European Cybersecurity Reloaded

The EU and NATO allies should start preparing for an increased number of cyberattacks in the future

BY MERLE MAIGRE

For several years now, cyber has featured at the top of the threat assessments for ministers, diplomats and security officials. States are increasingly weaponizing information to gain advantage, breaking into other countries' networks to steal data, and seeding misinformation or disrupting critical infrastructure. This is exemplified by the Baltic ministers of foreign affairs formally noting in April 2021 an increase in information and cyberattacks directed against European countries, aimed at undercutting their support for the democratic processes in Belarus and Russia.

Since early 2021, the trend of criminal groups using ransomware – a software used to deny targets access to data or to threaten to leak their stolen data unless they pay a ransom – has been growing at a global level. In May, the attack on the US energy company Colonial Pipeline affected the pipeline that provides almost half of the fuel used on the east coast of the United States. A few weeks later, an attack on the Irish healthcare system cut access to diagnostics and medical records for over a week.

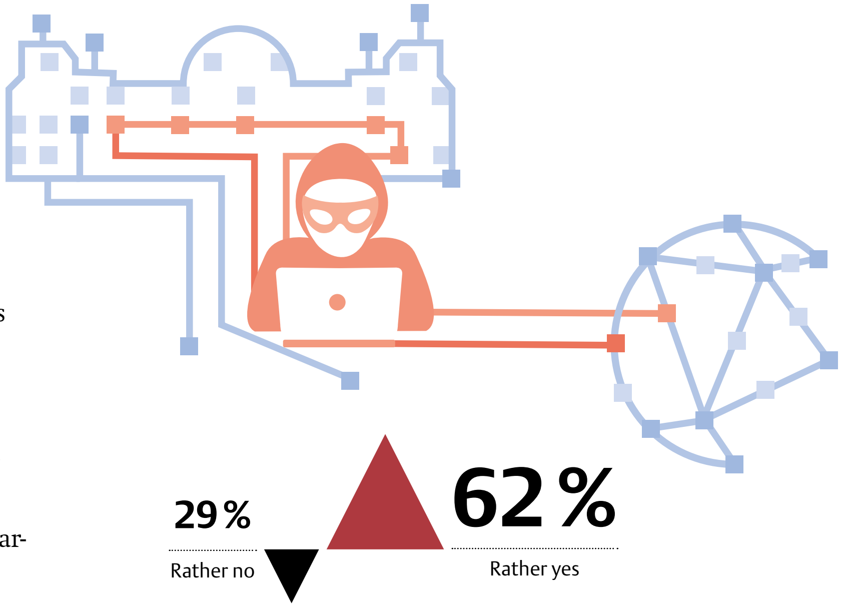
How can European decision-makers better anticipate and understand the effects of cyberattacks? First, holding exercises for how to respond to cyberattacks is one of the best ways to raise awareness at the political level. In September 2017, Estonia organized the first-ever cyber exercise for all EU defence ministers, with the NATO secretary-general also attending. Germany's defence minister at the time, Ursula von der Leyen, called it an 'extremely exciting' war game that showed the need for EU governments to be more aware of the impact cyberattacks have on critical infrastructure. In 2018 and 2020 similar exercises were organized with EU home affairs ministers in Helsinki and during the Nordic-Baltic foreign ministers meeting in Tallinn.

Cyber exercices raise political awareness

Russia's Zapad 2021 military exercise in September in Russia and Belarus included one of the largest uses of electronic warfare. Even if the Baltic-Polish defence leadership did not monitor navigation or communication disruptions during it, it is nevertheless important that NATO continues to adapt to the evolving cyber threat landscape.

At the NATO Summit in Brussels in June, the allies endorsed a new policy that highlights collaboration as key to strong cyber defence. One step that NATO and countries on its eastern flank should take is to rehearse jointly responding to cyber threats. Regular cyber exercises should take place in the multinational NATO battle groups in Estonia, Latvia, Lithuania and Poland that are led by the United Kingdom, Canada, Germany and the United States.

When faced with a cyberattack, should Germany react with offensive countermeasures (‘Hackback’)?



2021: don’t know 8 %, no answer 1 %

Second, accountability must be increased by applying existing international law to cyberspace and creating a clear legal framework that regulates state behaviour in it. Accountability also requires transparency and attribution. Until recently, cyber incidents were not discussed publicly by governments. Since 2018, however, public disclosures by several Western powers of details of cyberattacks indicate a new multinational policy of state transparency. Greater public knowledge of cyberattacks makes cyber conflict comprehensible and leads to greater public acceptance of cyber countermeasures.

Attribution is the basis for self-defence

Ultimately, what matters is that states engaging in unlawful actions using cyber means will not escape without consequences. With attribution, policymakers show that they know what is going on in networks and can investigate incidents. It also clearly states what unacceptable behaviour is and can help create state practice. Attribution is the basis, under international law, for countermeasures and self-defence.

Third, European decision-makers must respond clearly to harmful actions of other state actors.

The EU Diplomatic Toolbox adopted in 2017 is an example of collectively pre-agreed possible response measures. It offers a framework for joint EU diplomatic responses to malicious cyber activities, such as adopting condemning statements, declaring diplomats persona non grata or imposing sanctions on an adversary.

Another example is the CERT-EU Computer Emergency Response Team that provides for a close exchange of information at a technical and operational level in Europe. On top of that, the EU Joint Cyber Unit proposed by the European Commission in June 2021 aims at bringing together resources and expertise available to the European Union and its member states to prevent, deter and respond to mass cyber incidents and crises. The central pillar of the Joint Cyber Unit is the rapid-reaction teams composed of experts designated by member states. These teams can be deployed when EU countries face a cyberattack and allow them to call other members for help. Therefore, it is high time for Germany to prepare and think about its role and willingness to help when European allies are in need.

Most real-world crises in the future will have cyber components that require a political and diplomatic response in addition to technical responses. How our national cybersecurity strategies are translated into policies and procedures needs to be understood by all stakeholders. What governments and enterprises – including in Germany – can do today is to prepare to respond and to prepare through regularly engaging in realistic cyber exercises.

MERLE MAIGRE
is senior cyber expert at the e-Governance Academy in Tallinn.