking care against the computer

Precautions in military operations on digital infrastructure

Simon McKenzie and Eve Massingham

Digital infrastructure — the hardware, systems and connections that support access to and use of digital data through public, private or secret networks, including the internet and electromagnetic spectrum — is central to modern life. Its prominence makes understanding how it can be designed for and deployed in armed conflict consistently with international legal obligations more important than ever.

States must take precautions against hostile military operations against digital infrastructure

One obligation that designers of digital infrastructure must consider is the requirement to take precautions against the effects of hostile military operations. This obligation, found in Article 58 of Additional Protocol I to the Geneva Conventions (API), requires the defender to minimize the risk that civilians and civilian objects will be harmed by enemy military operations. At its most basic, it obliges defenders to locate military installations away from civilians and, where appropriate, clearly marking the status of objects. The way that the obligation to take precautions against hostile military operations should be met in the context of operations against digital infrastructure is unclear, particularly as the bulk of the actions will have to occur in anticipation of future actions.

While Article 58 is open to a few interpretations, the most protective — and convincing — looks beyond attacks (resulting

in direct kinetic consequences), and instead treats the obligation as requiring a response to the risk of military operations more broadly conceived. Properly recognising the extent of Article 58 is particularly important in the context of digital infrastructure because not all military operations against digital infrastructure result in direct kinetic consequences. That is, the incapacitation of a computer system can take place without the underlying computer hardware being physically damaged.

Operations against digital infrastructure will become more frequent and potentially more destructive

The range, scale, and targets of operations against digital infrastructure differ enormously and come in a variety of forms. Indeed, a vast number of them take place outside of the context of an armed conflict. Some are akin to classic forms of espionage, where attempts are made to steal information from governments or companies. Others are political operations aiming to have some real-time influence (harming the operation of systems or introducing disinformation). There is also widespread criminal activity, such as using ransomware to hold software and systems hostage.

The usefulness of operations against digital military systems is increasing. Many States are developing the capacity to carry out offensive cyber operations that 'manipulate, deny, disrupt, degrade or destroy targeted computers, information systems, or networks'.[1] The capacity of AI systems to filter vast quantities of data, including audiovisual material, make it particularly helpful in conducting these operations. The deep links between civilian and military systems increase the risk that these operations may have flow on effects on essential services and the broader economy.

Maintaining separation between military and civilian networks is hard

Military and civilian infrastructure are not easily separated. They operate using at least some of the same infrastructure, relying on the same cables, systems, and electromagnetic spectrum. In addition, the speed at which operations against digital infrastructure can occur increases the difficulty of complying with the obligation — particularly if such operations involve a degree of automation or the use of artificial intelligence (AI).

The obligation to 'avoid locating military objectives within or near densely populated areas' (Article 58(b) of API), was drafted with military assets, such as tanks and military personnel, front of mind. However, there is nothing inherent in the wording of the provision that would exclude its application to less tangible objects, such as a crowded computer networks or radio-frequencies. The objective of the provision is to prevent bad consequences for civilians by limiting the placement of military objectives near them.

There are several measures that can be taken to protect civilian digital infrastructure

The simplest measure for complying with Article 58 would be to have entirely separate military and civilian networks for the transmission of all forms of information and communications. It should be adopted where possible as it would (hopefully) make it more likely that an algorithm carrying out a cyber operation would recognize when it had found a valid target. However, the interconnectedness of much of the internet means that such separation will be, at least in some circumstances, impossible (so definitely not feasible); this is even more true for the electromagnetic spectrum. Nevertheless, States should seek to identify the military (and civilian) infrastructure that can be safely isolated from the rest of the internet.

States should also consider adopt computer programming practices which make it possible for malicious code to recognize when a piece of digital infrastructure was protected. This can be thought of as the digital equivalent of painting a red cross or crescent on the top of a hospital or the display of the symbol of cultural heritage protection on UNESCO listed buildings. These 'digital markings' would allow military digital infrastructure to be distinguished from civilian infrastructure.

These steps will help keep civilians safe during armed conflict

Designers should take into account the legal obligation to take feasible measures to separate the civilian and military population. They should invest in creating and exploiting technologies that ensure this barrier or isolation between what is a legitimate military objective and what must be protected. They should also continuously try to develop new digital measures which protect the civilian population in a feasible way.

After all, time is of the essence: the speed at which operations against digital infrastructure can occur means that the time after an operation commences will be very limited. This makes considering the precautionary obligations of attackers and defenders in the design digital military systems more important than ever. ●

1 Australian Cyber Security Centre, 'Offensive Cyber Operations'.

Simon McKenzie & Eve Massingham, 'Taking Care against the Computer: Precautions against Military Operations on Digital Infrastructure' (2021) 12(2) *Journal of International Humanitarian Legal Studies* 224–250

This research received funding from the Australian Government's Next Generation Technologies Fund through Trusted Autonomous Systems, a Defence Cooperative Research Centre. The views and opinions expressed are those of the authors, and do not necessarily reflect the views of the Australian Government or any other institution. They also do not constitute legal advice. Cover image by Blue Planet Studio / stock.adobe.com

Law and the Future of War
School of Law
The University of Queensland
law.uq.edu.au/future-war

TRUSTED AUTONOMOUS SYSTEMS DEFENCE CRC

THE UNIVERSITY OF QUEENSLAND AUSTRALIA