A liberal response to current and emerging cyber threats

The Congress of the Alliance of Liberals and Democrats for Europe (ALDE) Party convening in Dublin, Ireland, on 2-4 June 2022:

Notes that:

- every year, cyber attacks all over the world are getting more sophisticated and more frequent. Additionally, the COVID-19 pandemic has sparked an enormous increase in the dissemination of disinformation all over the world and also in Europe;
- over the past decade, large-scale cyber attacks, though believed to be a problem of the future, have affected the functionality of whole European countries (e.g. 2007 cyber attacks on Estonia, NotPetya in 2017);
- various member states of the European Union have recorded cyber-driven attempts to sabotage their elections in recent years;
- while the overwhelming majority of international lawyers agree that international law applies to the cyber domain, use of force in the cyber domain is rarely publicly attributed to a specific threat actor;
- there is no such thing as an effective export-control for cyber weapons;
- national parliaments within the European Union rarely pass legislation that provides clear guidelines to their governments with regard to the development or use of offensive cyber capabilities;
- deterrence does not work in the same way in the cyber domain as in other domains since every piece of software can be leaked or stolen even from powerful agencies such as the U.S. National Security Agency (NSA). The NotPetya malware made use of an exploit that is believed to have been created by the NSA;
- undersea cables are the central link in the internet, and today around 95% of international data traffic flows via them;
- Admiral Tony Radakin, head of UK's armed forces, warned in The Guardian of 8 January 2022 that there had been a "phenomenal increase in Russian submarine and underwater activities" over the past twenty years. Russia could threaten and possibly exploit undersea cables, "the world's real information system", and added that any attempt to damage them could be considered an "act of war"

Believes that:

- the EU is to play a key role in the field of cyber-security in the world;
- the EU's approach towards cyber threats must be de-escalation. Non-offensive, peaceful conflict resolution, prevention, dialogue, cooperation and training are the language of the EU in this context. The

Resolution:
A liberal response to current and emerging cyber threats

Year and Congress:
Dublin, June 2022

Category:
EU Single Market and Economics

Page:

EU also has to engage with unlike-minded countries in questions of cyber security;

- the EU needs both defensive and offensive operations to meet cyber threats. Defensive operations aim to defend information systems, while offensive operations aim to prevent the opponent from carrying out the attacks, by for example conducting deceptive activities that cause the opponent to discontinue an attack;
- the EU should take a forward-looking approach to tackling cyber-security, ensuring proper information sharing and pan European efforts to protecting Europe's critical infrastructure from future cyberattacks;
- while the framework of cyber sanctions has turned out to be a dynamic regime, Europe can still improve in this area. e.g. effectiveness of cyber sanctions is often doubtful. Also, the EU could find its role in the global debate about cyber attacks in calling out irresponsible and unlawful behaviour by other big players. e.g. regarding espionage or sabotage;
- further proliferation of cyber arms makes the world less safe. The goal is to get the big players in the field to invest more in defensive and less in offensive capabilities;
- a "cyber treaty" that merely repeats rules already enshrined in international law is unnecessary and might even undermine trust in international law;
- the preservation of EU's citizens' fundamental rights and liberties must be a primary concern in all debates with regard to the Member States' and the EU's cyber security;
- unproportional use of surveillance technology by state institutions is inacceptable;
- the EU does not only need means of defence against potential attackers, it also needs clear rules with regard to the actions of allied countries in its cyberspace;
- cyber attacks below the threshold of an armed attack are equally dangerous in the long run as a large-scale attack: Theft of strategically important information or information on vital infrastructure, dissemination of disinformation, sabotage and other attacks that do not constitute an armed attack bear a big potential to undermine and severely damage our democracies and economies;
- effective cyber defence needs adequate financing;
- resilience is key in all of our efforts to keep the European Union and its allies safe from cyber attacks. This includes public awareness as well as developing and maintaining its own digital infrastructure;
- undersea cables on the seabed are of great geopolitical importance: whoever controls them may be able to read or even influence the flow of information.

Calls for:

- deterrence not through proliferation of weapons but proliferation of talent, skills and knowledge. To scare off attackers the EU should aim at becoming as resilient as possible to drive up the cost of attacking us for the Union's adversaries;
- a concrete and feasible plan for Europe to develop, own and control all vital cyber infrastructure within Europe to secure strategic autonomy within the cyber domain as soon as possible;
- an expansion of competences for the European Union for Cyber Security (ENISA), fully funded by the EU budget, to enable it to secure the EU cyber space and critical infrastructure;
- the creation of units under ENISA focusing on cyber-attacks, cyberterrorism and cyber-security, equipped with the appropriate resources and mandate to fulfil these goals, as well as research units;
- a united effort to increase reaction speed in the fight against disinformation by building stronger alliances between public and private institutions and citizens in this regard. A united effort to strengthen digital literacy throughout all socio-economic groups of European society;
- financial incentives for people to find and report vulnerabilities to the authorities to make it beneficial to fight crime rather than commit it;
- a European framework for united statements of attribution and condemnation of cyber-attacks within the EU and in third countries;
- a joint European Union position on the acquisition and use of so-called "zero day exploits" by EU national governments;
- the use of accurate language in the cybersecurity debate. Not everything is a cyber war. Liberal parties need to strike a balance between using legally correct, de-escalating words and clear messages that convey the seriousness of the issue;
- clear conditions under which allied third states are allowed to operate in European networks and vice versa for security reasons. The EU needs a standard procedure for e.g. prior notification of the relevant state;
- EU Member States and NATO to stepping up their efforts to protect critical undersea infrastructure that is crucial to communication systems around the world.