

Offensive cyber warfare must be banned

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

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

17 Targets have included large internet infrastructure providers, such as Akamai
18 and Juniper, and financial institutions such as the Bangladesh Bank.

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

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

30 Similar arguments were used to ban chemical and biological weapons in 1997 and
31 1975, respectively. These international agreements have been used successfully
32 to remove biological and chemical weapon stockpiles from several countries.

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

38 Such agreements must facilitate solving the attribution problem in cyber
39 warfare: it is very hard to identify the identity or even the country of origin

40 of an attacker. Arms-length adjacent actors can be used to cover nation-state
41 involvement while, on the other hand, there are proven cases where nation-states
42 or non-government actors have tried to masquerade as other nation states.
43 Therefore, it is important that these international instruments create ways for
44 governments to share information and provide mutual assistance to attribute
45 emerging cyber threats.

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

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

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

66 ~~Information and cyber operations and measures taken against citizens have also~~
67 ~~affected their freedom of expression and the freedom of the press. During~~
68 ~~Russia's current attack on Ukraine, independent journalists were blocked from~~
69 ~~major social media channels after the platforms flagged their accounts as~~
70 ~~suspicious. This has resulted in both chilling effects and difficulties for~~
71 ~~anti-war activists. Social media is an important public sphere: for example,~~
72 ~~YouTube provides a major alternative news medium in the highly controlled~~
73 ~~Russian media environment.~~

74 The **European Green Party:**

75 Calls on the EU institutions and the Member States to cooperate to ensure
76 protection of critical infrastructure against cyberattacks and to
77 strengthen overall preparedness and capability to mitigate the effects of
78 such attacks and welcomes the agreement on the NIS 2 directive, strengthening EU-wide
79 cybersecurity and resilience;

80 Calls on the European Commission to introduce initiatives and funding for
81 research and development into the preparedness and resilience of Member
82 States against cyberattacks;

- 83 Calls on the competent European Agencies and the Member States to
84 cooperate in investigating and prosecuting those responsible for
85 cyberattacks to oblige all actors to report security breaches and to reject Hackbacks as an
86 instrument for cyber defence;
- 87 Calls on the European Commission to ensure social media platforms are kept
88 accountable for their role in limiting independent journalists' freedom of expression;
- 89 Calls on EU institutions and the Member States to keep large internet
90 service providers accountable for maintaining adequate cyber protection;
- 91 Calls on EU institutions and NATO to cease the development of mutual
92 offensive cyber capabilities between Member States;
- 93 Calls on the Greens in all Member States to call for the cessation of
94 offensive cyber activities in their respective countries;
- 95 Calls on the Member States to promote an international agreement to ban
96 offensive cyber activities, help attribute cyber activities and provide
97 clear distinctions between other military activities and potentially
98 dangerous cyber activities;
- 99 Calls on the Member States to maintain a balance between defence against
100 cyber/information operations and civil rights;
- 101 Calls on the European Data Protection Board and the Member States to
102 maintain a high bar to approve new high-risk automated data processing as
103 this poses a particularly high risk of damage to fundamental rights and
104 freedoms.