THE ROLE OF TECHNOLOGY IN CYBERWARFARE AND INFORMATION WARFARE

Category: IT Law,Technology Law
written by Sadia Rizvi | May 13, 2024

It would be remiss to disregard the ongoing and prevalent armed conflicts happening all over the globe today. According to the Geneva Academy, more than 110 armed conflicts are currently occurring all over the world, more prevalently in the Middle East and Africa.[1] In Europe, the Russia-Ukraine war has seen the deployment of technologically advanced weapons and the introduction of advanced defence technologies. Experts have termed it as the most technologically advanced wars that the world has ever seen.[2] The age of the internet and digital technologies have brought about the possibility of war occurring on multiple fronts – cyber warfare and information warfare. Cyber warfare is a modern form of war that involves the launch of cyber-attacks against a country with the aim of gaining strategic or military advantage.[3] Information warfare refers to information and information systems that are used as a weapon to contribute to a conflict to gain an information advantage over an opponent.[4]

According to NATO, information warfare is not new phenomenon.[5] Historically, and during other conflicts, traditional news media agencies were used to portray news that are fabricated or misleading to advance a particular narrative. Currently, and in the context of the connected world that we live in today, the dissemination of news has been revolutionised so that fabricated information and false narratives can easily be spread across the world within a few seconds. Information warfare is particularly dangerous to democracies around the world. For example, in 2015/2016, Russian government hackers compromised the United States Democratic National Committee's computer systems.[6] The information harvested related to Hillary Clinton's presidential campaign and was weaponised in order to disrupt the American democracy. At the same time, Russian linked entities exploited social media platforms such as Facebook and Twitter to advertise the hacked data in order to promote anti-democratic content with the sole purpose of undermining the US constituency.

Cyber warfare techniques include the use of technologically advanced weapons such as unmanned aerial vehicles, Artificial Intelligence (AI) systems, and other forms of cyber-attacks on infrastructure

and critical systems. For example, in 2007, Russian backed entities carried out a series of distributed denial-of-service (DDoS) attacks against Estonia's state and commercial websites, in the context of Estonia's decision to relocate a statue of a Soviet soldier.[7] To mitigate against the effects of the attacks, Estonia's internet and web traffic was temporarily blocked. More recently, recent investigations have revealed that the Israeli military utilises an AI program to identify and target Hamas operatives in the Israel-Gaza war.[8] Identifying targets was previously a manual operation with human involvement, however, in contrast, the AI program is able to draw on data from various sources to statistically assess what constitutes a potential target.[9] More importantly, the system is trained on data sets to produce a profile of a Hamas operative, and the parameters of the development of a profile can be set as stringently or as loosely as desired. This raises a number of concerns surrounding biases, accuracy and flaws with potential disastrous consequences for civilians.

These campaigns demonstrate that the internet has enabled opportunities for war on multiple fronts, and fundamentally alters how conflicts around the world develop. Technologically advanced countries have a greater dependence upon cyber capabilities and the ability to use those capabilities to its advantage, however, that dependence comes with a number of vulnerabilities. Attacks on critical infrastructure such as power grids and transportation systems are even more serious and have the capability to leave a path of destruction while opening the door for chaos in organised societies. The international laws of armed conflict do not sufficiently address cyber conflicts nor is there a cohesive approach for the use of cyber weapons in our technologically developed world. Information technology is now the underpinnings of global infrastructure in the developed world, and this means that we need to give serious consideration to the large-scale and potentially disruptive effects of cyber warfare and information warfare.

With this in mind, we must consider the legal implications of information warfare and cyber warfare. With information warfare and cyber warfare becoming the new battlefield, states should implement laws that seek to protect critical infrastructure during times of war, aligned to the international laws of armed conflicts. For example, in October 2023, advisers to the International Committee of the Red Cross sought to propose a set of rules for "civilian hackers" during war.[10] Rule three provides that when planning a cyber-attack, attackers must do everything feasible to avoid or minimise the effects on civilians.[11] In as much as armed conflicts can have disastrous consequences for civilians on a physical scale, cyber-attacks against critical infrastructure and the dissemination of propaganda on social media may have even more significant impacts. Unlike conventional methods of warfare, these types of attacks have the potential to disrupt the operations of governments in delivering crucial services to citizens. Moreover, information warfare tactics compromises the ability of citizens to receive relevant information that is impartial and fair.

In light of this, and our increasing reliance on digital technologies, we must consider the measures we can take to protect against cyber warfare and information warfare. Our international legal frameworks must be aligned to address the proliferation of fake news, propaganda, misinformation and disinformation. Data privacy laws and intellectual property rights are especially important in protecting our cyberspace and safeguarding against cyber threats. Social media platforms can further implement accountability measures to protect freedom of expression but at the same time, curbing harmful content used in information warfare tactics. Lastly, given that 4 billion eligible voters may potentially be heading to the polls this year, we must be extra cautious by verifying the credibility of the information we receive to safeguard from information warfare tactics.

Contact us for more good, clear, precise advice.

---

[1] https://geneva-academy.ch/galleries/today-s-armed-conflicts as of 16 April 2024.

[2] https://www.freiheit.org/ukraine-and-belarus/use-technologies-russia-ukraine-war.

[3] https://www.avast.com/c-cyber-warfare.

[4] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.

[5] Ibid.

[6] https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

[7] https://www.cfr.org/cyber-operations/estonian-denial-service-incident.

[8] https://www.businessinsider.com/israel-using-ai-gaza-targets-terrifying-glimpse-at-future-war-2024-4#:~:text=Recent%20investigative%20reports%20suggest%20the,and%20thousands%20of%20civilian%20casualties.

[9] https://theconversation.com/gaza-war-israel-using-ai-to-identify-human-targets-raising-fears-that-innocents-are-being-caught-in-the-net-227422.

[10] https://theconversation.com/governments-and-hackers-agree-the-laws-of-war-must-apply-in-cyberspace-216202.

[11] https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/.