# Cyber-attacks: Not just a phantom menace

Some 96 % of young people (and 70 % of citizens) in Europe use the internet every day. The young communicate, play, shop, learn and work online. While offering a galaxy of opportunities, the digital environment also has a dark side. Cybercrime knows no borders and cyber-attacks can take on various forms, targeting all kinds of things, ranging from our devices and wallets, to our way of life. How can we make our digital society more resilient and our cybersecurity stronger? How does the EU help us reinforce our cyber-preparedness and response?

## Should we be afraid? The threat landscape

According to a 2017 Eurostat survey, 86 % of Europeans feel increasingly exposed to the risk of falling victim to cybercrime. Indeed, the number and variety of attacks have reached unprecedented levels. In some European countries, cybercrime accounts for half of all crimes committed. With its economic impact having risen fivefold between 2013 and 2017, cybercrime has inflicted losses worth hundreds of billions of euros a year. Moreover, people identify cyber-attacks from other countries as a main threat to national security.

*Where is my money?* The survey reveals that Europeans are most worried about the potential misuse of their personal data and the security of online payments. These concerns are largely justified: cybercriminals use different techniques, such as phishing attacks, to steal credit or debit card data and make unauthorised bank transactions or purchases online. Such 'card-not-present fraud' is a growing trend in the EU.

*I want my data back!* Criminals are not only attracted by your money - they have a huge interest in the new 'black gold': your data. Every day, over 5 million data records are lost or stolen. Among the recent massive data breaches, the Uber case triggered a lot of attention and a joint investigation in Europe, after the company paid hackers US$100 000 to hide a breach that exposed the data of 57 million users and drivers.

*Should I pay or should I not?* To achieve their goals, attackers use various types of malware: viruses, worms, trojans, ransomware, etc. Ransomware attacks, which block access to your device or data unless you pay a ransom, have grown exponentially since 2016, targeting not only individuals but also businesses and critical infrastructure. In May 2017, a global ransomware attack of unprecedented scale – WannaCry – infected around 300 000 systems in over 150 countries, including targets such as the UK's National Health Service.

*Smart or dangerous?* Smart homes, cars or toys are not science fiction anymore – the Internet of Things is becoming part of our everyday life. By 2020, tens of billions of (often poorly secured) devices will be connected to the internet, offering attackers a new battlefield. In 2016, several DDoS attacks were launched from a botnet linking an estimated 150 000 IoT devices (such as routers and security cameras), infected with the Mirai malware. One such attack brought down several major websites, mainly in the US.

*The dark side of the web.* While people may legitimately use anonymising networks, such as Tor, the invisible part of the internet where Tor resides – the Darknet – also hosts criminal websites selling illicit goods, such as weapons, drugs, fraudulent documents and stolen financial data, with a fast growing trend of sales of cybercrime tools and services (e.g. malware) as well. Not only the deep web but also the internet in general can be misused to distribute illegal content such as hate speech, extremist or terrorist propaganda, and child sexual abuse material. Disinformation is also spread online to influence democratic processes in Europe.

**Hacks, leaks and disinformation – what is their impact on democracy?**

Hacks and leaks play a key role in the ongoing spread of disinformation, the intentional spread of false information (as opposed to misinformation, or wrong information with no ill intent). Disinformation operations are not limited to false headlines, hoaxes and conspiracy theories. In spring 2018, the US imposed new sanctions on Russia, accusing Moscow of 'malign Russian cyber activity', including the 'attempted interference in US elections, destructive cyber-attacks, and intrusions targeting critical infrastructure'. In the context of the 2017 French presidential election, hacks and leaks played a prominent role in the public debate. During March-May 2017, there were attacks against Emmanuel Macron's election campaign, including spear-phishing campaigns

Authors: Sofija Voronova and Naja Bentzen, Members' Research Service

(email attacks targeting a specific organisation or individual, and seeking unauthorised access to sensitive information), controversial leaks aiming to discredit Macron, and a massive data leak (#MacronLeaks). Emails between Macron, his team, other officials and politicians, as well as original documents and photos, were leaked just a few hours before the pre-election news blackout began. The leaks, boosted by bots (programs that work automatically on the internet) and the official WikiLeaks Twitter account, were spread (mainly in English) by a network of political activists. However, the French electoral commission urged the media to respect the blackout period and to refrain from commenting on the 'Macron leaks'. The Macron campaign and the French media steered public attention towards the fact that a disinformation campaign had been launched, instead of letting rumours about Macron's alleged offshore accounts dominate the debate hours before the election. Curiously, some of the bots used to spread disinformation in France had previously been used in the US election to spread pro-Trump content, suggesting that there might be a black market for reusable disinformation bots. There is concern that the European elections in May 2019 could be targeted by manipulators.

## A more resilient digital society: what is the EU doing?

The EU plays an increasingly active role in addressing the multiple threats described above. In 2013, it adopted its first cybersecurity strategy. Cybersecurity is also one of the priorities of the European agenda on security, the digital single market strategy and the EU global strategy. In September 2017, the European Commission proposed a new holistic approach to cybersecurity, covering three main pillars of EU action: increasing cyber-resilience, enhancing criminal-law response and reinforcing international cooperation. Over the years, the EU has adopted relevant legislation and set up networks for operational cooperation on these matters.

*Protecting networks and personal data.* From May 2018, two major new acts apply in the EU: the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR). These acts introduce an obligation to report cyber incidents and data breaches, respectively, to national authorities. Moreover, the GDPR integrates the principles of privacy by design and by default, while the NIS Directive requires Member States to adopt national cybersecurity strategies and set up cyber-incident response teams (CSIRTs).

*Fighting criminals by means of the law.* Two laws aimed at combating cybercrime have been adopted: on sexual abuse and exploitation of children (including online) in 2011, and on attacks against information systems in 2013. Under the September 2017 package, the Commission proposed to reform the 2001 law on card fraud and counterfeiting of non-cash means of payment, in order to adapt EU legislation to evolving threats.

*Tackling illegal content.* In March 2018, the Commission issued a recommendation on operational measures to be taken by online platforms and Member States to protect citizens from harmful online content. The EU is also active against fake news through its East Stratcom Task Force and other initiatives.

*Uniting forces against malicious actors.* While the responsibility for citizens' security lies primarily with the Member States, the EU has created specific structures to coordinate their efforts. The body in charge of building the EU's cyber resilience is the European Network and Information Security Agency (ENISA). The 2017 proposal on the Cybersecurity Act, currently under consideration, will reform ENISA into an EU Cybersecurity Agency, with a permanent mandate and adequate resources. On the other hand, a European Cybercrime Centre (EC3) has been set up within Europol to coordinate the law-enforcement response. The EU also fosters public-private partnerships on cybersecurity and cybercrime. One concrete example is the www.nomoreransom.org website, helping victims of ransomware to regain access without paying. The project, launched by the EC3 in cooperation with Kaspersky and McAfee, now has more than 100 partners.

*Acting globally*. To strengthen global cyber stability, the EU aims to build and maintain robust alliances with third countries and international organisations, such as the Council of Europe, the UN and NATO. EU-NATO cooperation on cybersecurity, defence and hybrid threats is increasing, as shown by the creation of the European Centre of Excellence for Countering Hybrid Threats in Helsinki, open to NATO allies. A 'Cyber Diplomacy Toolbox', set up in 2017, will enhance the EU's response to malicious cyber activities.

*This note has been prepared for the European Youth Event, taking place in Strasbourg in June 2018.*