SWP Comments

Stiftung
Wissenschaft und
Politik

German Institute
for International and
Security Affairs

The EU’s Revised Cybersecurity Strategy

Half-Hearted Progress on Far-Reaching Challenges

Annegret Bendiek, Raphael Bossong and Matthias Schulze

In September 2017 the EU updated its 2013 Cyber Security Strategy. The new version is intended to improve the protection of Europe’s critical infrastructure and boost the EU’s digital self-assertiveness towards other regions of the world. But the reformed strategy leaves open a number of questions as to how its objective of an “open, safe and secure cyberspace” will be credibly defended, both internally and externally. The EU has neither properly defined resilience or deterrence nor made sufficiently clear how it intends to overcome institutional fragmentation and lack of legal authority in cybersecurity issues. Moreover, controversial topics – such as the harmonisation of criminal law or the use of encryption – have been entirely omitted. Member states should abandon their stand-alone efforts and speed up the legal regulation of cybersecurity at the EU level.

It has been obvious for some time that China is increasingly sealing off its national Internet, Russia is trying to spread its authoritative understanding of information sovereignty, and the USA is engaged in a military-offensive form of cyber-defence. Experts already speak of the era of “data nationalism” and the end of the global Internet. In view of these strategic challenges, the EU’s member states are seeking a path to digital self-assertiveness. “Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks”, Commission President Jean-Claude Juncker said in his State of the Union speech in mid-September 2017. At the digital summit in Tallinn in late September, European Heads of State and Government restated their determination to complete the digital single market to replace the currently existing patchwork of rules in all 28 member states. In the run-up to the summit, Germany, France, Italy and Spain were particularly ambitious. Inter alia, they called for a common tax on US Internet giants and the creation of a secure environment that protects citizens, businesses and governments in exerting their rights.

The European Commission and the High Representative for Foreign Affairs and Security Policy have also proposed to create a “solid cybersecurity structure”. Whilst the EU’s 2013 Cyber Security Strategy remains in place, the updated version introduces an extensive package of new measures. Some of these have provoked lively debate, such as the creation of a Union agency for cybersecurity that would build on the work of

Dr. Annegret Bendiek is a Senior Associate, Dr. Raphael Bossong an Associate in the EU/Europe Division at SWP.
Matthias Schulze is an Associate in the International Security Division at SWP.
This SWP Comments was written in collaboration with Magnus Römer, an intern in the EU/Europe Division at SWP.

SWP Comments 47
November 2017

the EU Agency for Network and Information Security (ENISA). In addition, there are plans to introduce a European system for cybersecurity certification to improve the security of networked devices and digital products and services. The updated strategy foresees five major reforms: First, the formation of a European research and competency centre for cybersecurity; second, establishing a Europe-wide crisis-response mechanism to deal with future large scale cyber-attacks; third, the creation of a cybersecurity emergency fund; fourth, the development of common projects in military cyber-defence as part of Permanent Structured Cooperation and with the help of the European Defence Fund; and fifth, the promotion of confidence-building measures and state responsibility, so as to contain cyber risks worldwide. All these proposals are intended to increase the EU's resilience in the cyber domain.

A more significant role for the EU in cybersecurity is needed for the protection of the digital internal market, but obviously it cannot become the single dominant policy forum in this domain, given the global interdependence of technical infrastructures and software as well as changing national ambitions in cyberspace. Yet since the EU is the world's largest common market, it also represents the largest framework for binding regulation. Seen from this angle, the current set of proposals for reworking the European cybersecurity strategy appears rather half-hearted. Five problems or deficits need to be addressed. First, the EU's understanding of resilience as a strategic approach remains vague. Second, European cybersecurity suffers from institutional fragmentation and a weak financial base. Third, the proposed measures for increased cybersecurity lack legal force. Fourth, this is particularly true for the harmonisation of criminal law in the fight against cybercrime. Fifth, it remains unclear how defensive cyber-deterrence as a credible component of cyber-diplomacy is supposed to work in detail.

For these reasons, the EU's updated strategy is no turning-point in the ever more politicised debate on cybersecurity. It is time for the EU and its member states to overcome limited, step-wise initiatives, and to address more challenging topics head-on so as to provide strategic orientation. Otherwise, repeated calls for EU "strategic autonomy" will remain empty words.

Resilience as Guiding Principle

Both the EU's 2013 Cyber Security Strategy and the new package of proposals maintain a preference for civilian, police and military-defensive instruments to protect information-technology (IT) systems and infrastructures. The underlying guiding principle of resilience corresponds to the EU's Global Strategy of June 2016. However, the meaning and impact of resilience on European cybersecurity needs to be defined more clearly.

The term of "resilience" is not synonymous with comprehensive security. Instead, resilience refers to the capacities of any technical or natural system to regulate itself. The concept of resilience replaces the measurement and control of risks with the decentralised and flexible ability to resist varied disruptions and often unforeseen shocks. A resilient system can tolerate the loss of individual building blocks, and may even thrive through so-called "creative destruction". An example is the early Internet, which was founded on the principles of radical self-organisation and dynamic change. Similarly, many technical experts and activists advocate the development of open-source software, decentralised networks and use of encryption as the best way to cyber resilience.

However, the past few years have shown that such a decentralised approach is insufficient. The growing vulnerability of infrastructures to cyber-attacks or software errors cannot be addressed by voluntary cooperation and technical innovation alone. In liberal societies, cybersecurity is also increasingly viewed as a public good that can only be generated through binding regulation. Yet in order to maintain a balance between the stability and necessary openness of cyberspace, the EU needs to formulate a more precise understanding of resilience.

The European Commission rightly calls for an approach to resilience that encompasses economic, societal and political actors – in other words, the whole of society. This comprehensive approach includes a unified market for cybersecurity, based on "security by design" in networked devices, the centrepiece of the digital single market. Mandatory cyber-hygiene – meaning the obligations to update and carefully use networked devices – concern each market participant, since the behaviour of the weakest link can determine the resilience of the whole system. At the same time, the shortage of IT and cybersecurity experts is identified as the most fundamental challenge. Calls for harmonised training and curricula to build up human resources are therefore necessary and welcome. However, the EU has almost no formal competences in education. This structural deficit cannot be compensated by further proposals for a European "blueprint" on crisis-response mechanisms or reinforced cybersecurity exercises alone.

Overall, these measures are coherent with a notion of distributed resilience, but fail to set clear priorities, which could accelerate the necessary structural changes in member states. An overly vague concept of European resilience may instead conceal badly coordinated practices and introduce a lack of accountability. Blueprints, certificates and education plans do not guarantee resistance to actual crises or operative security. More detailed concepts should show how the EU could make progress here despite its limited legal competences. In the long term, early and comprehensive training will be the only way to close the digital skills gap and tackle the lack of corresponding human capital.

Institutional and Financial Fragmentation

The EU should also be more decisive when it comes to the fragmented institutional and multi-level set-up for cybersecurity. The EU's updated strategy makes some important proposals in this regard. The legal basis and budget of ENISA should be strengthened in order to work on cybersecurity certification and to oversee the implementation of EU legislation on IT infrastructure security. Furthermore, the agency's range of tasks and budget should be expanded, flanked by more structured and intensive cooperation with other relevant EU actors for cybersecurity, especially the Cybercrime Centre (EC3) within Europol. The agency should also take the lead on new operative solutions, such as serving as a one-stop shop for handling acute cyber-attacks. Affected businesses would have only one interlocutor when it comes to the security of cross-border data transfers – on whose pronouncements they should then rely. However, alongside ENISA the Commission foresees the creation of a further centre and network of excellence, which should boost both security research and the roll-out of new security technologies. This additional centre of excellence would be built on, and incorporate existing national research centres for cybersecurity. The European Defence Agency (EDA) should also become involved step by step. Finally, the new excellence centre should "buttress" ENISA's certification processes for IT products, whereas ENISA will retain the main responsibility for strategic risk analysis.

Not all tasks can meaningfully be bundled into a single EU cybersecurity agency. Yet the overlapping competences and interfaces between these different actors must be specified as quickly as possible. Larger member states might complicate the development of an effective governance network at the EU level, because they are already heavily invested in their own national solutions. The German Federal Government puts much effort into a new cyber-defence cluster in Munich while France has taken a strategic policy decision to promote research into artificial intelligence. To date, it remains wishful thinking on the part of the Commission that these and other national initiatives will be smoothly integrated into a comprehensive European network. Not even ENISA's role vis-à-vis national cybersecurity bureaucracies – for instance, Germany's Federal Office for Information Security (BSI) as well as its newly established Central Office for Information Technology in the Security Sphere (ZITis) – has been adequately clarified.

Meanwhile, all state agencies compete with the private sector for IT experts, but they are often much less attractive than private employers. EU institutions should avoid unnecessary competition for qualified staff; the scarce human resources to deal with acute security challenges need to be concentrated as much as possible. The desired substantial increase in training and human resource development in all member states is a very long-term ambition, which needs to be bridged and supported by an effectiveEuropean process of pooling and sharing of knowhow.

For immediate impact, member states should at least support an ambitious financing of the new excellence network, as the Strategy calls on them to do. This is clearly necessary given the enormous sums that competitors such as China, India and USA invest in their IT industries and research. The new cybersecurity emergency fund suggested by the Commission can only be the beginning of a much more substantial reallocation of EU budgetary resources. However, the coming negotiations about the EU's next Multiannual Financial Framework risk getting bogged down in national net contributions and compensations for the loss of UK net payments.

Weak Standard-Setting

All stakeholders should be ready to support more EU legislation to strengthen cyber resilience. In the updated strategy, the EU rightly stresses the certification of IT products as a central step. The European (digital) single market as biggest global market has the necessary leverage, which could also help to increase global standardisation. Yet even if ENISA should work onstricter product certification and security testing, the EU does not commit to making such procedures compulsory. By contrast, the new EU directive on protecting critical IT infrastructure (Network and Information Security, NIS) has shown that previous voluntary approaches reached their limits. All too often, public-private partnerships for cybersecurity could not overcome structural hurdles to the timely reporting and early prevention of cyber-attacks. The new NIS Directive therefore obliges operators and providers of "essential services" – such as energy, water supply, transport, finances, health and the Internet – to make adequate investment and organisational reforms for cybersecurity. Member states, too, have to create national reporting systems. The widely divergent cyber capacities of member states are the critical issue for a reliable implementation of the NIS Direction under the leadership of a strengthened ENISA. In the medium term, the definition of critical infrastructures covered by the NIS Directive needs to be reviewed as well, because Internet providers or smaller digital businesses can be gateways for attacks.

Considering this, the revised strategy's cautious approach to further product security regulation comes as a surprise. Not to envisage a shift from voluntary to obligatory product certification is a missed opportunity for a forward-looking document. Traditionally centralised infrastructures increasingly overlap with the private use of technical devices in the so-called Internet of Things, which is creating multiple new vulnerabilities. Mandatory certificates and enforceable liability would also force producers from other parts of the world to adapt to European standards, if they want to maintain access to the single market. Early regulatory action could, in turn, create competitive advantages for European businesses (first mover advantage). Last but not least, the growing public demand for IT-product security justifies transitioning from voluntary to compulsory standardisation processes at the earliest opportunity.

Fighting Cybercrime

The EU's ambitions for legal reform outside the single market remain limited as well. To contain cybercrime effectively criminal offences and investigative tools for prosecuting authorities need to be harmonised. The updated strategy mentions the EU's ongoing policy debate on how to facilitate the cross-border transfer of electronic evidence. This, and its proposal to use the technical communications protocol IPv6 as widely as possible, could help to simplify IT forensics. However, other important debates are dealt with in an overly cautious manner or simply left out. For instance, The proposal to draw up voluntary guidelines on how public-private partnerships to combat cybercrime could comply with EU data-protection laws can only be a first step. Evolving European data-protection laws for the single market (e.g. E-privacy) create significant tensions with the practices by many global companies. The US has shown, too, that public-private collaboration for law-enforcement in cyberspace requires binding rules, so as to avoid surveillance scandals or high-profile court cases that damage mutual trust.

Moreover, the EU's revised strategy does not take a stance on whether encryption technologies could be weakened to allow for easier access by law-enforcement and intelligence organisations. Encryption is a crucial pillar of dispersed and resilient cybersecurity, as it makes it more difficult for all malignant actors to steal data. EU member states soon have to decide jointly whether to allow "back doors" or "telecommunications surveillance at source", i.e. to break into devices to intercept communications before encryption. In this context, member states also have to consider maintaining a trustworthy regime of cross-border law-enforcement cooperation. Online as offline, criminal evidence has to be acquired in line with core principles of the rule of law and fundamental rights. Hence, EU interior ministers have been negotiating on the challenging issue of encryption for some considerable time already. The fact that the updated cybersecurity strategy fails to engage with this debate is a further sign of its weak political ambition and overemphasis on compromise.

Similarly, the strategy fails to touch on the thorny question of how criminal content on the Internet and social media should be tackled. Most EU member states have signed the Budapest Convention and thus committed themselves to prosecuting criminal offenses committed in cyberspace. Nevertheless, there is a wide discrepancy between European states regarding which actions constitute a crime in the digital domain. The main contention is over the scope of freedom of expression, or the definition of illegal "hate speech". Whereas the Commission has drawn up another voluntary code of conduct in partnership with the private sector, several EU member states have passed stricter liability laws for social-media providers. Uncoordinated national efforts, however, have limited effect and may endanger freedom of speech both within and outside the EU. For instance, authoritarian regimes such as Russia have explicitly referred to Germany's new Internet Enforcement Law *(Netzwerkdurchsetzungsgesetz)* of September 2017 to justify their own growing online censorship. Coordination problems are aggravated by the fact that private actors are urged to delete content directly. This frequently results in excessive private decisions to take down content and may create a wider "chilling effect" on freedom of speech. Generally speaking, the reach and power of Facebook and Google underline the need to draw up binding rules at the EU level. These rules need to define clear, balanced, accountable and enforceable mechanisms for protecting fundamental rights as well as addressing illegal content.

Cyber-Defence and Cyber-Foreign Policy

The EU's revised strategy contains little new on international rules and norms for the conduct of states in cyberspace, despite the intensifying global debate on digital sovereignty and cyber-deterrence. In cyber-defence, the EU continues to pursue a defensive approach. This is in line with its guiding principle of resilience, according to which certain risks must be accepted and their impact minimised. However, it would be helpful to spell out more clearly how systemic resilience combines with effective deterrence. Resilience first and foremost deters – or rather undermines the effectiveness of – denial of service attacks and cyber operations that seek to disrupt critical infrastructures. By contrast, misinformation campaigns or cybercriminals may only be deterred by more active measures and effective prosecution. Hence, further bilateral agreements between the EU and third states on fighting cybercrime would be useful.

When it comes to military cyber-defence, the EU strategy primarily refers to its existing cooperation with NATO, the option of Permanent Structured Cooperation under its Common Security and Foreign Policy (CSFP), and the potential of the Defence Fund agreed in June 2017. Because of the widely different levels of capacity and speed of digital transformation among the armed forces of EU member states, it makes sense to make cyber-cooperation within the CSFP more flexible. More EU exercises and capacity-building in the weaker member states are certainly useful as well. Nevertheless, the question arises how these countries can catch up and use the new defence fund, while they may simultaneously be excluded from Permanent Structured Cooperation due to their lagging capacities in the cyber domain.

NATO, in any case, remains the first point of reference for Europe's defensive cybersecurity. The European Council had already decided in December 2013 to intensify EU-NATO cooperation and adopted the Cyber Defence Policy Framework a year later. This framework is meant to improve the protection of CSFP missions and the communications security of the European External Action Service (EEAS). EU-NATO cooperation on hybrid threats, which also includes cyber-attacks and misinformation campaigns, should be channelled through a new Hybrid Fusion Cell established in Helsinki in early April 2017. All NATO and EU member states are represented on its supervisory board, and common EU-NATO cyber-exercises now regularly take place. Nevertheless, the joint EU-NATO strategic framework remains unclear. In the Tallinn Manual of 2013 and 2017, NATO's Cooperative Cyber Defence Centre of Excellence made proposals for codifying the right to wage war *(jus ad bellum)* and the laws of war *(jus in bello)* in cyberspace. This should not be construed as a joint policy with the EU and its member states.

Many academic researchers take a critical view of the digital counter-attacks considered by NATO. It is often impossible to identify either the perpetrators of cyber-attacks or the targets for counter-strikes, a difficulty known as the attribution problem. There is a high risk of attacking systems that were uninvolved or hijacked themselves – and that might even be needed for critical supply tasks in other countries. Counterattacks may also trigger an escalating spiral of reciprocal cyber-attacks. The problem needs to be addressed urgently, since some private companies already practice digital counter-attacks, known as hack backs. Under the EU's guiding principle of resilience, states should define their red lines and levels of escalation readiness, including corresponding sanctions. This is predicated on the creation of uniform attribution standards and a common situational awareness of cyber-threats. ENISA or the Hybrid Fusion Cell in Helsinki would be suited to this task. To prevent conflicts from spiralling out of control in cyber-space, further political instruments need to be specified. The EU agreed to develop a so-called Cyber Diplomacy Toolbox, which sets out possible counter-measures in case of an external cyber-attack and raises the costs for perpetrators. The toolbox is expected to encompass the summoning of diplomats, further political, economic and penal sanctions, as well as digital responses. However, the fundamental problem of attribution applies even to diplomatic responses. And since the use of the Toolbox is not only voluntary but also requires the unanimous support of all EU member states, there are multiple hurdles to a mount an effective defensive deterrence.

Finally, the EU's updated strategy declared that cybersecurity issues would be prioritised in all relevant external relations. As a starting point, the strategy proposes a further "platform" to support third states in their cybersecurity capacities. This can also be seen as a concession to Eastern European states, aimed at improving protection from Russian interference in the EU's neighbourhood. Yet further global or multilateral processes for negotiating common norms on cybersecurity are only mentioned in passing.

Outlook: The EU as Digital Power

The reform proposals contained in the updated EU Cyber Security Strategy of September 2017 are a step in the right direction. Taken together, they would help the Union to resist cyber-attacks technically, legally and politically. However, effective resilience requires a deeper engagement by member states. They need to adopt a more strategic perspective and systematically tackle any weak points. To date, ambitious proposals have tended to meet with resistance. Some EU member states do not see the EU as the appropriate organisation for IT regulation but prefer the OECD. Representatives from the information and communications technology (ICT) industry complain that EU institutions currently lack the requisite expertise.

That is why the EU must take a step beyond the reticent approach that still characterises the new package of proposals. The first litmus test will be the envisaged European certification and identification framework. Led by ENISA and the European Commission, member states need to rapidly reach agreement on adequate security standards and move towards legally binding rules for the security of ICT products as quickly as possible. The private sector and academia must also be involved in the process to maintain the right balance between innovation and regulation. A competitive European ICT industry depends on a level playing field, which would also enable it to do better on global markets. This shared understanding should help to reach agreement among all stakeholders.

The greatest challenge to building multilayered cyber-resilience remains the creation of reliable and trusting relationships between all participants. This holds true between strong and weaker cyber-nations as well as between member states, EU authorities and private actors. Looking beyond the EU, clear strategic guidelines for cyber-foreign policy and credible links to decision-making are becoming ever more important. These include reinforcing encryption and responding to cyber-threats from outside Europe with political, economic and legal sanctions.

Taken individually, EU member states and businesses cannot handle these tasks. If the EU truly wants to become a digital power, close cooperation in all mentioned areas, a legally binding European framework and technical standardisation are indispensable.

These Comments reflect the authors' views.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3−4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761

Translation by Tom Genrich

(English version of SWP-Aktuell 72/2017)