35th Council
3-5 June 2022
Riga
by the European Greens

# Offensive cyber warfare must be banned

Cyber warfare has become an integral part of many military doctrines as control of the digital battlefield is currently a strategic priority for most militaries. However, there are numerous examples of major military powers abusing cyber weapons in a way that has the potential to cause uncontrolled harm to civilian populations.

In 2015, Russian intelligence and military forces and their adjacent actors undertook large cyber operations in Ukraine as part of their ongoing hybrid warfare activities. These actions resulted in more than 200,000 Ukrainian consumers losing their access to the power grid for up to six hours. In 2009, the USA and Israel released the Stuxnet worm in Iran and neighbouring countries with the aim of disabling the Natanz uranium enrichment plant. While searching for the plant, the worm infected hundreds of thousands of computers, causing malfunctions. Most large nations have active cyber warfare units and programs, such as Israel's Unit 8200, China's Unit 61398 and North Korea's 'Lazarus Group', USA's NSA or have used the Pegasus software, some of which have attacked companies and civilians using ransomware and other malware. Targets have included large internet infrastructure providers, such as Akamai and Juniper, and financial institutions such as the Bangladesh Bank.

These are examples of a culture of neglecting collateral damage to civilian infrastructure while to reach military targets, although the attacks in Ukraine directly targeted civilian infrastructure.

A key identifying characteristic of weapons of mass destruction is their proclivity to affect both military and civilian targets equally, with very little or no ability to target or limit their effects. Suddenly disabling the power grid has major effects on vulnerable civilian populations, although the real risk comes with attacking traffic and industrial control systems directly. It is well documented that even the industrial control systems in hydroelectric power plants have been directly exposed to the internet, as well as traffic control and telecommunications systems.

Similar arguments were used to ban chemical and biological weapons in 1997 and 1975, respectively. These international agreements have been used successfully to remove biological and chemical weapon stockpiles from several countries.

It follows that an international treaty to ban offensive cyber warfare is an appropriate measure to deal with this threat before it results in civilian casualties. Although discussions to extend existing humanitarian law to cyber warfare are currently ongoing, these instruments are much less effective than widely ratified international agreements.

Such agreements must facilitate solving the attribution problem in cyber warfare: it is very hard to identify the identity or even the country of origin of an attacker. Arms-length adjacent actors can be used to cover nation-state involvement while, on the other hand, there are proven cases where nation-states or non-government actors have tried to masquerade as other nation states. Therefore, it is important that these international instruments create ways for governments to share information and provide mutual assistance to attribute emerging cyber threats.

Problems of attribution notwithstanding, there are actions that should not be limited or restricted. Non-violent forms of hacking by non-government actors in the interest of transparency and against oppressive regimes should not be criminalised.

These agreements should make a clear distinction between defensive and offensive cyber actions. In addition to helping attribute cyber threats operating on their own soil, nations must commit to not maintaining attack-oriented cyber warfare units and to providing clear distinctions between signals intelligence, electronic warfare and other similar, military-targeting activities and potentially uncontrollable cyber activities.

There are valid concerns as to whether such agreements would reduce the abilities of participating states to adequately defend themselves against non-parties. Unlike weapons of mass destruction, cyber weapons are relatively cheap and easy to develop and deploy, requiring minimal infrastructure. However, cyber warfare also maintains a continuing uneasy balance between defence and offence since most attacks are based on unknown vulnerabilities in widely used software. Most cyber warfare agencies pursue policies to withhold public disclosure of non-exploited vulnerabilities in order to use them as future cyber weapons. Banning offensive cyber operations would put an end to this balancing act and force public agencies to work for the public good.

The **European Green Party**:

- Calls on the EU institutions and the Member States to cooperate to ensure protection of critical infrastructure against cyberattacks and to strengthen overall preparedness and capability to mitigate the effects of such attacks and welcomes the agreement on the NIS 2 directive, strengthening EU-wide cybersecurity and resilience;
- Calls on the European Commission to introduce initiatives and funding for research and development into the preparedness and resilience of Member States against cyberattacks;
- Calls on the competent European Agencies and the Member States to cooperate in investigating and prosecuting those responsible for cyberattacks to oblige all actors to report security breaches and to reject hack backs as an instrument for cyber defence;
- Calls on the European Commission to ensure social media platforms are kept accountable for their role in limiting independent journalists' freedom of expression;
- Calls on EU institutions and the Member States to keep large internet service providers accountable for maintaining adequate cyber protection;
- Calls on EU institutions and NATO to cease the development of mutual offensive cyber capabilities between Member States;
- Calls on the Greens in all Member States to call for the cessation of offensive cyber activities in their respective countries;
- Calls on the Member States to promote an international agreement to ban offensive cyber activities, help attribute cyber activities and provide clear distinctions between other military activities and potentially dangerous cyber activities;

- Calls on the Member States to maintain a balance between defence against cyber/information operations and civil rights;
- Calls on the European Data Protection Board and the Member States to maintain a high bar to approve new high-risk automated data processing as this poses a particularly high risk of damage to fundamental rights and freedoms.