EUROPEAN POLICY CENTRE

POLICY BRIEF

8 June 2017

European cybersecurity policy – Trends and prospects

Iva Tasheva

BACKGROUND: facing new challenges

Increased digitalisation has brought both economic benefits and cybersecurity challenges. According to Europol, an expanding cybercriminal economy is exploiting our increasingly Internet-enabled lives and low levels of digital skills. This became publicly evident in May 2017 with the biggest ransomware attack so far; the WannaCry cryptoworm exploited a security gap in widely used, and often not updated versions of the Windows operational system. The cyber weapon, which enabled hackers to lock (encrypt) the victims' computer files until they paid a ransom, was stolen from the US National Security Agency. It spread within a few hours, affecting 200,000 computers, compromising the security and preventing the work of critical infrastructures, such as hospitals (NHS), public transport (Deutsche Bahn), banks (Deutsche Bank), service providers (Telefónica), delivery services (FedEx), and businesses across the globe.

This incident established the shortcomings of critical infrastructures' computer systems, and it was not an isolated case. Highly publicised attacks appear in the news every day, undermining trust in society. In the US, Russian email hacks interfered in the US elections, demonstrating the (potential) political and societal impact of relatively simple hacks. In Europe, a cyberattack targeted Emmanuel Macron's electoral campaign during the French presidential elections, and hacking incidents in the upcoming German federal elections cannot be excluded.

All of these examples underline the urgency for a coordinated crisis response, while creating a fresh impetus for the introduction of new information security rules. This paper looks at the priorities for EU action on cybersecurity, including efforts to improve information and systems' security, tackle cybercrime, counter cyber warfare, and improve the security of citizens online. It explores the available instruments and suggests action of particular importance to achieve these goals.

STATE OF PLAY: (insufficient) awakening

Since 2013, much has been achieved in terms of EU cybersecurity policies. Cybersecurity is already at the heart of the European Commission's political priorities, ranking high in the Digital Single Market Strategy, and the fight against cybercrime is one of the three pillars of the European Agenda on Security[1]. The EU Global Strategy[2] focuses, among other things, on building cyber resilience, including strong cooperation with NATO.

The Commission took a twofold approach to strengthening EU cybersecurity. On the one hand, the EU and its members are boosting investment in the area of security, encouraging cybersecurity capacity building and industry development, e.g. the Cybersecurity Public Private Partnership, a successful measure for the uptake of the cybersecurity industry and knowledge exchange between the public and private sectors.

On the other hand, the Commission is developing common European policy guidelines, rules and institutions. The 2013 EU Cybersecurity Strategy[3] aims to protect the online environment and preserve freedoms, focusing on five priorities: 1. building resilience; 2. fighting cybercrime; 3. developing cyber defence policy; 4. fostering the industrial and technological resources; 5. embedding the EU values in the cyberspace. It has already delivered

tangible results. This is, along with the Directive on Attacks against Information Systems[4], the first set of common rules on information systems' security – the Network and Information Security (NIS[5]) Directive adopted in 2016. The NIS Directive provides legal measures to increase the level of EU cybersecurity by ensuring that member states: (i) are prepared to respond to cybersecurity incidents via a Computer Security Incident Response Team (CSIRT) and competent national NIS authorities; (ii) support strategic cooperation and the exchange of information on specific incidents and risks; and (iii) identify and encourage cybersecurity among critical infrastructure operators, including the introduction of reporting obligations for incidents. The EU has also made progress in building common cybersecurity institutions since 2013, such as the EU Network and Information Security Agency (ENISA), Europol's European Cyber Crime Centre (EC3), EU Computer Emergency Response Team (CERT-EU), and European Defence Agency. These already helped improve cybersecurity awareness, education, cooperation, and helped investigate attacks, and enforce the law. However, these could be further developed.

At the international level, the EU's diplomatic role on cybersecurity issues is increasing. The EU Global Strategy and the Communication 'A Strategic Approach to Resilience in the EU's External Action'[6] recognised cybersecurity as an emerging global security challenge for the EU and for future cooperation with partners (e.g. NATO, US, China, India). The Union and its members recognise that international cooperation will be significant in order to tackle cyber threats and have established platforms for dialogue and cooperation on cybersecurity with major actors, such as the US in the context of the EU-US Working Group on Cybersecurity and Cybercrime. The EU is also active on cybersecurity issues in multilateral fora, including the Organisation for Economic Co-operation and Development (OECD), the United Nations General Assembly, the International Telecommunication Union, the Organisation for Security and Co-operation in Europe (OSCE), the World Summit on the Information Society, and the Internet Governance Forum. In line with the EU's ambition, the G7 Cyber Expert Group[7] will develop a set of non-binding fundamental elements for effective cybersecurity assessment by October 2017, working on third party risks and in coordination with finance and other critical sectors.

Despite all these recent developments, WannaCry proved large networks of unsecured devices are very vulnerable, and while many attacks are prevented or effectively countered, mobilising a timely response to multiple cybersecurity incidents remains challenging. The need to empower citizens, businesses and public administration to protect themselves is imperative.

PROSPECTS: empowerment and coordination

In May this year, the Commission included cybersecurity as one of the three emerging challenges in its Digital Single Market Strategy mid-term review[8]. On 7 June, the Commission sketched out three options for the future of European defence, emphasising the need for stronger EU cybersecurity cooperation[9]; this should be pursued further. In September, the EU will update its Cybersecurity Strategy. Based on achievements so far, this will be an opportunity to reflect on cybersecurity threats' evolving nature and address persisting issues related to resilience, capacity, and cooperation. To achieve these goals, the EU should live up to its ambition and keep cybersecurity high on the policy agenda, while being realistic given legal and technical limitations. In more concrete terms, six priority actions seem particularly important and need to be further developed.

1. Work across silos

Cybersecurity, given its crosscutting nature and the overwhelming speed of the digitalisation of non-digital sectors beyond the ICT sector, EU policymakers should find synergies and mainstream cyber requirements in all relevant policies, including the (Digital) Single Market, skills, consumers' protection, health, energy, transport, banking, trade, and foreign policy. To achieve this, cybersecurity principles of information and system integrity, transparency, confidentiality, non-discrimination, and competence should be reflected upon in the decision-making process, e.g. in the impact assessment (IA) of legislation. For instance, the Commission's digital contract proposal requires suppliers to store and link data to specific consumers to allow consumers' retrieval, creating privacy and data breach risks. This needs to be addressed in the IA process. Businesses will apply a privacy IA under the new General Data Protection Regulation as from 2018.

2. Reduce Single Market fragmentation

To complete the (Digital) Single Market and enable cross-border trade, the EU needs to remove the technical barriers for the supply of cybersecurity products and services. For example, mutual recognition through EU certification schemes for cybersecurity products could remove administrative and compliance costs. It will enhance trust by setting minimum security requirements for ICT products, a key for the growing number of connected,

Internet of Things devices floating in the market. On the other hand, it is crucial to timely and properly implement the NIS Directive to improve the overall EU security level. Some member states are on track (e.g. Germany, France, Austria, Estonia, and Czech Republic), partly because cybersecurity was already their national priority and similar acts were implemented. Other member states, which have lacked attention and awareness of the severity of the challenge, or underestimated the consequences, need to speed up and implement the NIS Directive as a national security priority.

3. Manage cybersecurity risks

Although the exact impact is sometimes difficult to assess, cybersecurity risks have an economic and societal impact, preventing growth of the digital economy and carrying a financial cost associated with cybersecurity incidents (e.g. theft, interruption in services, costs to recover the data, service, and trust after an incident). The risks cannot be completely eliminated but could be mitigated. To do so, there is a need to create a risk management framework through assessing the risks, analysing the appetite for risks, the acceptable level thereof, and finally, supporting the creation of mitigation tools, for example, developing defence capacity, as well as developing, similarly to the US, cybersecurity insurance schemes to mitigate the losses from incidents (e.g. data breaches, business interruption, cyber fraud, intellectual property theft, and network damage). Considering the cross-border nature, this framework should be developed at the EU level by ENISA for example, and in close cooperation with national authorities.

4. Raise awareness to develop skills

People play a key role in cybersecurity (users, developers, policy-makers) and the EU should empower them to protect themselves. Member states should raise awareness among the less digital savvy (about half of Europeans[10]) through media campaigns and training, available at local services for unemployed and seniors, at work places for employees and officials, and at schools for the youth (some best practices include Finland, Sweden and Germany). This could be done in cooperation with businesses, civil society, regions, and EU institutions, supported by the member states' budget for education and retraining, while tax incentives could encourage additional private sector investments. EU structural funds could also provide financial support. The outcomes should be disseminated across the EU, and the knowledge shared between universities and local communities.

The EU also needs to address the digital skills gap. EU initiatives, such as the New Skills Agenda, Digital Skills and Jobs Coalition, and the Digital Opportunity pilot project are not enough; a long-term framework is urgently needed. For example, students in legal, public policy, management or security studies could take cybersecurity classes where available in the EU, inspired by the success of Erasmus; the programme is already well-known, has an extensive network and secured EU funding. To address the shortage of professionals, work placements for cybersecurity students/graduates (e.g. *Cyberasmus+* for experience in private sector security providers and public entities, e.g. ENISA, CERT-EU, EC3) could help in the short term. In the long term, reinforcing the EU's security and boosting the cybersecurity industry requires talent and the modernisation of education systems. Collaborative professional education, provided online by a network of EU universities and the private sector (see Ubiquity University[11]) could help address the need for affordable, cutting-edge, large-scale training schemes for cybersecurity experts and practitioners.

5. Strengthen the role of ENISA

ENISA's revision could be used to address some of the above issues, taking into account the new responsibilities, such as the mandatory incident reporting for e.g. digital service providers under the NIS Directive, trust service providers (i.e. certificates for e-signature) under the eIDAS Regulation, and telecommunication operators under the Telecom Framework Directive. With growing threats to the critical sectors and increasing cross-border interdependence of economic actors and sectors, ENISA should provide an overview of the ongoing cybersecurity initiatives across the EU. As the Commission's think tank, the European Political Strategy Centre (EPSC), puts it, it is to "be transformed into a fully-fledged European Cybersecurity Coordination Platform, equipped with adequate resources and executive competences"[12] to respond effectively and timely to security incidents.

6. Strengthen the EU-NATO and international cooperation

The majority of EU member states are also NATO members and it is of mutual interest to find synergies between the two cybersecurity efforts and investments. Based on their July 2016 Joint Declaration, reiterated in the Commission's white paper on the future of defence, EU-NATO cybersecurity cooperation is (slowly) progressing with a focus on "cooperation on cybersecurity defence, including in the framework of military missions, exercises,

and education and trainings" and "development of coherent, complimentary interoperable defence capacity for EU member states and NATO allies, as well as multilateral projects"[13]. Exchange of good practices, policies, and information is needed, as well as aligning cybersecurity policies and strengthening the operational cooperation. This is also valid for the EU cooperation with third countries, including in the framework of G7 where cybersecurity cooperation and knowledge exchange are already featured, and in bilateral agreements with the US, Japan, Canada, Australia, and India.

Moreover, the EU should address the growing phenomena of state-sponsored cybersecurity threats. Diplomacy can be a powerful multiplier of influence in the field of dialogue, agenda-setting, and coalition-building for a more peaceful (i.e. attacks) and respectful (i.e. privacy) interactions in cyberspace. Member states' defence capabilities (i.e. cybersecurity intelligence) and legal certainty are needed to counter state-sponsored attacks. The Tallinn Manual 2.0, NATO's analysis of how existing international law applies to cyberspace in day-to-day operations is a good start; it should also include analysis/guidance on the application of the legal framework on armed conflicts to cyberspace. The EU should work with international organisations (e.g. UN, OECD, WTO, OSCE), academia, civil society, and the defence community to achieve these objectives.

In conclusion, the European approach to cybersecurity should pursue a balanced course between security and freedom, guided by common principles rather than fear. Maximum security would require a top-down approach and citizens giving up some online freedoms, while absolute freedom would entail security risks. As recent terrorist and criminal attacks demonstrated, we need a societal debate on what societies we want to live in, and how to preserve the EU values in the cyber domain, considering the differences in values and preferences across the Union.

The initiatives outlined in this paper, alongside other measures in the pipeline, would help the EU to improve its resilience, build capacity, and strengthen the internal and international cooperation on cybersecurity issues. These are needed to improve information and systems' security, tackle cybercrime, counter cyber espionage and attacks on critical infrastructure, and improve citizens' security online. The EU is on the right track, but with digitalisation progressing at full speed and the evolving nature of cyber threats, the EU should embed cybersecurity principles in all relevant policies, such as the (Digital) Single Market (e.g. online platforms, and the data, collaborative, and app economy), education (knowledge, skills, and life-long learning), industry, innovation, investment, as well as in defence cooperation.

Iva Tasheva is Junior Policy Analyst at EPC's Sustainable Prosperity for Europe Programme

This publication was presented at a Conference "Europe: Global Threats and Integrated Security. Security in the Black Sea Region" on 19 May 2017 at the New Bulgarian University, Sofia.

1 European Agenda on Security, available at goo.gl/X8OtcH
2 A Global Strategy for the European Union's Foreign And Security Policy, available at goo.gl/ynHjdQ
3 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at goo.gl/9VndnM
4 Directive 2013/40/EU from 12 August 2013
5 Directive 2016/1148 from 6 July 2016
6 Available at goo.gl/drJKAt
7 Communiqué, G7 Finance Ministers and Central Bank Governors, 13 May 2017, Bari
8 Mid-term review of the 2015 Digital Single Market strategy, available at goo.gl/Ls1LIM
9 Reflection Paper on the Future of European Defence, goo.gl/Nox1WD
10 The Digital Skills and Jobs Coalition, available at goo.gl/Fz3rRX
11 See goo.gl/ng5ADV
12 Building an Effective European Cyber Shield - Taking EU Cooperation to the Next Level, available at goo.gl/gznFTH

European Policy Centre ■ 14-16 rue du Trône, 1000 Brussels, Belgium
Tel: +32 (0)2 231 03 40 ■ Fax: +32 (0)2 231 07 04 ■ Email: info@epc.eu ■ Twitter: @epc_eu ■ Website: www.epc.eu

Europe for Citizens Programme

With the support of the Europe for Citizens Programme of the European Union.