EPSC Strategic Notes

European Commission

Issue 24
8 May 2017

Building an Effective European Cyber Shield

Taking EU Cooperation to the Next Level

European Political Strategy Centre

Breaches of sensitive data, mass disinformation campaigns, cyberespionage and attacks on critical infrastructure – these are no longer futuristic threats, but real events that affect individuals, businesses and governments on a daily basis. Yet they remain largely unprosecuted. Though so far below the threshold of outright war, **cyber aggression is emerging as a major new vector that can be activated to achieve strategic superiority, destabilise states, and cause large-scale economic damage**.

2016 marked a turning point in the offensive use of cyber power. The United States formally accused Russia of sponsoring cyberattacks against the Democratic National Committee with a view to interfering with the US Presidential election, while media reported a 'record year for data breaches'.[1]

In this rapidly evolving context, the European Union and its Member States need to anticipate and plan for hitherto unimaginable scenarios in which they would be put under severe attack. Given the non-territorial nature of cyber threats and their increasingly disruptive effect, it is urgent to build up cyber resilience in each Member State and scale up European cooperation.

Entering a new cyber reality

Cyberattacks are already occurring on a daily basis – in some cases even recognised as state-sponsored. Such aggressions are likely to be used with greater intensity and accuracy in the future, moving ever closer to the sphere of cyber wars that could fall within the remit of Article 5 of the NATO Treaty. In this context, building up Europe's cyber capabilities is a major priority.

Institutional collaboration must be ramped up

The EU's recent Directive on Security of Network and Information Systems[2] paves the way for stronger cooperation on cybersecurity. A swift roll-out of this new framework will be key. But given the intensification of threats, the EU and Member States must already consider practical ways to further enhance competence sharing – one option would be to establish a European Cybersecurity Coordination Platform.

Europe is insufficiently prepared

Citizens, companies, governments and, increasingly, underlying critical infrastructures are all at risk. Yet the scale and rapidly changing nature of digital security risks have not been fully grasped by European society. As a result, forward-looking policies and investments have been lacking. Actions towards updating and retaining skill sets and strengthening the European digital industry will be crucial for the future.

New public policies and partnerships

Cybersecurity must be prioritised in public policies and backed up with appropriate resources. Joint European risk strategies and coordinated political responses against large-scale attacks are urgently needed. New forms of collaboration should be investigated with industry and civil society, as well as with third countries, to close the loopholes in Europe's cyber shield.

EPSC Strategic Notes are analytical papers on topics chosen by the President of the European Commission. They are produced by the European Political Strategy Centre (EPSC), the European Commission's in-house think tank.

New tools, new risks

Although the shift towards a digital world offers huge opportunities, it also comes with new types of risks and threats. As all sectors of our lives increasingly depend on cyber activity, any one of them could be targeted by a cyberattack (Figure 1).

These attacks can be carried out at the micro level, targeting individual citizens and businesses, or – as is increasingly the case – at the macro level, with a view to **destabilising governmental institutions and state security, public policies and entire economies**.

Attacks can stem from various sources, using multiple vectors and taking different forms. New vulnerabilities appear constantly and cyber threats evolve very quickly to take advantage of them. Traditional vectors of attack, such as spam and adware – seen as major threats just a few years ago – are rapidly being replaced by more complex threats. These include sophisticated denial of service attacks or ransomware, i.e. a type of malicious software designed to block access to a computer system to extort or blackmail the victim.

Cyberfighters and cyberterrorists are now active in addition to more 'conventional' cyberspies, while **cybercrime 'as a service'** – cybercriminals selling their services over the dark net – is developing rapidly.[3] As a consequence, the lines between the different types of threats and attackers are increasingly blurred.

At the same time, the spread of the 'Internet of Things' means the vulnerability to cyberattacks now extends beyond digital assets to physical assets, including critical infrastructure, such as household appliances, transport systems and communications networks.[4]

Until recently, cyberespionage was largely confined to the economic domain, used by large corporations – in some cases, with states sponsoring them – to gain unfair advantage over their competitors. The main risks, from a business perspective, pertain to intellectual property infringements, disclosure of trade secrets, and economic espionage. In this particular field, China is still widely perceived to be the main player.[5]

However, **cyberspace is now also increasingly being used for political purposes**.

Figure 1: No critical sector escapes the cyber threat

This figure features only a small selection of incidents that took place in 2016. Many more attacks occur every day all over the world.

November 2016
NHS hospitals
Hospital machines were frozen to demand ransom cash; at least four NHS (National Health Service) funds were attacked

November 2016
Yahoo
Data breach of 1 billion accounts

December 2015 & December 2016
Power grid in Ukraine
230,000 people were left without power for up to 6 hours; first time that a cyber-weapon was successfully used against a nation's power grid

November 2016
Tesco Bank
Around £2.5 million was stolen from around 9,000 customers in this hack, the largest on a UK bank

November 2016
Deutsche Telekom
900,000 (or about 4.5 percent of its 20 million fixed-line customers) suffered Internet outages over two days

October 2016
Australian Red Cross
Personal data of 550,000 blood donators stolen

February 2016
Central bank of Bangladesh
USD 81 million were lost and a further USD 850 million in transactions were prevented from being processed

February 2016
FBI and Homeland Security
Personal details of over 20,000 employees of the Federal Bureau of Investigation and 9,000 of the Department of Homeland Security were accessed

April 2016
Philippines' Commission on Elections (COMELEC)
Personal information of every single voter in the Philippines — approx. 55 million people — was compromised by Anonymous

October 2016
Domain name provider Dyn
A distributed denial of service attack resulted in the break-down of some of the biggest websites in the world including Twitter, The Guardian, Netflix, Reddit, Airbnb and CNN

April 2016
Democratic National Committee
Publication of 20,000 e-mails stolen from the Democratic National Committee

Source: European Political Strategy Centre, based on media reports

Cyberattacks are emerging as a new instrument for both state and non-state actors to pursue specific geostrategic interests. They represent a new 'hybrid threat', i.e. a 'mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner'.[6]

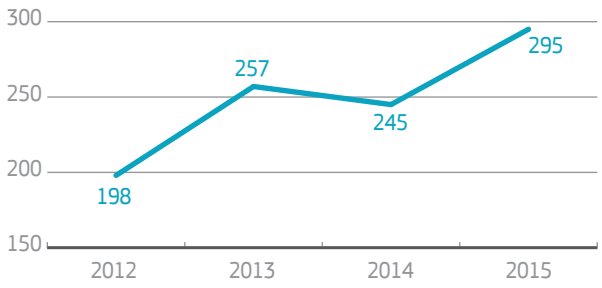
North Korea[7] and Russia[8] are regularly pointed out as the main countries actively sponsoring cyberattacks, with the world's most effective hackers said to be located in Russia.[9] Although Russia has not openly admitted to interference in foreign affairs, there is increasing evidence of the involvement of Russian hackers in many strategic attacks.

In fact, for many countries, as well as non-state actors such as Daesh or al-Qaeda, **cyber tools offer an attractive weapon: cheap, effective, high-impact, difficult to predict, and hard to trace**.[10] In Russia's case, cyber warfare appears to be becoming a fully-fledged component of an aggressive foreign policy – a new 'fifth domain', after land, sea, air and space.[11]

In this context, critical infrastructure is increasingly drawing the attention of politically-driven cyberattackers because of the potential for destabilising or harming large parts of the population.[12] In fact, attacks on critical infrastructure have been rising fast in Europe and in the US (Figure 2).[13]

Figure 2: Attacks on critical infrastructure are on the rise in the US

Number of reported cyber incidents against US critical infrastructure



Source: Department of Homeland Security, 2015

To date, such state-sponsored cyberattacks have mostly been used to test the waters and see how affected governments and organisations would react. The manipulation of the Ukrainian power grid in 2015, for instance, came across as primarily designed to signal and demonstrate an ability to disrupt.[14]

Nonetheless, recent high-profile attacks, such as those against the German Parliament in 2015, against Chancellor Angela Merkel's Christian Democratic Union party in 2016, or against the US Democratic National Committee in 2016, are a clear sign that **politically-motivated cyberattacks are gaining in scale, hostility and sophistication**.

Whether aimed at gathering sensitive information for propaganda and smear campaigns, or at disrupting critical infrastructures, **these attacks perniciously seek to challenge and undermine the very functioning of, and trust in, Western democracies**.

In this context, attacks targeting Western economies' critical infrastructures, including their democratic institutions, are likely to continue in 2017, with growing intensity and accuracy. And, as these infrastructures become increasingly interconnected and interdependent (e.g. with communication networks or oil and gas pipelines spanning across Europe), the risk of incidents evolving and cascading into large-scale events affecting several Member States becomes all the more real.[15]

Tip of the iceberg?

The costs related to cybercrime and data breaches are thought to be significant and growing fast as digitalisation spreads into all spheres of our lives.

A 2014 study estimated the economic impact of cybercrime in the Union to stand at 0.41% of EU GDP (i.e. around 55 billion euro) in 2013; with Germany being the most affected Member State (1.6% of GDP).[16] Europol currently estimates the cost at 265 billion euro per year.[17] And the trend is set to rise. A recent study forecasts that the economic cost of data breaches will quadruple by 2019, to reach 2 trillion euro worldwide.[18]

The most affected sectors are financial services, energy, technology, services, industry and defence.[19] At the level of individual companies, various studies relating to French, German and UK-based enterprises have found the economic impact of cybercrime to range from 100,000 euro per year per affected company to as much as 20 million euro, depending on the type of attack.[20] These figures are likely to increase as more and more economic infrastructures become connected.[21]

One of the main reasons why it is so difficult to estimate the financial cost of cyberattacks is that many companies are guarded about sharing information on the number of attacks they face and the extent of the losses they incur, for fear of reputational damage. This is particularly true for companies whose business models are built around trust in the protection of private data. The LinkedIn and Yahoo breaches illustrated the vulnerability of such companies, as well as the potentially important detrimental impact on image and long-term business perspectives of such attacks.

In light of such considerations, **a significant proportion of incidents and related costs are never reported** to the competent authorities.[22]

Other factors of corporate under-reporting include reluctance of IT management teams to inform senior management; lawyers advising their clients against reporting; or those affected **simply not knowing who to turn to in the event of an attack**.[23]

Under-reporting appears to be particularly prevalent in Europe, where, so far, very few large companies have publicly acknowledged a cyber breach. This is partially due to the fact that, contrary to the US, there is currently no provision at EU level mandating the disclosure of cyberattacks.[24] The entry into force of both the General Data Protection Regulation (GDPR)[25] and the national implementation of the Directive on Security of Network and Information Systems ('NIS' Directive),[26] as of May 2018, will subject certain companies to reporting requirements and should increase public awareness.

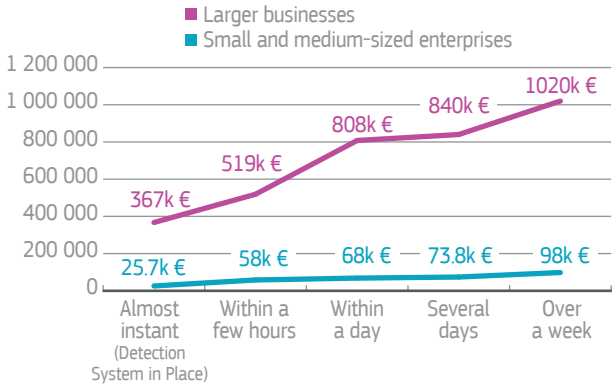
Lack of reporting and information-sharing relating to cyber incidents represents a major hurdle to better understanding and addressing cyber threats and provides scope for new vulnerabilities to spread more widely.

Adapting mindsets

Often enough, under-reporting actually results from an **unawareness of breaches and other intrusions due to a lack of detection capabilities**. Many types of breaches take weeks or months to detect; a fair number may never be detected at all.[27] This is particularly the case in small and medium-sized companies and organisations with low levels of cyber protection. But larger government bodies can also be affected. A recent intrusion into the Czech Foreign Ministry's email servers went on for months before it was discovered.[28]

Figure 3: Financial impact of cyber breaches according to detection time

Average cost to SMEs and to businesses, in thousands of euro

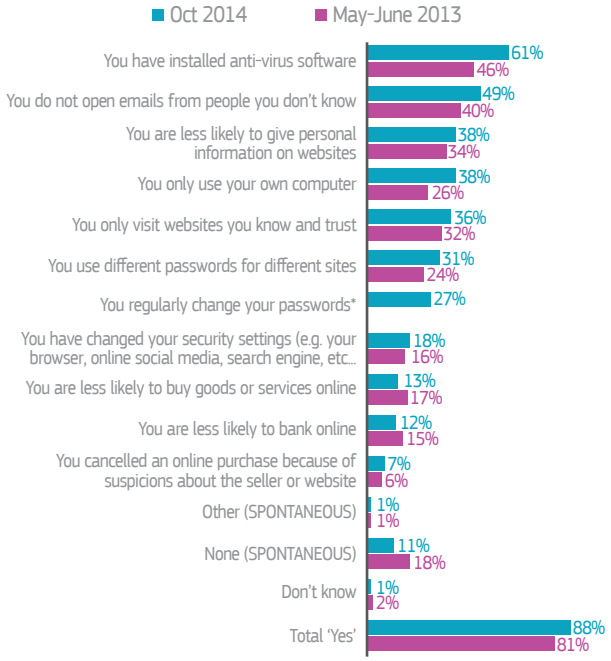


Notes: Survey of 4,000 business representatives from 25 countries.

Source: Kaspersky Lab, '*Measuring Financial Impact of IT Security on Businesses*', 2016

Figure 4: Change in behaviour of Internet users due to security concerns

Responses from Internet users to the question: 'Has concern about security issues made you change the way you use the Internet in any of the following ways?'



* New item

Source: Special Eurobarometer 423 on Cybersecurity, February 2015

In fact, the time lag between cyber intrusions and their detection is estimated to be as much as three times longer in Europe than in the rest of the world.[29] And, according to experts, the financial impact of cyber breaches can increase by as much as a factor of four when undetected for seven days, compared to the cost of it being detected instantly (Figure 3).

Despite this, security is still far from being a first-hand consideration for many Europeans. **Businesses, public organisations, law enforcement authorities, and individuals remain largely unprepared for many of the potential new dangers of the cyber world**. Although 9 out of 10 Europeans are changing the way they use the Internet to address security concerns,[30] many still consider security measures to be more of a burden than an indispensable necessity and only take the most limited action to counter the hazards (Figure 4). A recent business survey also saw 45% of respondents declare themselves 'under-prepared' to handle a targeted cyberattack, while 30% had still not fully implemented anti-malware software, let alone any additional measures.[31]

Yet, new digital technologies are emerging on a daily basis and citizens and organisations often adopt them without due caution. These are frequently designed without security in mind, as evidenced by the widespread hijacking of new, connected 'Internet of Things' devices.

Even where organisations are aware of the potential risks and vulnerabilities linked to the increasing spread of digital technologies, the tools and policies they put in place do not necessarily match the speed and creativity of attackers. In most places, cybersecurity is approached as a 'technical problem calling for technical solutions'.[32] Cybersecurity strategies remain confined to IT departments, with little involvement of senior management. The strategic nature of cybersecurity on organisations' operations and the rapidly changing nature and scale of digital security risks have not yet been fully apprehended.

Similarly, cybersecurity is still not adequately enshrined in public policies, nor is it on the radar of many public administrations. **Many states consider that the situation remains within their 'tolerance threshold' affecting less then 2% of their GDP**.[33] The discrepancy between the gains generated by digital technologies, which are visible on a daily basis, and the potential losses, which are more diffuse and less tangible, results in inertia and a passive acceptance of the risks linked to the growing digitalisation of society.

Skills matter

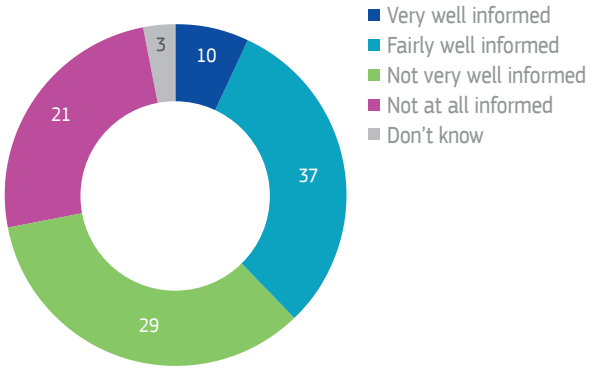
95% of successful hacks are said to be enabled by 'some type of human error' – intentional or not.[34] The fact that there is such a strong human factor at play means that a significant share of cyberattacks could be prevented or countered by means of prudence. In this regard, merely sensitising private users and offering basic training to employees and public officials could have a significant impact. This is true, for instance, of the most common and successful technique used, which is phishing, i.e. the fraudulent practice of sending emails to induce individuals to reveal personal information, such as passwords or credit card numbers.

Today though, **individuals in Europe do not feel sufficiently informed of, or prepared for, cyber threats** (Figure 5). Until they do – and even then – human failure will remain a critical factor, especially as the levels of sophistication of attacks increase. Indeed, lack of digital skills will be one of the major challenges for the future. Demand for highly-skilled ICT staff today far exceeds availability on the labour market. The European private sector is already facing serious shortages in this regard: 41% of EU enterprises that recruited or tried to recruit ICT specialists in 2015 reported difficulties in filling vacancies.[35]

The situation is predicted to get much worse.[36] The public sector, and in particular law enforcement authorities – where specialists are increasingly needed at all levels to ensure sufficient levels of cyber and data protection, and guarantee the independence of our democratic institutions – are especially disadvantaged. European governments will have to find solutions to ensure they are able to hire and retain skilled ICT professionals as they risk drifting off towards better-paid, more competitive private firms.

Figure 5: Level of information among EU citizens regarding the risks of cybercrime

Responses from EU citizens to the question: 'How well informed do you feel about the risks of cybercrime?'



Source: Special Eurobarometer 423 on Cybersecurity, February 2015

Dependence on external technologies

Another key feature of the European cyber landscape is its reliance on externally-developed technologies.[37] Most hardware and software are built outside the EU. Although the largest global suppliers (Microsoft, IBM, CISCO and Symantec) and companies managing large flows of data (Google, Facebook) currently originate from North America, **China is also a rapidly growing player in this domain**.

Aside from having developed a small niche market in the defence sector thanks to specific public procurement restrictions limiting external competition, **the European cyber industry remains fragmented and highly dispersed**. There are no major market players, while as many as 600 small European companies are currently active in providing support to critical infrastructures and public authorities in Europe.

The dominance of the US is partly the result of an impressive cybersecurity investment strategy that saw federal funding raised to 19 billion US dollars in 2017 – a 35% increase compared to 2016.[38] European ambitions in this domain are only just starting to materialise. In July 2016, the European Commission signed an agreement with key cybersecurity market players, represented by the European Cybersecurity Organisation (ESCO), in the hope of triggering 1.8 billion euro of investment in research and innovation by 2020.[39] The EU will itself invest 450 million euro from its research and innovation programme Horizon 2020 in this new contractual public-private partnership, which should become operational in the first half of 2017.

Although the limited European offering is primarily a matter of economic competitiveness, the EU's 2013 Cybersecurity Strategy[40] also underlines an additional aspect, namely the 'risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers'.

Box 1: Where does data protection fit in?

The EU is a global front runner in the field of data protection. To uphold citizens' rights to privacy, the Union has set up a comprehensive regime in the form of the General Data Protection Regulation (GDPR)[41], which sets free flow of data as a principle and protects personal data (i.e. data linked, or linkable, to a specific person) while it is being processed. Controllers and processors of personal data will have the obligation to implement 'appropriate' safeguards to ensure a level of security appropriate to the risk. This may include pseudonymisation and encryption of personal data.[42] They will also be required to disclose any personal data breaches to their supervisory authorities and, in some cases, to those affected by the breaches.

The European Commission also proposed a new Regulation on Privacy and Electronic Communications, in January 2017, reviewing its former 'ePrivacy' Directive.[43] While guaranteeing the free movement of electronic communications data, the proposal aims to ensure 'the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector'.

However, these guarantees become meaningless if personal data can, at any time, be accessed, hacked into and exploited by third parties. Therefore, increasing cybersecurity at all levels – from those who collect data, to those who transmit it, process it, store it, and use it – will be crucial to offering the envisaged level of protection of personal data at European level.

There is, however, a growing tension between ensuring adequately high levels of cybersecurity and personal data protection, and broader security concerns that can lead national authorities to seek bulk access to data or to attempt to bypass encryption in the course of their investigations. These frictions have been reflected in high-profile disputes, such as the one pitting the US Federal Bureau of Investigation (FBI) against Apple.[44] More recently, in December 2016, the European Court of Justice (ECJ) ruled against the UK's Investigatory Powers Act that provides UK security services and police with powers to hack into computers and phones and to collect communications data in bulk, saying it could 'not be considered to be justified within a democratic society'.

These cases reveal a shift in the debate from a focus on privacy to a broader understanding that encryption is also critical for security. **Backdoors created for security investigations can be discovered and misused and this risk has to be carefully weighed against any potential benefits.** With this in mind, the High Level Group of the European Commission's Scientific Advice Mechanism advises against any weakening of encryption and recommends that 'cryptographic standards in the EU reach and remain at state-of-the-art levels'.[45]

Europe's fragmented cybersecurity environment

Building on the European Agenda on Security, adopted in April 2015, the European Commission put forward a new Communication in April 2016 aimed at paving the way towards an effective and genuine Security Union. It sets out a roadmap for achieving a common European approach to security, underscoring that transnational threats cannot be addressed effectively by the Member States individually. '**In the area of security, as in many other areas in Europe, fragmentation is what makes us vulnerable**,' European Commission President Jean-Claude Juncker stressed when presenting the Communication.[46]

Confirming the importance of the security agenda, a new Commissioner's portfolio was created, charged with the delivery of an operational and effective Security Union. Sir Julian King was appointed to this function in September 2016. He is assisted by a cross-cutting Task Force that draws on the expertise of the whole of the European Commission to reflect on future needs and opportunities to improve internal security.

Cybersecurity is an essential component of the Security Union and of the Commissioner's portfolio.[47] The European Directive on Security of Network and Information Systems ('NIS' Directive), adopted in July 2016, and which is to be implemented by Member States by 9 May 2018 is therefore an integral part of the strategy.[48] It aims to bring cybersecurity capabilities to the same level of development in all Member States, to reinforce trust and confidence among them and ensure that information exchange and cooperation are efficient, including at cross-border level. To achieve this, it establishes a **new, multi-level governance structure for European cyber protection** (Figure 6).

Finally, the 2015 Digital Single Market Strategy also aims to make the EU a stronger player in digital technologies, while acknowledging the importance of trust and security in order for digital goods and services to flourish across Europe.

Within this regulatory and policy framework, **four different constituencies** are currently engaged in cybersecurity at European level, respectively covering IT security; law enforcement; intelligence; and diplomacy and defence-related aspects.

1. From the general **IT security perspective**, the frontline actors are the **Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)**[49] that exist both at EU level and at national level to respond to concrete information security incidents and cyber threats. The EU response team (**CERT-EU**) has limited resources (**30 people**) and provides its services to EU institutions only. At national level, the structures of these teams diverge significantly both in form and functioning. Although there is some level of technical cooperation among European CERTs via the European Government CERTs group (EGC group), only 10 Member States are currently represented in this restricted circle, alongside the CERT-EU and respresentatives of Norway and Switzerland. New members are accepted only on application and if deemed to have sufficiently developed capabilities.[50]

   In addition to these operational teams, the EU has established an **Agency for Network and Information Security** (**ENISA**), which acts as a centre of expertise dedicated to enhancing network and information security within the Union. With a **staff of 65**, the Agency's main aim is to raise awareness of cybersecurity issues in the Member States, support the development of European and national cybersecurity strategies and facilitate capacity-building and cooperation.

2. From the **law enforcement** perspective, Europol's **European Cybercrime Centre** (**EC3 – 52 people**) provides important operational support to national authorities in Member States in the fight against cybercrime and has become a key hub of expertise on cybercrime operations, e.g. facilitating international information exchange, and providing cyberintelligence, forensic analysis, legal assistance and specialist support.

   In the four years since its creation in 2013, the European Cybercrime Centre has helped to dismantle numerous cybercrime operations, from financial fraudsters to child sexual exploitation networks. In November 2016, it contributed to taking down the major international criminal infrastructure platform 'Avalanche', responsible for mass global malware attacks, operating as many as 500,000 infected computers in over 180 countries, and thought to have caused hundreds of millions of euro in damages worldwide – of which 6 million euro in concentrated cyberattacks on online banking systems in Germany alone.[51] In this regard, the European Cybercrime Centre is, however, a victim of its own success. Given the importance and recognition it has gained, it would need to see its resources significantly reinforced.

3. **Intelligence services** mostly operate at the national level, although there is cooperation at European level. The main connection point to the European institutions is the **Intelligence Centre** (**INTCEN – 3 people**), located in the European External Action Service (EEAS).

4. Finally, the **diplomacy and defence**-related services consist of a team of **3 people** in the **European External Action Service** that focuses on diplomatic responses to coercive cyber operations and capability-building in third countries, as well as a team of **3 people** in the **European Defence Agency** (**EDA**) that supports cyber defence capability development in Member States and greater cooperation in this field. In addition, the **EU Military Staff** (**3 people**), also in the European External Action Service, brings cyber expertise to military strategic planning of Common Security and Defence Policy (CSDP) operations and missions.

Not only are resources limited but interactions between these different constituencies continue to prove difficult for institutional, technical, legal, budgetary and cultural reasons. In addition, the existence of different regulations and approaches towards cybersecurity and the heterogeneity in the levels of maturity of cybersecurity in Member States present a further hurdle to effective collaboration – as is, for instance, evidenced by the limited number of Member States participating in the European Government CERTs group.

The predominance of silos is a major limitation in the fight against sophisticated cyberattacks. For example, while IT response teams faced with an attack will focus primarily on the compromised systems themselves – and only on those in their geographical remit – in many cases, the involvement of police or law enforcement services, or of IT response teams from other Member States would help to solve the incident.

Towards a cybersecure Europe

From technical to political cooperation

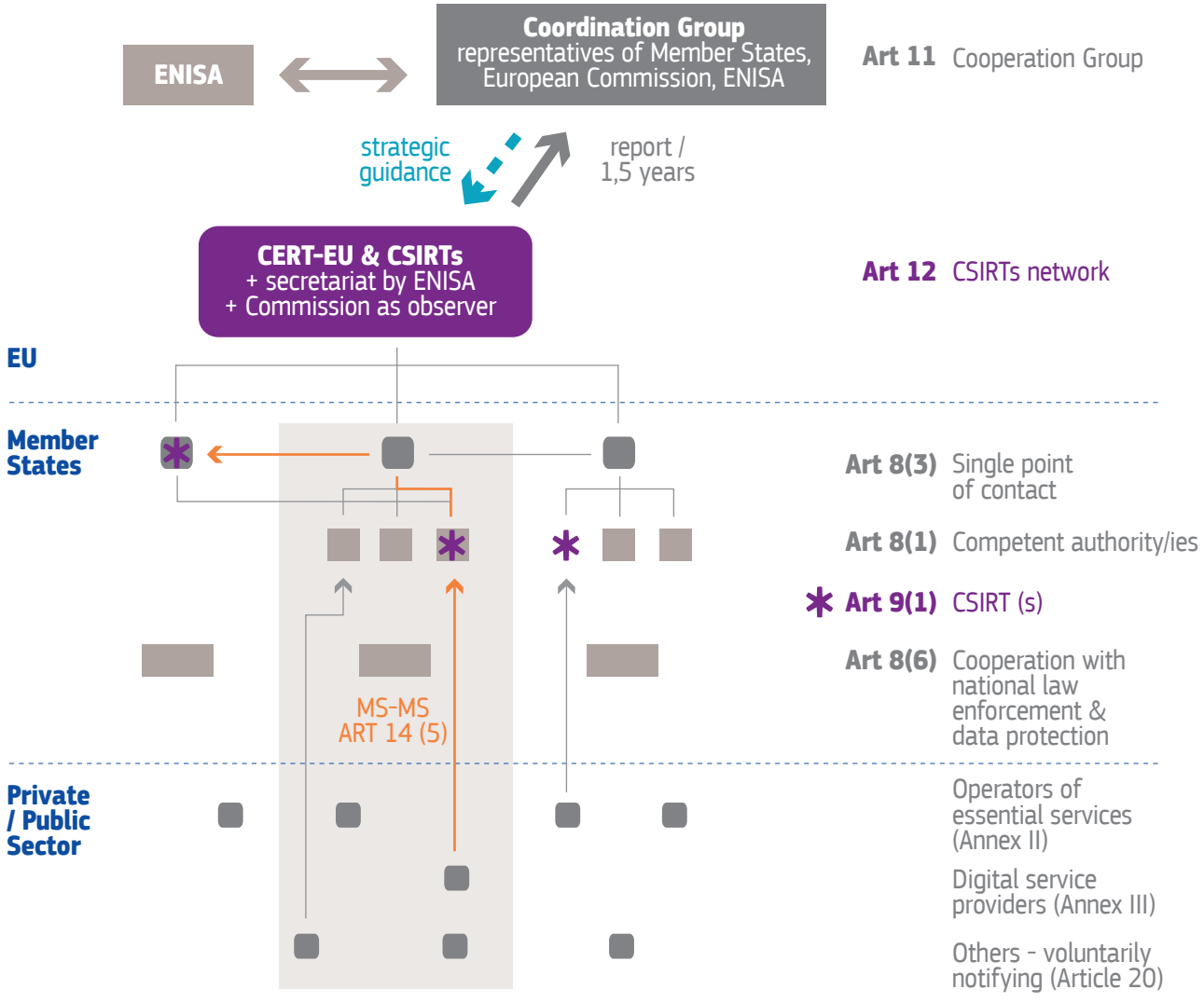
The Directive on Security of Network and Information Systems (NIS Directive) **represents a first key step towards strengthening trust and cooperation between countries and constituencies**. It seeks to upgrade national cybersecurity capabilities with a view to creating a more level playing field, for instance by requiring that all Member States designate national response teams (CSIRTs) and equip them with 'adequate' resources to carry out their tasks and responsibilities effectively.

It seeks to reinforce technical cooperation across borders via a novel 'CSIRT network', while a 'Cooperation Group', composed of representatives of Member States, the European Commission and the Agency for Network and Information Security (ENISA), is also established to facilitate strategic cooperation and exchange of best practices (Figure 6).[52]

Because the cooperation network set up by the Directive on Security of Network and Information Systems (NIS Directive) is still very new, the immediate focus should be on **accelerating the roll-out of this novel framework and fully exploiting all possibilities for effective collaboration.** However, given the rapid acceleration and intensification of cyber threats in the short time since the Directive was adopted, ongoing work to improve the cyber resilience of Member States should also be scaled up at a similar pace and with appropriate resources. **It should therefore be assessed whether a system based on loose cooperation of national authorities and mostly voluntary exchanges will suffice to make the EU cybersecure**.

Beyond creating a network of capable national structures and boosting technical cooperation across borders, there is a need to further develop political cooperation among Member States and to build up capabilities at European level. EU tools and responses should complete and broaden national capabilities in responding to cyber threats – especially those sponsored by states – so as to maximise the deterrent effect.

Figure 6: Directive on Security of Network and Information Systems foresees new cooperation structure on cyber



Source: European Political Strategy Centre

Towards a European Cyber Coordination Platform

Recognising that the European cyber environment is evolving fast, the European Commission plans to publish a proposal for a 'cooperation blueprint',[53] encouraging Member States 'to make the most' of the collaboration mechanisms foreseen in the Directive on Security of Network and Information Systems (NIS Directive) in order to be in a position to handle large-scale cyber incidents on an EU level.[54] The hope is that this might facilitate and accelerate a more systematic sharing of information between national response teams (CSIRTs).[55]

The creation of a **European Cybersecurity Coordination Platform** could give a greater impulse to these efforts. Such a platform could take on different forms. One option would be to mirror the position of the European Counterterrorism Coordinator – by creating a **European Cybersecurity Coordinator**. This person could report to the Council, similarly to the European Counterterrorism Coordinator. Alternatively, **given the nature of the competences that need to be coordinated**, **there is clearly scope for such a Coordinator to be placed under the authority of the European Commission**, or at the very least, to work in close consultation with the Commissioner for the Security Union. Indeed, the portfolio would involve not only defence and diplomacy-related policies, but also shared competences such as security and justice or the internal market, and would involve technical, digital, and research aspects, as well as ensuring the protection of EU institutions and agencies. In any case, the function would have to draw on existing in-house skills and resources – in particular those of the EU's Computer Emergency Response Team (CERT-EU) and the Agency for Network and Information Security (ENISA).

Box 2: Vision of stronger cooperation is backed up by EU legal framework

Member States are traditionally reluctant to share competences on matters relating to security and the European regulatory framework is not necessarily conducive to stronger cross-border cooperation. Article 4(2) of the Treaty of the European Union, in particular, notes that the EU shall respect 'essential State functions, including [...] maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State'.

However, this clause need not be an insurmountable barrier. Indeed, Article 4(2) TEU refers only to 'national security'. In this regard, **the abolition of internal borders between Member States and the establishment of the area of freedom, security and justice are strong arguments in favour of measures relating to safeguarding 'Schengen security'**, defined by the cross-border effects of internal security. These arguments are in particular supported by Article 4(2)(j) of the Treaty on the Functioning of the European Union (TFEU), which lists the area of freedom, security and justice as a 'shared competence between the Union and the Member States'.

This is precisely the logic of the Security Union, proposed by President Juncker in March 2016, which is based on the assumption that freedom and security are two sides of the same coin and that the EU and its Member States must act jointly to uphold them (see EPSC Strategic Note: '*Towards a 'Security Union*'). Cooperation will make Europe stronger: whereas national security remains firmly the responsibility of each Member State, threats to safety and wellbeing are transnational and multifaceted. No Member State, even the biggest or the most powerful, can face them alone.

In fact, the EU has already acted in the field of cybersecurity based on the competences enshrined in the Treaties. Once when adopting the Directive on Security of Network and Information Systems (NIS Directive), using the legal basis for the internal market (Article 114 TFEU), and again when adopting the Directive on attacks against information systems,[56] using the legal basis to establish minimum rules on the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension (Article 83(1) TFEU).

With regard to possible further coordination at European level, a more general legal basis is provided for in Article 74 TFEU, which calls for the adoption of 'measures to ensure administrative cooperation between the relevant departments of the Member States'.

As with all EU legislative initiatives, legislation based on this provision would have to carefully follow the limitations set by the principles of **subsidiarity and proportionality** (Article 5 TEU). In this context, it is interesting to note that the European legislator acknowledged that the Directive on Security of Network and Information Systems (NIS Directive) complies with the principle of subsidiarity. This in justified by the cross-border nature of European network and information systems, and the interdependencies among them, which make deeper cross-border cooperation, based on a level playing field, indispensable. In this sense, there is still margin to manoeuvre for future European legislation.

Yet, to be effective, such a coordination function would probably merit a stronger structure. With this in mind, **the ongoing review of the ENISA mandate**, for which a public consultation was launched in January 2017,[57] **presents a clear window of opportunity** that could be seized in light of the new challenges faced by the EU in the cybersecurity field. **ENISA could be transformed into a fully-fledged European Cybersecurity Coordination Platform**, equipped with adequate resources and executive competences to guarantee the speed, accuracy, efficiency and effectiveness of European cyber responses.

ENISA currently works under a *safety* mandate, not a *security* one, and the review could provide an impetus to enlarge the Agency's competences in the future. Developing a coordination function on the basis of such a revised mandate would also require an extensive and thorough review of ENISA's governance structure and competences if it were to be in a position to undertake this function effectively.

While various options are available, **Member States and EU institutions will have to decide together where, how and to which extent they are willing to set up further cooperation**. Since the cyber domain is so closely linked to national security, this must be a joint decision – just as it will have to be followed by joint efforts and joint resources so that both greater vertical (with Member States) and horizontal cooperation (across EU institutions, entities and Directorate-Generals) can be achieved.

Responsibilities of a European Cybersecurity Coordination Platform could, for instance, include improving capabilities in the following areas:

a. **Detection**: acting as a focal point for the collection and oversight of relevant information and data channelled by EU entities or Member States. Data would still be collected by different authorities but brought together under the authority of a European Cybersecurity Coordination Platform so as to better **connect the dots**. In this context, interoperability through taxonomy and a joint sharing mechanism would be of high importance.[58] In fact, this would already be useful now to facilitate information sharing between law enforcement authorities and the European CSIRT community.

b. **Prevention**: providing strategic **risk assessments** of cyber threats on the basis of gathered information and data analytics; developing European **deterrence and counter-strategies**; monitoring the implementation of current and future European legislation at Member State level; mapping and monitoring the development of national cybersecurity capabilities, including against **benchmarks** such as the percentage of the GDP spent on cybersecurity; conducting **stress-tests and friendly hacking exercises** to assess the cyber resilience of critical infrastructures, raising the awareness of administrative staff at EU and Member State levels (e.g. by means of compulsory training); and promoting education and training would all be part of the strategy.

c. **Cooperation**: facilitating synergies between internal and external security by working closely with the Council (especially the European Counter-Terrorism Coordinator), the European External Action Service (especially the Intelligence Centre INCENT), the European Defence Agency on defence capability-building (training and exercise, and research) and with NATO (building on the technical agreement signed between EU-CERT and NATO in February 2016). In this context, any European Cybersecurity Coordination Platform should also be able to rely on a **military EU cyber command**, potentially hosted by the EU Military Staff in the European External Action Service. Such a command function would facilitate interactions with defence ministries, help to set up and protect secured networks and assets deployed in the framework of EU-led military and civilian operations, and enable, through close coordination with NATO, the development of doctrine and close inclusion of cyber defence in national defence planning. In parallel, centralised coordination could also be facilitated through the deployment of a **highly-secured network among relevant EU institutions**, allowing for plug-ins with national secured communication systems for the exchange of classified information.

d. **Protection**: providing robust support to EU institutions, including EU delegations; and establishing a framework for greater cooperation among Member States to enable coordinated responses to large-scale EU cyberattacks that remain under the threshold of Article 5 of the Washington Treaty. Although an EU protocol for countering hybrid threats was agreed in July 2016,[59] outlining specific steps to be followed (including coordination with the Council via the 'Integrated Policy Crisis Response'[60] and NATO), there is still a need to develop a **shared protocol in case of large-scale cyber incidents**. This could build on the diplomatic cyber toolbox developed by the European External Action Service, which includes a variety of responses and instruments to be activated depending on the severity of the attack; ranging from official statements to sanctions. This protocol should also foresee the possibility to pool resources and skills at European level to provide assistance to overwhelmed Member States or groups of Member States, or in cases of attacks against critical European infrastructures. The roles and responsibilities of respective bodies should be identified and tested as part of this protocol. Such a European mechanism could possibly build on the legal framework of Article 222 TFEU ('Solidarity clause').[61] It is also worth noting that enhancing protective measures would ultimately have a deterrent effect and therefore increase cyber resilience.

e. **Prosecution**: Although this should remain within the remit of the Member States and Europol, a European Cybersecurity Coordination Platform could contribute to 'spanning the lifecycle of an incident from prevention to prosecution'.[62] Europol's European Cybercrime Centre (EC3) – representing the law enforcement side – already engages in an exchange with CSIRTs and ENISA via joint conferences and advisory groups. In implementing the Directive on Security of Network and Information Systems (NIS Directive), cooperation will also be needed on a national level, as national authorities in the CSIRT community 'shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities'.[63]

Box 3: Increasing Euro-Atlantic resilience through closer EU-NATO cyber cooperation

Cyber defence is a priority in EU-NATO cooperation. In their joint declaration of July 2016, European Commission President Juncker, European Council President Tusk and NATO Secretary-General Stoltenberg agreed to 'expand their cooperation on cybersecurity and defence, also in the context of EU and NATO missions and operations, exercises, education and training'.

Cyber defence has been established as a core task of collective defence since the NATO Wales Summit in September 2014, where – driven by the recurrent use of cyberattacks – the international community recognised cyber as a domain of military operation, along with air, land and sea, meaning that **Article 5 of the Washington Treaty could potentially be invoked following a cyberattack as part of the offensive actions of Member States**.

Against this backdrop, NATO has developed a cyber defence policy, which is now included in the NATO defence planning process, to enhance cyber defence of national networks and infrastructures; develop the NATO cyber defence capability to protect NATO's own network and operations; and closely partner with industry. To this end, NATO has 100 members of staff dedicated to protecting NATO-owned infrastructures and networks.

On the EU side, the main objectives are to develop cyber defence capabilities of Member States, including through research and technology, reinforce the protection of communication networks for Common Security and Defence Policy (CSDP) structures, missions and operations; and raise awareness through training and exercises.

Greater cooperation in the field of cybersecurity, namely in the form of information exchange and operational cooperation, should ultimately be a cornerstone of ongoing efforts to increase resilience in both organisations.

Securing the value chain, closing the loopholes

Making Europe cybersecure requires the involvement of all actors in the growing digital community. Many essential services are nowadays operated by private companies or public-private partnerships rather than public authorities. Civil society and private citizens are also becoming key players in a world that is increasingly dominated by the 'Internet of Things'. Against this backdrop, the EU and its Member States must develop public policies that take into account the different actors of the cyber landscape at all levels.

a. **Raising security levels and boosting competitiveness through standardisation and certification**: Governments, businesses and consumers increasingly rely on electronic devices in their everyday activities. Yet, the 'Internet of Things' currently pays scant attention to security and data protection aspects. Developing an EU-wide certification system, based on minimum thresholds and mutual recognition of national certificates and labelling systems, would allow public and private actors alike to make a conscious choice in favour of increased digital security – whether purchasing a connected car, an intelligent fridge, a smart meter or a router, and regardless of where these products are made. This could provide a strong competitive advantage to European products proven to be cybersecure. It would also ultimately facilitate cross-sectorial business endeavours between sectors that are traditionally more cybersecure (e.g. finance) and those where cybersecurity has typically been less of an issue (e.g. transport). Any EU-wide certification system should encourage **cybersecurity by design** in industrial processes and should cover even the most critical hardware and software, such as aircraft technologies. Steps are already being taken in this direction[64] and the European Commission intends to present a proposal for a 'European ICT security certification framework' by the end of 2017.[65] This represents a real **opportunity to shape global standards relating to digital safety and security**. Such standards will be needed in order to fully exploit the economic benefits of the digital age.[66] It is, however, questionable whether the EU can achieve such influence through the voluntary and loose approach that is currently applied (cf. Article 19 of the Directive on Security of Network and Information Systems or 'NIS Directive').

b. **Strengthening the European cyber industry and moving towards digital autonomy in strategic areas**: In addition to developing certification and setting minimum security standards, the protection of Europe's strategic interests requires a certain degree of industrial autonomy in critical hardware, software and services. Having trusted tools, as well as the right skills at hand to fend off cyber threats is a key element of any cybersecurity strategy. This means strengthening the European cybersecurity industry (covering hardware, software and services) and enabling the development of European supply chains, as well as expanding skill sets through education, training and certification. This should be accompanied by policies aimed at ensuring security of supply of critical components and addressing the question of the foreign acquisition of strategic cybersecurity assets.

Ongoing initiatives such as the European Cloud Initiative, aimed at providing a European, world-class, online infrastructure to securely store and manage data, or the establishment of the public-private partnership (PPP) between the European Commission and the European Cybersecurity Organisation (ECSO) to boost investments in cyber research and innovation, present a good start. Building on this, consideration could be given to establishing a **cybersecurity Joint Undertaking under the next Multiannual Financial Framework** to help defragment markets and supply chains, enhance collaboration at European level and stimulate scientific excellence and innovation in the cyber domain. In the shorter term, other forms of incentives could be used to dynamise European market players and speed up the development of new skills, such as the organisation of challenges, competitions, hackathons and prizes.

Box 4: Safe cyber infrastructure – a pipe dream?

The spokesperson of an influential hackers club once compared the world's digital infrastructure to a poorly maintained system of water pipes in a developing country megalopolis. Leaks can be found in every nook and corner; technicians try to plug the holes 24/7 – but all they have is duct tape.[67]

What is often lost on the end users of the Internet is the nature of the network itself – a complex infrastructure that includes physical elements (from the 'traditional' infrastructure, such as cabling and power supply, to the hardware servers and devices), but also the software that runs the hardware; the services provided (e.g. routing); the protocols setting the rules of the game; as well as human resources – from administrators to end users.

It is widely acknowledged that **the factors that made the Internet a success in its early days – the loose governance and bias towards technologies that facilitated quick adoption rather than security – are what laid the ground for critical vulnerabilities in later years**. Some core features of the Internet included unfortunate compromises, e.g. the omission of encryption in the basic communication language of the Internet (the Transmission Control Protocol/Internet Protocol or TCP/IP), partly due the poor performance of early computers.[68] Others were introduced as temporary, imperfect fixes but are yet to be replaced, e.g. the Border Gateway Protocol (BGP) routing protocol created in 1989.[69]

The lukewarm attitude to security of many software producers (most notably in the 1990s and 2000s) did not help either. For a long time, the market pushed developers to put quick feature development ahead of security concerns. The term 'patch-and-pray' (a play on 'plug-and-play') describes well the dominant attitude of these times. Perhaps ironically, instead of governments leading the way on security, it seems to have been revelations of mass government surveillance that may have tipped the balance. Encryption became widespread around 2013, made visible by the 'https://' prefix users now see when visiting most major websites.

There are two distinct approaches to fixing the Internet's underlying infrastructure:[70] A '**clean-slate' approach**, according to which existing networks should be completely redesigned, using revolutionary models, such as decentralised, resilient peer-to-peer networks, inspired by technologies such as BitTorrent or the blockchain,[71] or a more **evolutionary approach**, building on the existing Internet infrastructure to find safe solutions that provide comprehensive fixes rather than temporary patches. The two approaches do not necessarily have to be at odds with each other and the EU should continue and scale up investments in research in both directions.

In addition, Europe should support a drive towards higher standards of due care with regard to the Internet – as it has done in many other fields, from the authorisation of vehicles and transport, food safety or environmental protection – the Internet has carelessly been left in a security limbo despite the fact that it has become the very foundation of most of people's lives and livelihoods.

c. **Bridging the gap between industry and public entities for a more proactive detection of threats**: To best anticipate and respond to potential cyberattacks, a multidisciplinary, cross-sector approach based on consistent information sharing is required. The challenge is to detect cyberthreats early on; to isolate them in the system under attack; and to best understand their nature and potential impacts before reacting. For this, the involvement of industry is a prerequisite. This is particularly true as regards critical infrastructures.

   To this end, the EU should accelerate the establishment of **'ISACs'** or **'Information Sharing and Analysis Centres for critical infrastructures'**. First launched at the end of the 1990s at the request of the US federal government, ISACs are sectorial member-driven organisations set up to collect, analyse and disseminate information on cyberthreats to help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats. The objective is neither to regulate nor to control the information, but to organise a structured dialogue among key actors in the sector. Today, there are 24 such organisations in the US, covering sectors such as automotive, aviation, IT, communications, electricity, gas, financial services, healthcare and real estate. These sector-based organisations collaborate and coordinate with each other within a National Council of ISACs – a cross-sector partnership, providing a forum for sharing cyber and physical threats and mitigation strategies among ISACs themselves, but also with government and private sector partners.[72] In the EU, similar initiatives are also emerging. Information-sharing networks covering critical infrastructures in energy and finance have been created, while others are being considered in the field of transport.[73] And the demand for such member-driven networks is increasing. Following the cyberattacks against the UK's Tesco bank in November 2016, the European Banking Federation called on the European Commission to facilitate the establishment of a cross-border information hub within the banking industry to combat the threat of cyberattacks.[74] Going forward, the primary focus should be on those sectors identified in the Directive on Security of Network and Information Systems (NIS Directive), e.g. **energy, transport, banking, health, finance**, but also on other critical sectors, such as **defence and telecoms**.

d. **Opening up a channel for reporting small-scale cyber incidents affecting civil society, small businesses and individuals**: Reporting of even the smallest incidents should be facilitated in order to build up sufficient awareness of the cybersecurity landscape in Europe and of the emergence of new vulnerabilities and threats. Protocols to support victims of cyberattacks should also be established. A European Cybersecurity Coordination Platform could guide Member States in establishing **national helpdesks** and developing such **protocols**. Incidents could then be reported back centrally, on a regular basis, to the European Cybersecurity Coordination Platform.

Box 5: What is a critical infrastructure?

The way in which critical infrastructure is defined can have an impact on the breadth of the cybersecurity measures that states put in place to defend themselves against attacks.

In a world of rapidly evolving cyberthreats, this concept must be understood in a dynamic and broad manner. Critical infrastructure will increasingly extend to the tools and mechanisms underpinning our democratic systems and everyday life, as state-sponsored interference in political matters and national elections grows.

The US Department of Homeland Security already defines critical infrastructure as 'the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof'.[75]

The EU's Directive on Security of Network and Information Systems (NIS Directive) also **recognises the critical role of operators of essential services**[76] and therefore sets up obligations for them to take certain preventive security measures and, under certain circumstances, to notify incidents that have an adverse effect on the security of their networks and information systems to their national authorities.[77]

The international dimension of cybersecurity

Digital security will always be a global issue and Europe cannot be a digital fortress. Making Europe more resilient through internal capacity-building will be of the essence, but **the EU must also contribute to the building an international framework on cyberspace that helps to strengthen trust among all stakeholders**.

An important shift in the global governance of the Internet already took place in October 2016, when the US handed over control of the domain naming system to the non-profit Internet Corporation for Assigned Names and Numbers (ICANN).[78] This organisation is now accountable to a global multi-stakeholder community, whose members include private sector representatives, technical experts, academics, civil society, governments and individual Internet end users. The move seeks to ensure that the Internet will be accountable to the people, businesses and organisations that use it worldwide, marking a shift towards a shared governance that should reinforce confidence in the openness and neutrality of the Internet. Governments will be a voice at the table – but not the only one. And not a controlling one, amid fears that more interventionist governments, such as China or Russia, would have attempted to interfere in online content management had the governance been handed over to an inter-governmental organisation such as the United Nations.[79]

With regard to cybersecurity more specifically, the United Nations had already set up a Group of Governmental Experts in 2004 with the aim of examining 'existing and potential threats from the cybersphere and possible cooperative measures to address them'.[80] The Ministerial Council of the Organisation for Security Cooperation in Europe (OSCE) also approved an initial set of confidence-building measures for cyberspace in December 2013,[81] and additional measures were put forward in March 2016.[82]

Yet, there remains a gap between the level of maturity of cyber threats and that of worldwide norms and definitions in the cyber context (e.g. what is an 'attack' in cyberspace?).

It will be indispensable to establish an agreed international regime, underpinned by **three principles**:[83] (i) **applicability of international law to cyberspace, just as to land, air or sea**; (ii) agreement of **norms concerning acceptable behaviour of states in times of peace**, voluntarily adhered to by states (e.g. no deliberate action against critical infrastructures); and (iii) **confidence-building measures** to build trust, reduce risks and increase transparency.

On all these questions, Europe's internal cyber set-up – as well as its ultimate resilience to cyberattacks – will define its credibility and weight in the global arena.

Conclusions

The past two years have seen a clear demonstration of the potentially disruptive effects of cyberattacks on all critical sectors. Loose coordination and soft policies are a first step but will clearly be insufficient to face new, complex and cross-border threats. Cybersecurity needs to become a political priority. **Anticipating and planning for the worst should drive the next steps at European level**. Robust policies on cybersecurity and the development of European capabilities, underpinned by significant EU funding, should form the basis of a European cyber shield to defend EU institutions, Member States, businesses and citizens.

Notes and References

1. Kharif, O., '*2016 Was a Record Year for Data Breaches*', Bloomberg Technology, 19 January 2017.
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19 July 2016, p. 1–30.
3. European Union Agency for Network and Information Security (ENISA), '*Threat Landscape 2015*', January 2016.
4. Beshar, P. J. and Cole, T., '*Cyber Risk: A Perfect Storm Approaching Europe?*', 27 January 2017.
5. Stout, K. L., '*Cyber warfare: Who is China hacking now?*', CNN online, 29 September 2016; Gertz, B., '*China cyber espionage continues*', The Washington Times online, 28 September 2016; Gady, F. Z., '*Top US Spy Chief: China Still Successful in Cyber Espionage Against US*', The Diplomat online, 16 February 2016.
6. European Commission, '*Fact Sheet: FAQ: Joint Framework on countering hybrid threats*', 6 April 2016.
7. Kim, J., '*North Korea mounts long-running hack of South Korea computers, says Seoul*', Reuters Technology News, 13 June 2016.
8. Bennett, C., '*Kremlin's ties to Russian cyber gangs sow US concerns*', The Hill, 10 November 2015.
9. Ibid.
10. Lipton, E., Sanger, D. E., Shane, S., '*The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*', The New York Times online, 13 December 2016.
11. Foxall, A., '*Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*', Russia Studies Centre, Policy Paper No. 9, May 2016.
12. Figures relating to attacks against critical infrastructures in the EU are not widely available. According to the European Union Agency for Network and Information Security (ENISA), '*Stocktaking, Analysis and Recommendations on the Protection of CIIs*', January 2016, only a minority of EU countries has implemented mandatory incident reporting across sectors. In its report on '*Communication network dependencies for ICS/SCADA Systems*' of December 2016, ENISA nonetheless finds that the number of cyber incidents targeting Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Systems has 'increased dramatically in recent years', namely 'due to their increased intercommunication and their exposure to private and public networks'.
13. As published in Business Insider, '*Cyber attacks against our critical infrastructure are likely to increase*', 26 May 2016.
14. Conference organised by Carnegie Europe and Microsoft on 15 December 2016, on key transatlantic challenges in cyberspace. Franck J. Cilluffo is an associate vice-president and director of the Centre for Cyber and Homeland Security at the George Washington University.
15. European Union Agency for Network and Information Security (ENISA), '*Communication network dependencies for ICS/SCADA Systems*', December 2016.
16. McAfee & Center for Strategic and International Studies, '*Net Losses: Estimating the Global Cost of Cybercrime*', 2014, p 9.
17. Europol, European Cybercrime Centre, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime.
18. Juniper Research, Press Release: '*Cybercrime will cost businesses over $2 trillion by 2019*', 12 May 2015.
19. Ponemon Institute, '*2015 Cost of Cyber Crime Study: Global*', October 2015.
20. European Union Agency for Network and Information Security (ENISA), '*The cost of incidents affecting CIIs*', August 2016.
21. Juniper Research, op. cit. 2015.
22. Von Friederike, K., '*Mehr Transparenz!*', Süddeutsche Zeitung, 7 December 2016.
23. UK National Crime Agency: '*Cyber Crime Assessment 2016*', 7 July 2016.
24. Beshar, P. J., '*How Companies Should Prepare For Europe's New Cybersecurity Rules*', Fortune Insiders, 3 August, 2016.
25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016/L 119/1.
26. Directive (EU) 2016/1148.
27. Verizon, '*Data Breach Digest*', 2016.
28. Associated Press, '*Czech foreign minister: ministry email hack took months*', 2 February 2017.
29. FireEye, Marsh & McLennan, '*2017: Cyber-Threats: A perfect storm about to hit Europe?*', January 2017.
30. European Commission, '*Special Eurobarometer 423: Cyber Security*', p. 41, Fieldwork: October 2014, Published: February 2015.
31. These figures are from a survey of 1,300 senior professionals, from small business to enterprise level, conducted by B2B International, in 11 countries, covering both developed markets, including the UK, USA and Japan and developing markets, including Brazil, China and India. See: Kapersky Lab, '*Ready or not? Balancing future opportunities with future risks. A global survey into attitudes and opinions on IT security*', 2015.
32. Organisation for Economic Cooperation and Development (OECD), '*Key issues for digital transformation in the G20*', Report prepared for a joint G20 German Presidency/OECD conference, January 2017, p 93.
33. According to the European Union Agency for Network and Information Security (ENISA), countries will tolerate malicious activity as long as it stays at 'acceptable' levels, i.e. less than 2% of GDP – which is currently the case in Europe, with only Germany seemingly nearing this 2% threshold. For more details, see: European Union Agency for Network and Information Security (ENISA), '*The Cost of incidents affecting critical information infrastructures*', August 2016.
34. IBM, '*The Cyber Security Intelligence Index*', 2014, referred to in Securitymagazine.com, '*95% of Successful Security Attacks are the Result of Human Error*', 19 June 2014.
35. European Commission, Eurostat, '*ICT specialists - statistics on hard-to-fill vacancies in enterprises*', November 2016.
36. OECD, op. cit., 2017, p 106.
37. European Cyber Security Organisation, '*European Cybersecurity Industry Proposal for a Contractual PPP*', June 2016.
38. The White House, Office of the Press Secretary: '*Fact Sheet: Cybersecurity National Action Plan*', 9 February 2016.
39. European Commission, Press Release: '*Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*', 5 July 2016.
40. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016/L 119/1.

41. European Commission and High Representative of the European Union for Foreign Affairs and Security Policy / Vice-President of the Commission, '*Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*', JOIN(2013) 1 final, 7 February 2013.
42. Article 32 of Regulation (EU) 2016/679.
43. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, published on 10 January 2017.
44. Barrett, B., '*The Apple-FBI Battle is over but the new crypto wars have just begun*', in Wired, 30 March 2016.
45. European Commission, Scientific Advice Mechanism, '*Cybersecurity in the European Digital Single Market*', High Level Group of Scientific Advisors, Scientific Opinion No. 2/2017, 24 March 2017.
46. European Commission: '*President Juncker: 'Europe needs a genuine security union''*, Announcement AC/16/2142, 13 April 2016. For more information on the Security Union, see the Strategic Note of the European Political Strategy Centre '*Towards a 'Security Union' - Bolstering the EU's Counter-Terrorism Response*', Issue 12, 20 April 2016.
47. Commissioner King's mission letter tasks him with supporting the fight 'against cybercrime through enhanced cybersecurity and digital intelligence'. Furthermore, the Task Force's fourth progress report from 25 January 2017 focuses on four key areas, amongst which cyberthreats.
48. Directive (EU) 2016/1148.
49. The terms CERT and CSIRT are used interchangeably.
50. The group currently consists of 14 members, including CERT-EU, as well as the CERT representatives of Austria, Belgium, Denmark, Finland, France, Germany, the Netherlands, Norway, Spain, Sweden, Switzerland and the United Kingdom. See: http://www.egc-group.org/.
51. Europol : '*"Avalanche" Network Dismantled in International Cyber Operation*', Press Release, 1 December 2016.
52. The first meeting of the NIS Cooperation Group will take place in February 2017, see: European Commission, '*Communication to the European Parliament, the European Council and the Council: Fourth progress report towards an effective and genuine Security Union*', COM(2017)41 final, 25 January 2017.
53. Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410, p 4.
54. Ibid.
55. Article 14(5) of the NIS Directive.
56. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.
57. European Commission, Public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA), open from 18 January 2017 to 12 April 2017.
58. 'While a taxonomy is a way of describing information through classification, a sharing mechanism structures the way the information is encoded'. For further information, see: ENISA, '*Information sharing and common taxonomies between CSIRTs and Law Enforcement*', December 2015, p 35.
59. Council of the European Union, Joint Staff Working Document, '*EU operational protocol for countering hybrid threats "EU Playbook"*', 7 July 2016.
60. Council of the European Union, '*The EU integrated political crisis response - IPCR – arrangements in brief*', November 2016.
61. For further detail, see the Strategic Note by the European Political Strategy Centre: '*From Mutual Assistance to Collective Security*', Issue 10, 22 December 2015.
62. Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410, p 3.
63. Article 8(6) NIS Directive.
64. For a summary of ongoing activities, see: ENISA, Cybersecurity standards and certification, https://www.enisa.europa.eu/topics/standards
65. Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410, p 10.
66. OECD, op. cit., 2017, pp. 71 et seqq.
67. Rieger, F., '*Jeder ist angreifbar*', in: Der Spiegel, 39/2015, pp 68 et seq.
68. Timberg, C., '*Net of Insecurity, A Flaw in the Design*', in The Washington Post, 30 May 2015.
69. Timberg, C., '*Net of Insecurity, The Long Life of a Quick "Fix"*', in The Washington Post, 31 May 2015.
70. Rexford, J. and C. Dovrolis. '*Future Internet Architecture: Clean-Slate versus Evolutionary Research*'. Communications of the ACM 53, no. 9: 36. doi:10.1145/1810891.1810906, 1 September 2010.
71. See for example the SAFE Network project: https://safenetwork.org/
72. For more information, see: National Council of ISACS
73. European Commission: '*Communication from the Commission to the European Parliament, the European Council and the Council: Second Progress Report towards an effective and genuine Security Union*', COM(2016)732 final, 16 November 2016: The Commission is also conducting work on aviation, maritime and land transport, particularly for cruise and ferry services, and for railway services. It has also strengthened its cooperation with strategic partners through the cooperation with the Department of Homeland Security in the US and Public Safety Canada as regards critical infrastructure protection, cyber security and resilience.
74. Smith-Meyer, B., '*Cybersecurity: Commission mulls middle-man role*', in Politico.eu, 21 November 2016..
75. US Department of Homeland Security, '*What is Critical Infrastructure?*', October 2016.
76. i.e. public or private entities providing services that are essential for the maintenance of critical societal or economic activities.
77. Member States are requested to identify the operators of essential services on their territory by 9 November 2018 and the European Commission is to report back to the European Parliament and Council on the consistency of the approach taken by Member States.
78. Internet Corporation for Assigned Names and Numbers (ICANN): '*Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends*', 1 October 2016.
79. US Department of Commerce, '*Op-Ed: ICANN Transition Protects Internet Freedom*', 14 September 2016.
80. United Nations Office of Disarmament Affairs (UNODA), '*Fact Sheet: Developments in the field of information and telecommunications in the context of international security*', July 2015.
81. Organisation for Security Cooperation in Europe (OSCE), 'Initial set of OSCE confidence-building measures to reduce the risk of conflict stemming from the use of information and communication technologies', PC.DEC/1106, 3 December 2013.
82. OSCE, '*OSCE confidence-building measures to reduce the risk of conflict stemming from the use of information and communication technologies*', PC.DEC/1202, 10 March 2016.
83. As promoted also by the US coordinator for cyber-issues Mr. C. Painter in his Testimony to the US Department of State, '*International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms*', 25 May 2016.

PDF: ISBN 978-92-79-68073-1 • doi:10.2872/955505 • ISSN 2467-4222 • Catalogue number: ES-AA-17-004-EN-N
HTML: ISBN 978-92-79-68074-8 • doi:10.2872/693696 • ISSN 2467-4222 • Catalogue number: ES-AA-17-004-EN-Q