Cyber: How big is the threat?

The internet has transformed the world into a global village transcending physical borders and palpable distances. Often described as 'fog' or a 'globalised network of networks', cyberspace is extremely complex, accessible to everyone and difficult to pinpoint. While thanks to these characteristics cyberspace has opened countless social, economic and political opportunities, it has also become a source of disruption, conflict and geopolitical rivalries. The European Union has recognised that cyber-security and cyber-defence are critical for both its prosperity and security, and is emerging as an increasingly capable cyber player.

Deciphering the cyber realm

Nowadays, 'cyber' (meaning 'of, relating to or involving computers or the internet') is used in combination with words such as security, defence, attacks and deterrence. Cyber-associated terms have numerous definitions and interpretations. For instance, even though often used interchangeably, cyber-security and cyber-defence signify different activities. Cyber-security includes information and communication security, operational technology and the IT platforms required for digital assets. Cyber-defence is usually understood as including cyber-security, and consisting of threat analyses and strategies to protect against threats directed at citizens, institutions and governments. As for cyber-attacks, these are deliberate activities to disrupt or destroy computer systems and networks. Cyber-deterrence refers to measures for dissuading potential perpetrators through robust systems, sanctions mechanisms and cyber-diplomacy.

Significance of the cyber threat

As society's dependence on the internet grows, so does the number of cyber-threats and the sophistication of cyber-attacks. Estimates suggest that by 2030, there will be 125 billion devices connected to the internet, and 90 % of individuals older than 6 will be online. Such connectivity also gives rise to vulnerability. Given the accessibility and relatively low cost of operations, anybody, be they individuals, professional criminals, state or non-state players, could become a perpetrator. Worldwide, countries are actively developing offensive cyber capabilities in the pursuit of geopolitical goals. The global cost of cybercrime is estimated at about €530 billion. Attacks are fast increasing in terms of number, disruptive potential and financial damage, outstripping governments' capacity to deal with them. In 2017, Commission President Jean-Claude Juncker said that cyber-attacks pose more danger to democracies and economies than guns and tanks.

Cyber-attacks can be damaging not only to the economy of the EU but also to its democratic foundations. When deployed together with other offensive actions, such as disinformation, economic pressure and conventional armed attacks, cyber can be part of a hybrid operation. Risks from the digital realm can destabilise governments and political systems, sow societal divisions and increase the risk of internal and external conflict. The World Economic Forum's 2019 global risks report places cyber among the top five likely risks and top 10 most impactful risks. One of the most notable examples is the WannaCry attack, which spread to 300 000 computers in 150 countries, and the Petya and NotPetya attacks, which caused financial losses worth hundreds of millions. These attacks illustrate the growing trend of actions targeting strategic sectors and critical infrastructure, causing enormous disruption and provoking interstate tensions. Cyberspace is an increasingly contested political space and a potential source of international tensions. A key challenge faced by law enforcement bodies lies in the difficulty of attribution and in tracing perpetrators. Another is the legal and ethical dimension regarding the appropriate state response.

Possible solutions

It is increasingly accepted that resilience to cyber-threats requires a collective, collaborative and wide-ranging approach. An example in this regard is the new initiative for establishing common international norms for tackling cyber threats, the 'Paris Call for Trust and Security in Cyberspace', launched by French President Emmanuel Macron in November 2018. Though not legally binding, the Paris Call is a high-level declaration for cooperation in cyberspace that was endorsed by 64 countries, as well as NGOs, universities and hundreds of private companies. Another example is the Tallinn Manual – an evolving document

Author: Tania Lațici, Members' Research Service
PE 637.980 – July 2019

examining conflict in cyberspace from an international law perspective, written by a group of independent experts. Besides resilience, prevention is also a key pillar of cyber-defence. Two possible approaches to prevention are deterring and dissuading adversaries. The objective is to make a cyber-attack so financially unfeasible, as to discourage potential perpetrators from launching it. A group of experts have also developed three scenarios for strengthening the EU's cyber-defence: 1) full implementation of the cyber package to increase operational capabilities; 2) creating a 'cyber-defence coordinator' with advisory and oversight powers and the task to decrease intra-EU fragmentation; 3) building on the first two, creating a 'cyber-defence agency' to add a strategic and operational mandate at the EU level.

In 2018, the United Nations General Assembly adopted two resolutions on cyber: on creating a working group to study cyber norms and possible dialogues, and on creating a group of government experts to study the applicability of international law to states in cyberspace. Again in 2018, UN Secretary General, António Guterres, also created a High-level Panel on Digital Cooperation to strengthen cooperation between all stakeholders, from governments to the private sector, in the digital sphere. American political scientist, Joseph Nye, argues that the diffusion of power from governments to non-state actors is one of the great shifts of this century. In a recent article, *Foreign Policy* magazine observed that even though 'cyberwarfare does have rules … these rules are not intuitive to generals used to fighting conventional wars'. The academic and industrial consensus points to the need for creating rules for the cyber realm.

The EU as an emerging cyber actor

Over eight in 10 (87 %) EU citizens see cybercrime as an important challenge, in line with the EU's 2016 global strategy, which says that 'our Union is under threat', including cyber-threat. The strategy emphasises that the EU needs to become a 'forward-looking cyber player' engaged in cyber-diplomacy and in building its partners' capacity. The evolution of the threat landscape since the EU's 2003 global strategy is obvious, as the earlier strategy made no mention of cyber. Since its first cyber-security strategy adopted in 2013, the EU has gradually developed cyber ambitions and tools to manage the challenge. The year 2017 was a landmark one for cyber in the EU, with the launch of the Commission's cybersecurity package. It includes, among other things: a permanent mandate to the EU Agency for Network and Information Security (ENISA); an EU cybersecurity certification framework; full implementation of the 'NIS' Directive; a blueprint for rapid emergency response; establishing EU-wide cyber-research centres; improving law-enforcement response; and improving the overall political response and deterrence. Since the Commission does not have operational capabilities of its own, it is supported by agencies and bodies, such as ENISA, Europol (especially its European Cyber Crime Centre), the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the Computer Emergency Response Team (CERT-EU) and the Intelligence and Situation Centre (INTCEN). As for the Council, its 2017 conclusions established a framework for a joint EU diplomatic response to malicious cyber activities. On 17 May 2019, the Council established an autonomous sanctions framework for cyber-attacks, meaning that the EU is now able to impose sanctions on perpetrators or accomplices.

Cyber-defence aspects have also been included in the 2016 European defence action plan, prioritised in the European Defence Agency's 2018 capability development priorities, addressed through several projects under permanent structured cooperation (PESCO), and listed as one of the seven concrete areas of EU-NATO cooperation. Cyber-defence also has implications for the EU's solidarity and mutual assistance clauses as well as for the functioning and protection of EU missions and operations. The EU also holds numerous cyber-dialogues with international organisations, such as the UN, the Council of Europe, the OSCE and the OECD, and with partners such as the United States, Canada and Japan, to name a few.

The European Parliament welcomed the Commission's cyber package, emphasising the EU's and NATO's 'special responsibility and capacity' to address cybersecurity and defence and calling on EU Members to prioritise their cyber-defence capabilities. In March 2019, Parliament approved the proposed cybersecurity act, establishing the first EU cyber-certification scheme and giving ENISA a permanent mandate.

Ensuring effective cyber-deterrence of malicious actors remains a challenge for the EU, and pan-European efforts for resilience, deterrence and defence should be strengthened and streamlined further. Experts have argued that deeper engagement by EU countries can hone a more systematic approach to fixing weak links and gaps, and can generate more robust and effective EU action on cyber.