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

Final CAS Amendments to R5: Offensive cyber warfare must be banned						
№	**Lines**	**Tabled by**	**Original text**	**Proposed amendment**	**Proposed procedure**	**CAS decision**
1	AM-15-2	Bündnis 90/Die Grünen	malfunctions. Most large nations have active cyber warfare units, such as Israel's Unit 8200, China's Unit 61398 and North Korea's 'Lazarus Group', which have attacked companies and civilians using ransomware and other malware.	**Insert from line 13 to 15:** malfunctions. Most large nations have active cyber warfare units, such as Israel's Unit 8200, China's Unit 61398 and North Korea's 'Lazarus Group', USA's NSA, Germany's Pegasus, some of which have attacked companies and civilians using ransomware and other malware.	Proposal: German and Finnish Greens: 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.	Accepted as amended
2	AM-45-1	FYEG	governments to share information and provide mutual assistance to attribute emerging cyber threats.	**Insert from line 44 to 45:** governments to share information and provide mutual assistance to attribute emerging cyber threats. Next to the problem of attribution, the other reason why International Humanitarian Law cannot address this issue is the question of physical impact of the attack. If a cyberattack has no physical impact on civilians it should be lawful in contrast to a cyberattack that physically impacts civilians lives.	Proposal by the Finnish Greens & FYEG: "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."	Accepted as amended

3	AM-63-1	Groen	Information and cyber operations and measures taken against citizens have also affected their freedom of expression and the freedom of the press. During Russia's current attack on Ukraine, independent journalists were blocked from major social media channels after the platforms flagged their accounts as suspicious. This has resulted in both chilling effects and difficulties for anti-war activists. Social media is an important public sphere: for example, YouTube provides a major alternative news medium in the highly controlled Russian media environment.	**Delete from line 63 to 70:** ~~Information and cyber operations and measures taken against citizens have also affected their freedom of expression and the freedom of the press. During Russia's current attack on Ukraine, independent journalists were blocked from major social media channels after the platforms flagged their accounts as suspicious. This has resulted in both chilling effects and difficulties for anti-war activists. Social media is an important public sphere: for example, YouTube provides a major alternative news medium in the highly controlled Russian media environment.~~	Proposal: Discuss at CAS	Accepted
4	AM-75-2	Bündnis 90/Die Grünen	strengthen overall preparedness and capability to mitigate the effects of such attacks; cooperate in investigating and prosecuting those responsible for cyberattacks;	**From line 74 to 75:** strengthen overall preparedness and capability to mitigate the effects of such ~~attacks;~~attacks attacks and welcomes the agreement on the NIS 2 directive, strengthening EU-wirde cybersecurity and resilience; **From line 80 to 81:** cooperate in investigating and prosecuting those responsible for ~~cyberattacks;~~cyberattacks to oblige all actors to report security breaches and to reject Hackbacks as an instrument for cyber defence;	Proposal: Discuss at CAS	Accepted