EOS POSITION PAPER

EU DIGITAL AUTONOMY:

Challenges & Recommendations for the Future of European Digital Transformation

November 2019

EUROPEAN ORGANISATION FOR SECURITY

AUTHORS

	Florent Kirchner	CEA
	Giulia Antonucci	Engineering
	Mario Barile	
	Véronique Pevtschin	
	Paolo Roccetti	
	Lorraine Wilkinson	EOS
	Anna-Maria Osula	Guardtime
	Giorgio Mosca	Leonardo
	Angeloluca Barba	
	Nicola Iarossi	
	Ana Ayerbe Fernanda-Cuesta	Tecnalia
	Emmanuel Dotaro	Thales
	Alie El-din A Mady	UTRC

ABOUT EOS

The European Organisation for Security (EOS) is the voice of the European security industry and research community. Operating in 15 different countries, EOS Members provide security research, solutions, and services across many security domains, including border, cyber, transport and crisis management. EOS Members represent almost two-thirds of the European security market, including major industry players, SME's, research centres and universities from across the whole business cycle: from technology R&D, equipment manufacturing, and system integration, to service providers, and end-users. Within EOS, the Cyber Security Working Group represents industry leaders in cybersecurity products and services as well as the growing research community.

For further information please contact:

Email: Info@eos-eu.com

Website: www.eos-eu.com

Twitter: @eos_eu

Table of Contents

EXECUTIVE SUMMARY

Given the speed and complexity with which the global digital economy is evolving, EOS is keen to ensure that the EU is not left behind in the global digital market place, and has the means and capabilities to develop its own digital autonomy and secure its cybersecurity independently from third-countries.

Today, Europe's society and economy are dependent on digital infrastructures and services, and the cyber-security of these underlying elements must be ensured across increasingly complex value chains. Sourcing critical cybersecurity elements and services in Europe is the only solution that guarantees compliance with European values[1], protection of Intellectual Property Rights (IPRs) and continuity of operational capabilities. As such EOS recommends developing digital autonomy "enablers" ranging from skills to cyber-threats detection and response mechanisms.

By examining the key risks and opportunities for EU digital autonomy, across five distinct digital products and services, EOS has identified a range of recommendations for consideration and development by EU policymakers and regulators:

1. Sourcing and Sharing Cyber Threat Intelligence in Europe

The availability of autonomously developed European cybersecurity methods and tools is vital for European strategic security for several core reasons: to directly collect EU intelligence, to verify shared sources and to build trust in international sharing relations. A holistic EU plan for effective digital autonomy capabilities will increase the resilience and future proofing of the EU cybersecurity value and supply chain by allowing it to adapt to change and combat attacks more swiftly and independently. In order to have an effective and pervasive impact on the societal and economic ecosystem in the Union, the plan should consider development and deployment of both in-house and as-a-service capabilities. Furthermore, integrating EU R&D and deployment is essential to building the information sources, tools, skills and capabilities that are critical to the autonomy of its cyber threat intelligence.

2. The Internet of Things (IOT) & Cyber-Physical Security

The deployment of the Internet of Things is going to explode with the introduction of 5G (indications are that with 5G, the supported connected devices / km2 will increase from an average of 60.000 with 4G to 1 million with 5G). Current forecasts foresee 125 billion devices by 2030. This represents a huge increase in the attack surface and channels to reach into critical resources, but also in easing the connection from cyber-attacks to create dangerous impacts in the physical world.

Cyber-attackers are increasingly using IoT to damage or disturb physical environments as well as conducting digital data breaches – in effect using IoT's vulnerabilities as a channel to undermine cyber-

[1] EOS recommendations aim to identify, assess and foster the impacts of cybersecurity and Digital Autonomy upon European and globally agreed values. In fact, EOS aims to progressively align its proposals with the Sustainable Development Goals (SDGs), 17 global and interdependent goals adopted by the 193 countries of the UN General Assembly in 2015.

physical security environments. At the industrial level, the cybersecurity of the production process in which IoT is being used has a crucial role in maintaining the economic stability of European industry and should be certified to reflect EU interests and values. In the health sector, wearables and implantable devices are creating direct channels for cyber-attackers to impact the physical well-being of patients. Furthermore, the surge in IOT devices creates a related increase in transmitted data – and to keep this under control, the transformation of data will have to be done at the edge of networks as well as centrally.

EU policy and regulatory tools are needed to ensure the cybersecurity of and trust in the IoT in five key ways:

- ✓ Ensuring transparency and ethical considerations reflecting European values are integrated from the design stage, while also supporting innovation and the adoption of IoT
- ✓ Certifying cybersecurity products and services
- ✓ Encouraging a life cycle security approach and ensuring that industry takes responsibility for cybersecurity components throughout the value chain
- ✓ Clarifying the liability chain that is the most appropriate to manage risk in each use-case to both public and private stakeholders
- ✓ Ensuring the cyber-secure processing of information done at all the levels including individual IOT devices

3. Secure Data Lifecycle: A Cryptography Challenge

The greatest challenge to the secure data lifecycle comes from the fact that data protection and usability are usually seen as antagonistic concepts. At the macro-level, European crypto-agility, the ability to upgrade the hardware crypto layer when the quantum threat becomes reality, will be a critical factor in securing the EU's digital autonomy. At the micro-level, the EU must develop recommendations on what cryptographic algorithms and key lengths are considered safe for different applications, in order to raise security resilience and strengthen the Digital Single Market.

4. Artificial Intelligence (AI)

EU regulators have yet to prioritise the regulation of cybersecurity of AI-systems in Europe despite strong reference to the security-related aspects of AI applications in the 2018 AI Strategy. However, a comprehensive approach to AI in Europe must include EU standards for AI (cyber)-security applications, and R&I activities targeted at the security domains.

Defining a longer-term EU action plan on AI beyond the next Multi-Financial Framework (MFF) is needed to protect European AI-dependent security systems and applications from emerging cyber threats, while maintaining a leading EU position on the global AI market. Furthermore, evolving the European AI Alliance to include a formal and prominent role for the European security industry and research community, will ensure EOS technological expertise is mobilised to address security concerns more effectively.

5. Cyber Security as a Service

Software security assessment requires high specialization and constant update, and is well suited to the cybersecurity 'As-a-Service' model, particularly in a digital ecosystem where products and systems are assembled from differently sourced components. However, for it to evolve effectively, EU policymakers and industry must provide practical tools to cybersecurity product and service developers, in the following key areas:

- Addressing the definition of cybersecurity assessment targets, including in the scope differential assessment
- Including the creation and validation of proper audit trails for intrusion detection, impact assessment and forensics in software security assessments
- Establishing links with training programs to ensure that certified components and services are properly developed and operated

European customers should also be encouraged to trust cybersecurity services with the creation of an innovative certification framework applicable to the wide diversity of cybersecurity services, thereby developing a 'best of breed' EU cyber security industry, and maintaining EU autonomous cybersecurity protection capabilities. This certification framework should consider the process level, ensuring that the cyber-security is managed as an end-to-end enabler in complex workflows.

Conditions for Regulatory Success

EOS has identified some of the key conditions for the regulatory success of an EU Digital Autonomy policy, which include the need to balance over-regulation and laissez-faire approaches, and follow the principle of technology-agnostic regulation. Furthermore, EU Cybersecurity measures need to address ways to effectively **share responsibility across the supply chain**, including discussing extending the chain of liability to the end user. More efforts should be placed in developing EU cybersecurity intelligence capabilities, early warning and rapid information exchange system about the vulnerabilities and risks.

At the holistic-level, minimum EU security standards and a clear security-by-design approach are needed in domains such as critical infrastructure protection, supply chain management, as well as e-governance. Finally, the EU should strive for further MS policy harmonisation, taking a stronger role in cybersecurity through comprehensive policies such as promoting collective cybersecurity measures.

EOS remains committed to sharing the perspective of the European security industry and research community on the challenges and opportunities for the European digital autonomy. While there is no single-sweep solution to making the EU digitally autonomous, the EOS recommendations outlined in this paper aim to provide an overview of the practical policy and regulatory actions that might form part of a comprehensive package of measure EU policymakers could implement going forward.

Three core themes emerge from the recommendations, which EU policymakers should take under consideration:

- **An EU legal act to define priority investment areas and drive European Digital Autonomy forward is critical to overcoming current dependence on other regions' technologies and services.**
- **Designing and implementing activities for achieving European Digital Autonomy requires a roadmap with concrete benchmarks keeping in mind the challenge of effective coordination between governmental and industry stakeholders on domestic and regional levels.**
- **Further regulatory steps may be necessary for addressing Member States' fragmentation in implementing existing EU Digital policies, keeping in mind both the end-users and industry.**

EOS POSITION PAPER

EU DIGITAL AUTONOMY:

Challenges & Recommendations for the Future of European Digital Transformation

November 2019

1. INTRODUCTION

In 2017, Council Conclusions from the Tallinn Digital Summit saw EU Heads of State and Government calling for the EU to become "*a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet*."[2] This commitment followed a period of intense policy dialogue and legislative development around cybersecurity, initiated by the 2013 EU Cyber Strategy[3] including, amongst other things, the implementation of the NIS Directive[4], GDPR[5], e-IDAS[6].

Yet, despite EU policy initiatives and Member State political objectives, Europe has room to further develop a homogenous and inclusive approach to its strategic cybersecurity capabilities. Europe needs to foster EU cybersecurity champions, promote EU ethical standards in cybersecurity, and develop European cybersecurity skills and education.

The European Organisation for Security (EOS) would like to share its recommendations for how these objectives might be achieved efficiently and effectively.

For the past decade, EOS, which represents the voice of the European security industry and research community, has been promoting the development of EU policy to develop cyber-security solutions and combat cyber-crime. Through the work of its Cyber Security Working Group (CSWG), EOS has, since 2008, been advocating for cross-cutting cyber-security policies that are strategic to the European security, and to the European economy.

It is for this reason that EOS strongly encourages the development of a coherent and comprehensive EU policy framework on **European digital autonomy**, which would deliver critical value to the Union's economic standing through European sourced cyber-security services and solutions.

As such, this position paper provides EOS' industry expertise on the key areas of the European digital economy, where European strategic autonomy must be reinforced, as well as recommendations on how digital autonomy could be achieved. Going forward, EOS remains committed to supporting EU policymakers to fully realise policy that safeguards European digital autonomy in a fast-evolving digital

[2] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres; Brussels, 12.9.2018, COM(2018) 630 final -2018/0328 (COD);

[3] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013;

[4] 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;

[5] 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

[6] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

environment, support its coherent implementation to overcome market fragmentation and decrease the complexity for users of digital solutions, and use it as a driver for growth of our economy.

2. DIGITAL AUTONOMY

KEY TAKEWAYS

- ❑ Europe's economy is dependent on digital infrastructures and services
- ❑ The cyber-security of these underlying elements must be ensured across complex value chains
- ❑ Sourcing critical elements in Europe is the only solution to guarantee fast (re)-action capabilities, continuity of operational capabilities, compliance to European values and protection of IPRs
- ❑ EOS recommends developing digital autonomy "enablers" ranging from skills to cyber-threats detection and response mechanisms

The technological, architectural and business transformations that are companions of the digital age, are challenging Europe's strategic approach to cyber security. These fundamental shifts warrant close attention from European policymakers, and key industry and security stakeholders, given the evolving risk landscape that is impacting a wide range of societal & economic sectors.

2.1 Transformations are changing the game

The Digital Transformation is happening in the context of two major convergences. Firstly, between digitalisation, and Information and Communication Technologies (ICT), which is leading to the mainstreaming of technologies such as virtualization, softwarization, and cloudification. Secondly, the convergence of digitalisation and Operational Technology (OT), which is transforming critical transport, energy, medical, industrial and many other sectors.

As a result of the Digital Transformation, citizens and the digital economy, including vertical markets, are developing a critical dependency upon cybersecurity capabilities. Such capabilities go far beyond classical components (hardware and software) or product supply-chains, since Digital Infrastructure today relies on a combination of complex systems and services. Moreover, operational cybersecurity capabilities are necessary to implement any strategic protection policy.

As a consequence of the deployment of new digital paradigms and architecture, protecting the digital economy requires the development of expert cybersecurity capabilities for major digital architectural patterns such as service-dominant/cloud-based ecosystems, Internet of Things (IoT), Cyber-Physical

Systems (CPS), Edge Computing, 5G slices, etc. However, these game-changing technologies translate into constantly increasing exposure to cyber-risks, opening multiple channels through large attack surfaces. This in turn raises the need for trust management, security level awareness, and liabilities perimeters. Such challenges only serve to highlight the critical importance of enhancing and enforcing EU cybersecurity policies.

Finally, a never-ending list of disruptive technologies is continually challenging the ability to control European cybersecurity. The destiny of our products, systems and services, not to say citizens' rights and our economy, is fully dependent on European cybersecurity requirements and our control over deeply impactful technologies such as:

- Artificial Intelligence (AI),
- Distributed ledgers/blockchain,
- (I)IoT/CPS,
- Virtualization,
- Softwarization,
- Cloudification,
- Data-centric technologies (crypto, processing, sharing,…).

Cybersecurity solutions must adapt, and when possible anticipate, future digital transformations in order to sustain a strategic level of autonomy for European society and economy.

2.2 The Necessity and Opportunities for EU Digital Autonomy

The World is Digital, the World is Cyber

It is obvious that Europe can no longer afford to simply react to the current, disruptive, digital climate. In an increasingly digitalised world and the blurring frontiers between the cyber and physical worlds, cybersecurity has become a mandatory and intrinsic component with a transverse impact on other strategic digital trends. For example, none of the critical directions of High-Performance Computing (HPC), 5G, AI, or IoT, among others, will be able to grow without a sustainable "cyber security enabler" inside.

Our Policy , our Interest, our Digital Autonomy

The European Union and its Member States are defining their own strategic digital policies, which translate into cyber security-specific initiatives, including the 2018 proposal of the EU Cyber Act. The new threat landscape stemming from the digital transformation, specific policies to protect citizens' data (i.e. GDPR, e-privacy), ethical considerations, and global sustainability targets[7] have all highlighted the need

[7] In this context, the introduction of Sustainable Development Goals (SDGs) signed by 193 member countries of the United Nations has created a common language and common KPIs that are shared, monitored and understood around the world. Several organisations and industries, including technological ones, such as the GSM Association, started aligning their strategic objectives with SDGs to highlight how their business contributes to the realisation of one or more SDGs - i.e. SDG 9 (Industry, Innovation and Infrastructure), SDG 4 (Quality Education) and SDG 13 (Climate Action). Taking into account the essential role EU Digital

to define, develop and enforce cybersecurity independently from third parties that may not share Europe's fundamental values and interests. This is critical for maintaining European economic competitiveness for cybersecurity industry players, but also for all sectors dependant on digital infrastructures and digitally based value chains. What if for a given software component, we as the EU were not capable of feeding a "white list" with a relevant/compliant provider? What level of deterrence can be achieved by ensuring our autonomy over third parties' delivery? How can we protect our IPRs if the underlying infrastructure is not proven to be compliant to a European defined level of security as well as European values?

The question of autonomy should be raised for all aspects of the Digital Transformation:

- The adoption of the technologies mentioned above cannot be envisaged without addressing their cyber security. What is the benefit of a competitive HPC capability without a guarantee of its secure use in case of crisis? Can the promise of AI benefit the EU without mastering data ownership/protection, or confidence in algorithms? Is European industry ready to use 5G Infrastructure without essential features depending on cybersecurity?
- Change in software pattern architecture is also key for European autonomy. Recent examples using IoT weakness, but also lack of mastered Cybersecurity Enforcement Points in the architecture, highlight the need to (re-)consider critical mastered assets for cybersecurity deployment.
- Business' evolution towards the "as a service" digital paradigm recognises the vast number of products, tools and technologies that vendors can deliver to users as a service rather than provide them locally or on-site within an enterprise. However, it is also putting many sectors at risk if they are not operational and compliant with required EU policies. This is spanning pure "Security as a Service" for security delivery but also thousands of previous software or hardware applications delivered through the cloud and requiring cybersecurity protection.

Cyber security solutions and the security of these solutions themselves are critical for European citizens and industry in a competitive digital world, and EU policymakers must therefore seek to enforce digital policies that go beyond technical solutions, and operational capabilities across sectors and ecosystems, to address cyber security along the whole supply chain. This requires consideration of cybersecurity from both a component-level and process-level perspective.

2.3 Developing Enablers of European Digital Autonomy

Education and skill-building are the first step in strengthening Europe's digital autonomy, and require a two-fold approach: firstly, ensuring that the content of cyber security education delivers the required level of knowledge and operational practices; and secondly, educating enough skilled/operational people to

Autonomy will play in supporting sustainable digital transformation in Europe and beyond, EOS recommends that the EU consider how strategic choices in European Digital Autonomy are contributing to selected SDGs.

fulfil the needs of the cyber security industry, and all sectors needing to interface with or deploy cyber secure services and solutions.

Threat intelligence is also a key digital autonomy enabler; the current dependence on cyber-threat intelligence sourced outside of Europe can delay the detection of threats across European infrastructures and slow down Europe's capability to counter on-going attacks. Being open and cooperative regarding our knowledge of cyber vulnerabilities and attacks, for example, does not mean being dependent upon overseas expertise. Beyond critical assets or infrastructure, European cyber capabilities need to encompass horizontal and vertical risk awareness globally, thereby guaranteeing the highest level of protection and detection. Furthermore, threat intelligence needs to be contextualised to the users and companies that need to be protected, which means ensuring an analytic capability mixing cyber, physical and human intelligence acquired through trusted channels.

Protection from cyber threats is two-step process. On the one hand, the EU should be capable of evaluating and certifying the cyber security products, systems, solutions, services used in B2C, B2B and B2G. This benefits all users by building awareness of the level of security offered by the products, systems, solutions, services they purchase or use. On the other hand, European evaluation and certification should help our cybersecurity industry to achieve a "best in class" competitive offer. This creates a virtuous circle: the more competitive the European cyber industry, the more flexibility EU policymakers have to enforce their digital policies. As a side effect, this also contributes to Europe's overall deterrence of cyber threats.

Detection and incident response mechanisms are the key means to react to cyber-attacks. However, it is proving a major challenge to align European Member States' response standards and deploy cooperative mechanisms while respecting State sovereignty. This imbalance further raises the risk of dependency upon third-countries or companies, which may have different views or interests than Europe. Ultimately, digital autonomy strengthens European defence capabilities against cyber-attacks. In other words, our capabilities rely on knowledge, tools (products, systems, services), process/organization, and stakeholders mandating an agreed and pre-defined level of classified information and trust.

Digital autonomy benefits both cybersecurity users and providers that share the same goals and values. However, those with different cybersecurity perspectives or interests, may not share the strategy and vision developed by the European Commission and EU Member States. EOS believes that European dependency upon third parties that rely on different authorities or interests, must be overcome by coherent, and consistent ecosystem regulatory environment, forward-looking, cutting-edge policy, frameworks for enabling security technologies and applications to digital transformation, and a sustainable cyber industry providing best in-class solutions and services. EU cybersecurity capabilities should enable Europe to become a global digital pioneer.

2.4 European Digital Autonomy Initiatives

Since the EU Cybersecurity Strategy's adoption in February 2013[8], the pace and scope of European action in the field of cyberspace have increased considerably. In 2015, the European Commission released its Digital Single Market Strategy to strengthen Europe's digital economy and society and enhance its innovative and technological advantage.

The European Cybersecurity Strategy's focus and ambition were further enhanced in the September 2017 Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'[9]. Seen as a significant contribution to the EU's strategic autonomy, European Member States welcomed its aims "*to build a digital Europe that will be more secure, trust-enabling, conscious of its strengths, competitive, open to the world, respectful of EU's shared values on open, free, peaceful and secure global internet*."[10]

This Communication set the stage for new cybersecurity developments, notably through a 'Cybersecurity Act'[11]. Focusing on building resilience to cyber-attacks, it strengthens the role of the European Network and Information Security Agency (ENISA) via a permanent mandate, an increased budget and an extended role that includes the implementation of the NIS Directive and the proposed Cybersecurity Certification Framework. The Framework will have three priority areas: 1) Security in critical or high-risk applications; 2) Cybersecurity in widely-deployed digital products, networks, systems and services used by both the private and public sector that will help in mitigating the risk of attacks and 3) Application of regulatory obligations as well as the application of security by design.

The European Commission is also working to ensure Europe establishes the necessary cybersecurity infrastructures to manage and mitigate threats in a coordinated and effective manner. Investments have also been made through the Connecting Europe Facility to ensure that all Member States achieve a comparable level of operational cybersecurity[12]. Europe's latest proposal to establish the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres strives to secure the Digital Single Market through a coordinated cybersecurity network, the development of cyber competences, and the implementation of EU R&D programmes. The proposal, adopted by the European Parliament on 17 April 2019, envisages a Member State led governance structure, including an advisory role for the private sector. However, the final structures may change before the proposal is adopted by Member States after the new European Parliament and Commission begin their mandates later in 2019.

---

[8] European Commission & EEAS, Joint Communication on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013. JOIN (2013) 1

[9] European Commission & EEAS, Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017. JOIN(2017) 450 final

[10] Council of the European Union, Council Conclusions, 20 November 2017 14435/17

[11] European Commission, Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification. COM/2017/0477 final

[12] https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facility-cef-telecom-eu13-million-reinforce-eus-cybersecurity

A digitally autonomous Europe, is however, nothing without a skilled work force to implement the European digital technologies effectively. Developing the digital skills of the European work force is crucial if Europe is to create a secure Digital Single Market, and enhance its competitiveness. As such, ongoing EU initiatives to boost digital labour capabilities have emerged, including the Digital Skills and Jobs Coalition launched in 2016, and a Blueprint for Sectorial Cooperation to identify skills gaps in the sector.

The digital transformation in Europe has also highlighted the challenge of ensuring citizens' data privacy and to that end, the EU's General Data Protection Regulation (GDPR) entered into force on 25 May 2018. Guaranteeing EU citizens fundamental rights in the digital age, can only be guaranteed by strengthening Europe's digital autonomy.

In the context of the European digital transformation, Artificial Intelligence is increasingly being relied on to process mass quantities of data to produce actionable information, as well as predictive and response capabilities. With AI playing a key role in critical domains, such as cybersecurity, border management, public space and critical infrastructure protection, and transport security, it becomes clear just how vital digital autonomy is to European digital sovereignty, even more so in the cybersecurity sphere. The European Commission's 2018 Communication on Artificial Intelligence[13], has gone some way to acknowledging this link, outlining support for AI technologies for security, reinforcing the importance of AI in cybersecurity, and highlighting the security risks posed by AI used for criminal activities or attacks. But Europe's policymakers need to do more if they are to develop the levels of digital autonomy needed to enhance the strategic security of European digital realm.

[13] COM(2018) 237 Final. European Commission Communication on Artificial Intelligence for Europe. 25 April 2018.

3. KEY RISKS AND OPPORTUNITIES FOR EUROPEAN DIGITAL AUTONOMY

3.1 Sourcing and Sharing Cyber Threat Intelligence in Europe

KEY TAKEAWAYS

- ❑ The availability of autonomously developed European cybersecurity methods and tools is vital for European strategic security for several core reasons: to directly collect intelligence, to verify shared sources and to build trust in international sharing relations.
- ❑ A holistic EU plan for effective Cyber Threat Intelligence capability growth will increase the resilience and future-proof the EU cybersecurity value and supply chain by allowing it to adapt to change and combat attacks.
- ❑ Integrating EU R&D and deployment more coherently is critical to the autonomy of European cyber threat intelligence.

Intelligence is the collection and analysis of both open - publicly available - and hidden information with the goal of reducing decision-makers' uncertainty about a given security problem. Intelligence captures raw information and analyses it, placing it in the proper context and using it to draw conclusions about attributes of other actors, or about the state of the world, that are not directly observable. The threat intelligence challenge becomes especially difficult in relation to cyber threats. Cyber security incidents are constantly increasing in frequency, magnitude and complexity; furthermore, they are not constrained geographically by physical by borders. In today's technological environment, and in the wider context of the global digital transformation, threat intelligence is information about an existing or emerging threat that can be distributed to improve defences against or prevent a specific attack. Going beyond IP addresses, hashes, and other core identifiers, threat intelligence provides critical context around a threat activity, including Indicators of Compromise (IoC), Indicators of Attack (IoA), the tactics employed, and, potentially, the motivation of the adversary, supporting the very sensitive decision of the attribution of an attack to one or more perpetrators as well as structured groups.

The collection and analysis of threat intelligence is increasingly important for the European Union. European governments and Critical Infrastructures require timely and accurate intelligence to deal effectively with many of the threats they face today, including terrorism, proliferation of weapons etc; all these threats have a clear cyber component.

In the cyber-world even more than in the physical world, intelligence must not be collected in isolation, but on the contrary has to be shared, to speed up the detection of trends and block developing attacks, as early as possible. Sharing requires trust because decision-makers are often unable to verify

independently and/or swiftly, the accuracy and reliability of shared intelligence with the implied risk of manipulation. The availability of autonomously developed methods and tools, focused on the geopolitical, social and cultural characteristics of the European context, is vital for European strategic security for several core reasons: to directly collect intelligence, to verify shared sources and to build trust in international sharing relations.

Beyond the need for sharing, cyber threat intelligence also requires increasingly high-performance processing capabilities. Indeed, huge amounts of data is available, and its interpretation requires an extensive mix of computing power and human intelligence that must be available to interpret them. The capability to efficiently deliver threat intelligence is therefore based on the seamless, efficient and real-time integration of different capabilities: crawlers; real time processing, indexing and dispatching with high performance hardware architectures; advanced analysis tools supported by artificial-intelligence; innovative graphical interfaces for data/info correlations; and automated distribution of the results. On the other hand, whilst threat intelligence involves large computing capabilities, the value of the analysis is context dependant and the results have to be delivered to different users, including large organisations, SMEs, public administrations etc. Therefore, the delivery of tailored cyber threat intelligence should also aim to achieve an efficient use of limited and costly resources to benefit a maximum number of diverse users.

THREATS

Cyber security incidents can cause major damage to the economy, and hence, cybersecurity is one of the biggest issues that governments and businesses in the EU and globally are currently facing. The borderless nature of cyber incidents and attacks, regardless of sector or area, calls for rapid, cross-border and cross-sector responses. Efforts to prevent cyber incidents, strengthen cooperation, and enhance transparency must be stepped up. In the cyber security community, there is currently a strong need for the exchange of data to support the management of vulnerabilities, threats and incidents, as well as other cyber security activities. However, the challenge of providing anonymity in regard to cyberthreat/attack reporting, could be a strong call for the EU to establish a trusted network for such information-sharing activity.

EU dependence on third-country providers for technological tools, methods and procedures to support these capabilities poses a significant risk in terms of these solutions' trust, efficiency and effectiveness within EU, with the potential added risk of inaccessibility of back-up solutions in the case of geo-political crisis.

OPPORTUNITIES

Digital autonomy is the only way to implement a fully comprehensive and integrated European cyber threat intelligence ecosystem, incorporating the following core components:

- Technical: Creating resilient infrastructures for intelligence collection and data-sharing that can support a variety of data types and formats.
- Operational and inclusive: creating trusted channels for gathering of intelligence across both the cyber and physical worlds are key to involving a diversity of players (industrial, legal, technical

etc.) to capture the required information and transform it in actionable knowledge as fast as possible. In the fight against cyber-attacks, knowledge and speed are THE critical dimensions.

- Policy: Creating the appropriate legal structure(s) to foster comprehensive data-sharing, considering privacy and ethical issues, but without cumbersome legal liabilities.
- Governance: Creating business rules by which members of a network can share data, by defining what data they share, and with whom they share it (including anonymously).

Moreover, from a purely market perspective, the use of intelligence tools is forecast to grow significantly worldwide, especially given the growth of social media usage by criminal and terrorist organisations. In 2018 alone about 58% of large businesses acquired cyber threat intelligence services, according to Gartner[14]. Europe should not miss being part of such an opportunity in terms of financial, labour and knowledge impacts.

EOS RECOMMENDATIONS

It is critical that future policy decisions on the architecture of EU intelligence sourcing and governance lead towards the simplification and effectiveness of cyber threat intelligence, increasing the level of cooperation and exchange at the machine-to-machine, machine-to-human and human-to-human levels. Considering the rapid evolution of threats and the technologies to combat them, and the capacity and experience that national industry also builds through international collaborations and contracts, EOS believes that European public, private co-operation is critical to ensuring effective cyber threat intelligence. A European platform for co-operation would allow policymakers and regulators to focus on enhancing capacity, operations, and institutional and international cooperation; while industry can provide those technologies, skills and solutions that maximize results over organizational and budget constraints. Just as importantly, this European platform could structure a delivery model of contextualised cyber-threat intelligence 'as a service' to a wide variety of users, including the large population of SMEs that are part of Europe's economy.

EOS recommends that European cyber threat intelligence capability development be enhanced by EU and National-level initiatives to:

- Strengthen and shorten the technological value chain by encouraging through all possible instruments the creation and/or the return of current technological value in the EU area;
- Create skills and abilities that are currently lacking;
- Develop value chain & supply chain resilience: global world-wide chains are fundamental, but Europe needs to have a specific backup plan in case these fail.

We must build a value and supply chain that increases the resilience of the EU system to adapt to change and combat attacks. This does not require a return to State-financed sovereign champions, but rather an EU plan for effective capability growth, and several different strategies to guarantee the security of the EU area. EOS recommends several such strategies, including:

[14] Gartner, Information Security Spending Survey. 2018

- Building a Trust Relationship Circle among Security System Integrators, the Intelligence Community and the Customers;
- Encouraging third-country technology providers to cooperate according to agreed-upon rules;
- Gaining visibility on the real behaviour of third-country intelligence tools;
- Supporting the growth of a European market for intelligence technologies and systems ranging from cyber threat intelligence to surveillance: this encompasses supporting research but also deployment of solutions and services;
- Finding ways to appropriately tie R&D to deployment in order to maximise the effectiveness and efficiency of the Union actions supporting the development of tools, skills and capabilities in areas that EU defines as critical to the autonomy of its cyber threat intelligence.

3.2 Internet of Things/Cyber Physical Security

KEY TAKEAWAYS

- Cyber-attackers are increasingly using IoT to damage or disturb physical environments as well as conducting data breaches – in effect using IoT's vulnerabilities as a channel to undermine cyber-physical security environments.
- At the industrial level, the cybersecurity of the production process in which IoT is being used has a crucial role in maintaining the economic stability of European industry and should be certified to reflect EU interests and values.
- EU policy and regulatory tools are needed to ensure cybersecurity and trust in the IoT, by:
  - Ensuring transparency and ethical considerations reflecting European values are integrated from the design stage, while supporting innovation and the adoption of IoT
  - Certifying cybersecurity products and services
  - Encouraging a life cycle security approach and ensuring that industry takes responsibility for cybersecurity components throughout the value chain
  - Ensuring that both public and private sector stakeholders have a clear understanding of the liability chain that is the most appropriate to manage risk in each use case.

The Internet of Things (IoT) is the main enabler for cyber physical systems, where a physical environment is tightly integrated with cyber components for monitoring and controlling the physical phenomena. IoT has been a major cross-cutting technology, including the technologies that enable communication between things or systems, so that they can exchange data acquired by sensors. However, these things and/or systems also store data, process it, take decisions and even execute those decisions through appropriate executors. Technologies like sensors/executors, communication, IoT platforms & middleware, Artificial Intelligence, wearables as well as security are implicated in the IoT.

IOT is applied in many different application domains, such as Smart Cities, Smart Energy, Smart Living, Smart Environment and Industry 4.0/Industrial Internet of Things (use of Cyber Physical Systems). It is this combination of technologies that enables the digital transformation in such a wide set of application domains, and makes IoT so critical. Given the importance of IoT and the data it generates in decisions that impact our economy across a wide variety of sectors, the use of IoT requires EU digital autonomy. The deployment of 5G as the underlying enabler for increased connectivity for IOT will increase the pressure on Europe to ensure that it achieves this autonomy.

In an IoT context, the consumer market or business/industrial, cybersecurity must be considered in a dynamic way as it depends on how a networked device is used, which can differ from the original purpose for which it was manufactured, with exposure to different risk situations. Therefore, knowing the security status of a device at delivery is not enough to guarantee its cyber-secure operations; the level of exposure to cyber-threats is always specific to the device in relation to the context in which it is deployed and used. This in turn creates a complex (and as yet unresolved) chain of responsibility.

Responsibility for security breaches could lie with the manufacturer of the IoT component, the integrators, the user or even providers of the service, and the consequences of these breaches are not just economic, but also significantly damage trust in the IoT. Moreover, attackers have used IoT to damage or disturb physical environments as well as create data breaches – in effect using IoT's vulnerabilities as a channel to attack physical and digital resources. This evolution of attack models leads to the concept of cyber-physical security, where the vulnerability assessment and impact are performed jointly between the cyber and physical components. Consequentially, the intrusion detection and prevention are performed at the cyber and physical levels.

In terms of European digital autonomy, the different stakeholders in the IoT supply chain should be able to provide evidence of the cybersecurity data and this could allow appropriate decision-making based on the comparability of cybersecurity capabilities of the IoT devices and systems.

THREATS

Various, recent studies have identified the importance of addressing cybersecurity of the IoT at the European level. As such, the September 2017 Joint Communication on Cybersecurity tackled the cybersecurity challenges of IoT Technology to ensure trust of consumers in emerging technologies and protect critical infrastructure and provides recommendations to face cyber threats. These challenges were reinforced in ENISA's November 2017 recommendations raising awareness of cyber security threats of IoT in critical infrastructures[15]. In April 2018, the European Commission's "Liability for emerging digital technologies" study[16] provided a first mapping of the liability challenges also facing IoT technology.

IoT's cyber security should not be limited to critical infrastructures, but also extends to the consumer market devices. On this market, products and connected services are produced on a large scale and used by private users with little technical or security know-how, the privacy and confidentiality of users' data plays a crucial role and should be governed by the GDPR and e-Privacy Regulation. Cyber security breaches such as the 2016 Myriad attack, involved smart consumer goods used as an army of bots producing a Denial of Service for an important Internet Service Provider. It is therefore essential that European cybersecurity solutions for devices used in non-critical applications are not forgotten, particularly given the significant impacts an attack could have for EU businesses.

As for the Industrial Internet of Things, IoT is predominantly used to enable communication between different machines in sectors like Industry 4.0, Energy, Health or Agriculture among others, and users are companies. The cybersecurity of the production process in which IoT is being used therefore plays a crucial role in maintaining the economic stability of European industry and should therefore be certified to reflect EU interests and values.

[15] ENISA, Baseline Security Recommendations for IoT, 20 November 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[16] SWD(2018) 137 final. European Commission, Commission Staff Working Document 'Liability for emerging digital technologies' accompanying the document Communication on Artificial intelligence for Europe.

OPPORTUNITIES

EU digital autonomy for IoT will be critical for maximising opportunities to build new disruptive products and/or systems based on a trusted and cybersecure IoT ecosystem for the consumer market or industrial applications.

EOS RECOMMENDATIONS

Building trust in the IoT requires convincing a broad variety of European stakeholders, policy makers, regulators and supervisors, individual and corporate users, professional organisations, trade unions and opinion makers of the trustworthiness of IoT. This involves not only making credible commitments to building privacy, security, adequate risk management and associated liability governance, as well as transparency and ethics into IoT, but also providing evidence on those commitments in practice. In this sense, self-regulatory approaches may not be enough to respond to the public demand for trust, security, privacy, ethics and transparency in IoT.

EOS recommends EU policy and regulatory tools to ensure cybersecurity of the IoT, but these must be carefully designed to support innovation and the adoption of IoT, deliver positive outcomes from the IoT, and encourage new business opportunities, as well as certifying cybersecurity products and services.

From the Industry perspective, EOS recommends that every manufacturer in the value chain takes responsibility for cybersecurity by considering security by design in their final products, from device manufacturers, machinery manufacturers, systems integrators or operators. This implies that they must ensure their systems are secure, and support the analysis of their **secure usage within value chains**, considering European cybersecurity principles.

EOS also recommends that ethical considerations reflecting European values are delivered at the design stage, and a life cycle security approach should be considered. Users should be provided with adequate transparency including on the ownership of, access to, and usage of data generated by IoT devices. Equally, all players involved should share a clear understanding of the liability chain that is the most appropriate to manage risk in each use case.

3.3 Secure data lifecycle: A Cryptography challenge

KEY TAKEAWAYS

- ❑ The greatest challenge of a Secure Data lifecycle comes from the fact that protection and usability are usually seen as antagonistic concepts.
- ❑ At the macro-level, crypto-agility, the ability to upgrade the hardware crypto layer when the quantum threat comes true, will be a critical factor in securing Europe's digital autonomy
- ❑ At the micro-level, the EU should develop recommendations on what cryptographic algorithms and key lengths are considered safe for different applications in order to raise security resilience, and to strengthen the Digital Single Market.

Data is pervasive and often becomes the most valuable asset of individuals and companies. Every system and application produce, store, analyse, consume and/or exchange data with third parties. This is especially true when we consider the increasing use of decision-making algorithms and user-assistant products, which collect and exploit personal & sensitive data on a massive scale in existing and emerging applications and services. This calls for new and improved mechanisms to protect data at rest, in transit and in use, from malevolent and unsolicited usage while ensuring data usability. The adoption of GDPR also adds to these needs the processes to demonstrate to users the actual usage that has been made of their data, creating a new level of challenges related to traceability and accountability.

The greatest challenge of a Secure Data lifecycle comes from the fact that protection and usability are usually seen as antagonistic concepts. Public standard cryptography (and its randomness ability) is known as the best and often only acceptable solution. Unfortunately, its main drawback is that it creates data that is unsuitable for wide and distributed sharing without user or systems interactivity. Digital transformation is powered by data exchanges, so innovative solutions going beyond current cryptography limitations such as Multi-Party Computation (MPC), Full Homomorphic Encryption (FHE) or Zero Knowledge Proof (ZKP), represent key contributions to address the secure data lifecycle challenge.

Ongoing advancements in physics point toward the eventual construction of large-scale quantum computers, which might be able to decrypt present-day communications, allowing anyone to decrypt data transmitted today. The scientific community is prolific and wildly excited by the ongoing quantum supremacy challenge, to develop and deploy quantum-safe cryptography, even before quantum computers are built. This field of research expands across several domains, from fundamental cryptography to hardware design. Full-stack companies, which develop technologies that can provide the end customer with a complete product or service which handles the entire value chain of its activity, are regularly emerging and claim to deliver comprehensive solutions including: manufacturing of superconducting quantum integrated circuits, chips packaging and operation in cryogenic environment and even quantum-aware software development expertise.

Achieving a general purpose and efficient quantum-computer on one hand and leading the race for the most powerful quantum processor[17] on the other are two distinct objectives for competitors seeking to achieve quantum supremacy. Significant actors in its development include Google, IBM, Microsoft, Intel, several start-ups, academic groups, and the Chinese government. In October 2018, the European Union pledged to give $1 billion to over 5,000 European quantum technology researchers over the next decade, while venture capitalists invested some $250 million in various companies researching quantum computing in 2018 alone18. Both objectives, however, generate new threats and opportunities, in a context where protecting data lifecycles using European sourced innovations represents a major enabler of our economy.

THREATS

The evolving digital ecosystem creates a continuous challenge to securing the full data lifecycle, with key threats including:

- *Privacy versus systems and user-protection* - Efficiently monitoring systems made of obfuscated and cyphered information is the next challenge security software providers, SOC, CERT and CSIRT organisation will have to tackle.
- *Lack of Data reliability* (corrupted, falsified) - As automated data processing is largely in use, the ability to distinguish or support corrupted (on purpose or accidentally) information becomes prevalent.
- *Lack of Data usability* (incomplete, obfuscated) – Weakening of the digital eco-system by lack of efficient secure data sharing solutions. For system and application monitoring, data inspection is at the heart of both behaviour analysis and pattern matching techniques. Encrypted or anonymised data weaken, and sometimes disable, existing capabilities. Security operators and tools become mostly blind to attackers.
- *Weakened Law enforcement requirements* – Alternative proposals also consider weakening strong and proven cryptographic schemes for law enforcement agencies that require specific access during investigations. Such cryptographic backdoor and key escrow infrastructures may open unexpected data breach channels in the future.
- *Post-Quantum cryptography and quantum advantage / supremacy* – Modern public cryptographic algorithms rely on hard computing problems , which could in theory be broken by a powerful hypothetical quantum computer. Currently, however, publicly known, experimental quantum computers lack the processing power to break any real cryptographic algorithm[19] but many cryptographers are designing new algorithms to prepare for a time when quantum computing becomes a threat. Indeed, it will require another decade before a 'Quantum Advantage' can be

[17] Developments in Quantum Computing and Quantum bit milestones can be followed here: http://www.qubitcounter.com/

[18] Wired. "Inside the High-Stakes Race to Make Quantum Computers Work". 8 March 2019. https://www.wired.com/story/inside-the-high-stakes-race-to-make-quantum-computers-work/

[19] Eric Gershon, "New qubit control bodes well for future of quantum computing", PHYSORG, 14 January 2013. https://phys.org/news/2013-01-qubit-bodes-future-quantum.html

achieved, where quantum machines can provide higher quality, faster, or cheaper solutions than classical computers, but the concept remains a critical target for the technical and scientific community. Once this advantage has been achieved, the real threat comes from the potential for quantum computing to be used with malicious intent and the pressure will be on cryptographers to develop post-quantum cryptographical capabilities to counter quantum cyber-attackers.

OPPORTUNITIES

Despite the threats facing the concept of a secure data lifecycle, cryptography also offers two key opportunities for improving the digital environment. The first is a technical opportunity to create trusted computing (software / hardware), develop secure multi-party data sharing protocols, advance verifiable computing, and perfect forward secrecy. The second is the opportunity to evolve governance structures able to define the various contexts of use of state-sensitive and private data and the corresponding design and technological requirements. One such avenue for development could be for the European Innovation Council to develop a Horizon Prize dedication to advancing EU cryptography as one of the major challenges facing society.[20]

EOS RECOMMENDATIONS

While continuing to protect data privacy and confidentiality, the EU should overcome the drawbacks of cryptography by developing its standing at the digital avant-garde, through the development of fluid but secure solutions for data sharing. Transforming the problem in a competitive advantage, offering infrastructure, platforms and services where added value is derived from data while preserving the highest level of protection for citizens, enterprises and public sector.

Post-Quantum research is made of several mid- and long-term milestones. Thus, hybrid solutions, that deliver the benefits of innovation in this domain while retaining full compatibility with legacy systems should be addressed by the community. Crypto-agility, the ability to upgrade the hardware crypto layer when the quantum threat comes true, will be a critical factor in securing Europe's digital autonomy.

In order to raise security resilience and to strengthen the Digital Single Market, the EU should give direction or recommendations on what cryptographic algorithms and key lengths are considered safe for different applications. A regularly updated report or paper (produced, e.g., in partnership with Academia) would work as a guideline for both public and private sector when implementing systems that rely on cryptography – from encryption per se to implementing password in a domain or to managing file-sharing in an organization.

[20] European Commission. "Prizes". May 2019. https://ec.europa.eu/research/eic/index.cfm?pg=prizes_aid

3.4 Artificial Intelligence

KEY TAKEAWAYS

- ❑ EU regulators have yet to prioritise the regulation of cybersecurity of AI-systems in Europe despite strong reference to the security-related aspects of AI applications in the 2018 AI Strategy.
- ❑ A comprehensive approach to AI in Europe should include EU standards for AI (cyber)-security applications, and R&I activities targeted at the security domains
- ❑ Defining a longer-term action plan on AI beyond the next MFF is needed to protect EU AI-dependent security systems and applications from emerging cyber threats, maintain a leading EU position on the global AI market.
- ❑ Evolving the European AI Alliance to include a formal and prominent role for the European security industry and research community, to ensure EOS technological expertise is mobilised to address security concerns more effectively.

The digital transformation of the security ecosystem requires the processing of large quantity of data to produce actionable information necessary to respond to the threats in a timely manner. AI is increasingly being relied upon in the European security domain for cybersecurity, border management, public space and critical infrastructure protection, and transport security. These fields require their systems to operate in a secure and dependable manner and, increasingly, utilise AI-based predictive and response capabilities. Considering the sensitive nature of such intelligent systems, Digital Autonomy in AI-based technologies for security applications and operations is vital to the sovereignty of Europe's digital environment, even more so in the cybersecurity ecosystem. In fact, automated attacks conducted by sophisticated AI software require effective capabilities of detection and response that can be provided only by equally advanced AI-based systems.

The European Commission's 2018 Communication on Artificial Intelligence, outlined support for AI technologies for security, reinforced the importance of AI in cybersecurity, and highlighted the security risks posed by AI used for criminal activities or attacks.[21] This Communication underpinned the vision behind AI, which is based on three pillars: (i) increasing public and private investments in AI to boost its uptake, (ii) preparing for socio-economic changes, and (iii) ensuring an appropriate ethical and legal framework to strengthen European values.

On the basis of the third pillar, on EU Digital Day 2019, Commissioner Mariya Gabriel pointed out the added value of EU Artificial Intelligence strategy: 'Human-Centric AI'. AI systems need to be human-centric, resting on a commitment to their use in the service of humanity and common good. In the

[21] COM(2018) 237 Final. Artificial Intelligence for Europe? 25 April 2018. In the Communication it is clearly mentioned that "Testing of and experimenting with AI products and services is crucial to make them market ready, ensure compliance with safety standards and rules as well as security by design and enable policymakers to gain experience with new technologies to devise suitable legal frameworks."

framework of the "Ethical Guidelines for a Trustworthy AI" published the 8th of April 2019, the AI-HLEG (Artificial Intelligence High-Level Experts Group) set up in 2018 by the Commission, identified Trustworthy AI as a fundamental ambition. As the AI-HLEG reports, a trustworthy AI must be completely compliant with the law, ethical and robust from both a social and a technical perspective.

The truly innovative capacity of the EU strategy can be found in the identification of four ethical imperatives which all AI practitioners must follow: 1) Respect for Human Authority; 2) Prevention of harm; 3) Fairness; 4) Explicability. For the security domain a crucial component is technical robustness, which is closely linked to the principle of prevention of harm. Technical robustness requires that AI systems be developed with a preventative approach to risks and in a manner such that they reliably behave as intended while minimising and preventing unintentional and unexpected harm. This should also apply to potential changes in their operating environment or the presence of other agents (human and artificial) that may interact with the system in an adversarial manner, which may therefore include cyberthreats.

Indeed, in terms of addressing the cyberthreat to AI systems, the Commission's Coordinated Plan on AI[22], prepared with Member States to foster the development and use of AI in Europe, notes that "*the increasing potential and sensitivity of AI applications in many areas of the digital economy and society, […]means it is highly relevant to establish cybersecurity requirements for AI*."

AI tools, such as deep-learning systems are even crucial to the future work of public administrations. Member States and the Commission are discussing areas for joint procurement of AI solutions, including for cybersecurity, as well as specific challenges for the public sector. When AI is implemented for security and law enforcement, legal and ethical challenges arise, considering that public administrations are bound to act as prescribed by law, that they need to motivate their decisions and that their acts are subject to judicial review by administrative courts.

In terms of investments, on 6 June 2018, the Commission published its Proposal for a Digital Europe Programme (DEP), which allocates €2.5 billion under the next Multi-Annual Financial Framework 2021-2027, to help spread AI across the European economy and society. Following the speech of Commissioner Gabriel, investments in AI will have strongly increased by 2020.

THREATS

European Digital Autonomy for securing its AI technologies is not simply a question of Europe enhancing its position in an expanding global market. Rather, it comes as a result of AI technologies increasingly being relied upon to support Europe's critical infrastructures and strategic interests. AI technology providers, therefore, have a significant role to play in protecting European security, and ensuring that AI cyber security technologies are supplied by European providers will add a layer of strategic security in these critical environments. Protection of AI software and data sets from external attacks is of utmost importance to avoid tampering aimed at disabling the systems or distorting their operational behaviour. Yet, European regulators have yet to place the cybersecurity of AI-systems in Europe as a priority action

[22] COM (2018) 795 Final. Coordinated Plan on Artificial Intelligence. 7 December 2018.

for regulation, despite strong reference to the security-related aspects of AI applications in their 2018 strategy.

AI systems, like all software systems, need to be protected against vulnerabilities that can allow them to be exploited by adversaries, such as hackers. Attacks may target the data (data poisoning), the model (model leakage) or the underlying infrastructure, both software and hardware. If an AI system is attacked, e.g. in adversarial attacks, the data as well as system behaviour can be changed, leading the system to make different decisions, or causing it to shut down altogether. Systems and data can also become corrupted by malicious intention or by exposure to unexpected situations. Insufficient security processes can also result in erroneous decisions or even physical harm. For AI systems to be considered secure, possible unintended applications of the AI system (e.g. dual-use applications) and potential abuse of the system by malicious actors should be considered, and steps should be taken to prevent and mitigate these. In addition, processes to clarify and assess potential security risks associated with the use of AI systems, across various application areas, should be established. The level of safety measures required depends on the magnitude of the risk posed by an AI system, which in turn depends on the system's capabilities. Where it can be foreseen that the development process or the system itself will pose particularly high risks, it is crucial for safety measures to be developed and tested proactively.

Another relevant concern for AI is its use in the development of lethal autonomous weapon systems (LAWS). The EU's AI Strategy includes a section on the "Security-related aspects of AI applications and infrastructure, and international security agenda" which highlights the following: "*The application of AI in weapons systems has the potential to fundamentally change armed conflicts and therefore raises serious concerns and questions. The Union will continue to stress that international law, including International Humanitarian Law and Human Rights Law, applies fully to all weapons systems, including autonomous weapons systems, and that States remain responsible and accountable for their development and use in armed conflict. The EU's position further remains that human control must be retained in decisions on the use of lethal force and built into the full life-cycle of any weapons system*." Yet, mitigating the cyber vulnerabilities of AI systems are not addressed specifically in the context of the development of these autonomous weapons, nor are the Union's digital autonomy when it comes to autonomously providing the technologies and skills exist to counter cybersecurity threats in these emerging technologies.

Consideration must also be given to countering threats posed by AI-enabled systems employed by malevolent actors. Without capacity and capabilities to combat such cyber-attacks autonomously, European Members States and economies, remain vulnerable to attacks, or are reliant on cyber security measures developed by those who do not hold European security and strategic interests as a priority.

OPPORTUNITIES

AI can significantly improve people's lives and bring major benefits to our society and economy through better healthcare, more efficient public administration, safer transport, a more competitive industry and sustainable farming. The European security ecosystem is one significant area that will inevitably benefit from the addition of AI capabilities to its security technologies, if these can be equipped with effective and trusted cybersecurity protection.

AI, if designed and used securely, could become a central technology that could empower law enforcement authorities and end users to face effectively the new challenges, including in criminal use of digital technologies, and the growing quantity of information and data that law enforcement are required to be process in the course of their duties. AI could prove to be used in the following areas:

1. **Big Data analysis:** AI tools can be used to analyse content of a victim's mobile phone. Drawing data from this mobile device, AI can highlight the communication patterns and index the objects captured in the victim's images, making data collection and interpretation more manageable for identifying suspects and understanding events. Moreover, Data Analysis could prove to be beneficial also in the field of the fight against fraud and money laundering. Insurance company can deploy AI to illuminate patterns of fraud .
2. **Predictive and pro-active policing:** Currently, in Germany Precobs[23] is used to forecast the commitment of "near repeat crimes" for crimes like robbery, and motor vehicle theft. According to authorities, number of committed crimes diminished by 30% as compared to the previous year. Similar results were achieved in certain areas of Bavaria, where the numbers decreased by between 17.5 % and 42%.
3. **Image analysis**: Now Video Content Analytics (VCA) technology is helping law enforcement realize the full value of their video surveillance investments. By processing video and breaking it down into objects and behaviours that appeared, VCA enables law enforcement to search through more video evidence more efficiently, achieving results while dedicating fewer officers to video investigation. For instance, when multiple cameras cover the expanse of a crime scene, recording the area from every angle, the investigators can process all the video and search for evidence. Whereas having to manually review this video would require prioritizing which recordings and feeds to evaluate, with VCA, officers can leverage all the data at their disposal without having to dedicate significant manpower or time to the task. By utilizing video from multiple local sources, captured over the days leading up to the incident, law enforcement officers can effectively track suspects' movements at and around the scene, identify corroborators and help focus the investigation efforts to the relevant targets.
4. **Facial and object recognition**: Facial recognition is undergoing trials at airports to help move people through security more quickly. The London Metropolitan Police has started to use the tool to narrow their search for criminals. The system is not yet perfect, but it is still used as a supporting tool.
5. **Scanning social media** for illicit activities (like terrorist content or for individuals who might be radicalised) the New York Attorney General's Office co-authored research on a new pre-investigative method, developing a sophisticated algorithm of classifiers that searches hashtags and recent activity indicative of drug dealing. Once a target is identified, the technology passes that information along to the physical enforcement team to investigate.24
6. **Countering online child sexual exploitation**

[23] IfmPt. Home page. May 2019. https://www.ifmpt.de/

[24] Yang, Xitong and Luo, Jiebo. "Tracking Illicit Drug Dealing and Abuse on Instagram using Multimodal Analysis. University of Rochester. 25 May 2016. https://arxiv.org/pdf/1605.02710.pdf

7. **Robotics:** AI in this field could have a series of applications. Robots can be used to detect and deactivate bombs. Their functions are becoming increasingly sophisticated. Often, forces will send in robots to investigate explosive devices to determine whether a threat is a valid one. Soon, however, experts expect police robots will be able to deactivate bombs in addition to aiding in their detection. This capability seems more than plausible when you consider Dallas police recently made history when they used a robot to kill an active shooter. Moreover, AI could be helpful in using drones for surveillance and control crowds. As fascinating as that is, it's worth noting that surveillance drones powered by AI will soon be able to predict crimes before they occur with tools such as facial recognition software (to identify those with criminal records) and machine learning software (to determine when to report suspicious activity)
8. **Security Screening and Detection**: As technologies evolve to detect ever more specific security threats being carried by people and vehicles (including drones) such as explosives and weapons, so too increases the need for accurate and expert screeners to assess risks and mitigation strategies. AI as a technology is increasingly being incorporated into these screening and detection technologies to improve detection rates, resolve false alarms, and thereby reducing the need for a human factor in the decision-making process around threat detection and risk assessment.
9. **Cancer detection**: AI has increasingly been used to decrease the current false negatives rate that is between 20 to 30% when based only on the human analysis of mammography tests. Combining the use of AI with correlation between medical history and test results is bringing the detection accuracy to unprecedented rates – a key evolution in the health domain.

However, it is important to retain a certain degree of strategic autonomy in the development and deployment of cybersecure, AI-enabled systems employed within the European security ecosystem, particularly in an era of shifting political and trade alliances, where market access may not remain as stable in future. By developing European digital autonomy in AI-enabled systems, Europe can compete equally on the global market with the US, and China.

EOS RECOMMENDATIONS

EOS strongly encourages the establishment of EU standards for AI security applications, particularly from a cybersecurity perspective, as well as R&I activities targeted at the security domains, which are crucial to a comprehensive approach to AI in Europe.

As well as the proposed AI investments under the next EU MFF, a longer-term action plan on AI is essential if Europe is to establish the capabilities to protect its AI-dependent security systems and applications from emerging cyber threats and maintain a leading position on the global AI market. The level of investment in AI should be analysed, at a time where non-European led initiatives are being created . For example. MIT has committed $1 Bn to handle the challenges and opportunities of AI. [25]

[25] Massachusetts Institute of Technology. "MIT News: MIT reshapes itself to shape the future." 15 October 2018. http://news.mit.edu/2018/mit-reshapes-itself-stephen-schwarzman-college-of-computing-1015

EOS supports the establishment and development of the European AI Alliance, and calls for the European security industry and research community to maintain a formal and prominent role within the Alliance to ensure security concerns are addressed and EOS technological expertise is mobilised effectively.

3.5 Cyber Security as a Service

KEY TAKEWAYS

- Software security assessment and cyber threat intelligence require high specialization and constant updates and are well suited to the cybersecurity 'As-a-Service' model, particularly in a digital ecosystem where products , systems and information are assembled from variously sourced components.
- EU policymakers and industry must provide practical tools to cybersecurity product and service developers, in the following key areas:
  - Address the definition of cybersecurity assessment targets, including in the scope differential assessment;
  - Include the creation and validation of proper audit trails for intrusion detection, impact assessment and forensics in software security assessments;
  - Establish links with training programs to ensure that certified components and services are properly developed and operated.
- The European Institutions should incentivise and support the adoption of genuine EU threat intelligence services, promoting their adoption both at public and private level and giving a specific relevance to such services within the EU operational agencies and institutions.
- European customers should be helped to trust cybersecurity services with the creation of an innovative certification framework applicable to the wide diversity of cybersecurity services, thereby developing a 'best of breed' EU cyber security industry, and maintaining EU autonomous cybersecurity protection capabilities.

ICT components are increasingly emerging as services, from Cloud infrastructure (hardware and software) to network connectivity, and cybersecurity should be considered as a valuable, emerging platform for services too. The development of cybersecurity as a service is strategic at several levels:

- Relying on European Managed Security Service Providers (MSSP) provides benefits such as access to the latest, strategic information, and ensuring confidential oversight of current and emerging cyber-vulnerabilities and attacks;
- 'As-a-Service' life cycles increase the speed of adoption of the latest innovations for coherent cyber security solutions at every stage (protection, detection, remediation). Furthermore, considering the challenge of cybersecurity deployment, the 'as-a-service model' could address the dual challenges of scalability and skills issues.

While most types of cybersecurity activities could be provided, at least in part, as a Managed Security Service, (including Identity and Access Management as a Service, Key Management as a service,

IDS/firewalls, monitoring, log analysis,…) there are two areas that are particularly suited to this approach: software security assessment and threat intelligence (as already mentioned in 3.1).

Software security assessment is in fact challenging for three key reasons: access, coverage of end to end processes and the need for upgrades. With respect to access, the complexity of current developments makes in-depth, holistic understanding of some fundamental IT technologies, for example hardware or operating systems, completely out of reach to anyone but their developers. With respect to end-to-end processes, the assessment has to be done in the context in which software is deployed and used – two dimensions that complexify the assessment process to covering the actual attack surfaces. With respect to the need for upgrades, digital technologies are being introduced and deeply woven into new or existing systems and services, providing benefits such as energy efficiency, but also introducing new vulnerabilities and thus new risks as they are updated and reconfigured.

In this digital ecosystem, where products and systems are assembled from variously sourced components, assessment is quickly becoming a pivotal part of a digital autonomy strategy, and, requiring high specialization and constant update, is particularly suitable for an 'As-a-Service' approach.

THREATS

Without European capabilities for the assessments of cybersecurity tools and services, risk assessments and thus suitability are increasingly difficult, to the point of being economically impractical or technically impossible. Procurement strategies are unable to rely on "ground truth" evaluations, and SMEs cannot quantify their cyber-risk.

OPPORTUNITIES

Industrial and institutional actors can build on the strengths of the European cybersecurity risk assessment community to scale its approaches to dynamic and elastic systems, adapting techniques and investigating new avenues, including the use of adaptive security. This will contribute to building Europe's capabilities to ensure continuous trust in European and foreign-sourced components, systems, and services.

As introduced in section 4.1, the adoption of 'As-a service' solutions for cyber threat intelligence delivery is fundamental for SMEs but also for government agencies, critical infrastructure operators, and large enterprises with limited internal digital skills or limited budgets for specific cyber protection activities. Even for those organisations that do have the complete skills at their disposal, keeping up to date over the full range of complementary services diverts important financial and operational resources from the core business of the organisations. The diffusion of cyber security services in Europe will generate a more consistent ecosystem within all EU economies and societal layers contributing to strengthening threat-intelligence sources and dynamic knowledge base and thus reinforcing the global preventive security against the cyber-attacks.

Following the strategic direction of the EU Cybersecurity Act, an autonomous EU certification framework should enable customers to distinguish cyber-secure MSSP' services & solutions. The 'As-a-service' model should therefore be reinforced both towards the developers of innovation and towards the users.

EOS RECOMMENDATIONS

EOS recommends that European institutions and industry focus on providing practical tools to **cybersecurity product and service developers**, in the following key areas:

- Address the definition of cybersecurity assessment targets, including in the scope differential assessment;
- Include the creation and validation of proper audit trails for intrusion detection, impact assessment and forensics in software security assessments. They should also include in their scope the capability to go beyond risk assessments of components and products, but also complex services, to consider a more comprehensive component-based approach;
- Establish links with training programs to ensure that certified components and services are properly developed and operated.

In terms of innovation programs, the EU should address six challenges:

1. Developing more agile software security assessment and certification frameworks, similar to agile development.
2. Enabling automation by supporting developers in writing requirements and executing tests.
3. Defining the assessment of systems of systems and end-to-end processes, beyond individual components, and modularizing assessment to enable assessment of complex systems and services.
4. Creating lifetime dynamicity of cybersecurity environments that may have long lifespans, but where individual components might be replaced or upgraded.
5. Developing framework execution elasticity, particularly for services.
6. Developing advanced capabilities in terms of digital information crawling, cyber-related big data management and supporting hardware architecture, smart analysis tools, dispatcher and graphical user interphases for cyber threat information, also aligning with other initiatives on high-performance computing, AI, big data analytics, etc.

EOS recommends that tentative solutions to these challenges should be demonstrated over use-cases of increasing complexity.

Moreover, the European Institutions should incentivise and support the adoption of genuine EU threat intelligence services, promoting their adoption both at public and private level. Giving a specific relevance to such services within the EU operational agencies and institutions should also be an important sign of the importance given to such aspects of the cybersecurity domain.

Considering the wide diversity of cybersecurity services, the necessity and opportunity to develop a 'best of breed' EU cyber security industry, and maintain EU autonomous cybersecurity protection capabilities, **customers should be helped to trust cybersecurity services** with the creation of an innovative certification framework applicable to services.

4. CONDITIONS FOR REGULATORY SUCCESS AND COMPLIANCE

KEY TAKEAWAYS

- ❑ EU Digital Autonomy policy initiatives should continue to carefully balance over-regulation and laissez-faire approaches, and follow the principle of technology-agnostic regulation.
- ❑ EU Cybersecurity measures need to address ways to effectively share responsibility across the supply chain, including discussing extending the chain of liability to the end user.
- ❑ More efforts should be placed in developing EU cybersecurity intelligence capabilities, early warning and rapid information exchange system about the vulnerabilities and risks
- ❑ Minimum EU standards and a clear security by design approach are needed in domains such as critical infrastructure protection, supply chain management, as well as e-governance.
- ❑ The EU should strive for further MS policy harmonisation, taking a stronger role in cybersecurity through comprehensive policies such as promoting collective cybersecurity measures.

The EU's strategic goal is to build greater resilience and strategic autonomy in order to retain and develop essential capacities for securing its digital economy, society and democracy. Considering the proposals EOS has identified in this paper, EU digital autonomy policy must also address the best conditions for regulatory success and compliance to enable European cybersecurity actors to operate effectively.

The EU has made significant progress in reaching agreement on fundamental principles and outlining a set of shared strategic interests which are the foundation of effective cyber security governance. Existing legislative tools as well as institutionalised actors are identified to facilitate reaching a more harmonised status of European capabilities. However, the numerous challenges listed in this concept paper indicate a clear need for extended and in some cases new measures to speed up the implementation of a cyber-secure Europe, as well as an increased support to face emerging priorities.

THREATS

One of the foundations of EU's digital autonomy is a stable regulatory environment which nurtures investment in innovation, research and development, and novel technologies. Key technologies such as AI and robotics require stepping up **investments from both public and private sectors**, especially when compared to the markets in China and the US. Without boosting the EU's technological and industrial capacity, the EU risks **losing out on the opportunities offered by these new technologies, increasing on**

brain-drain and eventually becoming a consumer of solutions developed elsewhere.[26] As developed in this paper, this will in effect move Europe's economy totally out of its control.

OPPORTUNITIES

One of the options to enhance the current legislative landscape would be analysing options for **institutional and/or procedural mechanisms,** which would decrease the time needed from proposal to an adopted legal framework. Also, as in any other field, successful regulatory and compliance efforts need to continue to be undertaken in **constructive dialogue with various stakeholders** such as the industry and academia. Since its inception over a decade ago, EOS has established itself as a trustworthy partner in echoing the views of its the security industry and research community, and will keep on building on the efforts taken by EOS Members in providing valuable insights to the regulatory processes so far.

EOS RECOMMENDATIONS

Existing legal tools include several provisions on monitoring, information sharing and risk assessment. GDPR is a great example of incentives for making different actors across the EU more compliant with data protection principles. Upcoming regulatory initiatives should continue to **carefully balance over-regulation and laissez-faire approaches** and follow the principle of **technology-agnostic regulation,** which would ensure the adoption of future technologies.

We suggest that existing cyber security measures as outlined in the EU regulatory documents (such as the NIS directive) should be **reinforced and their deployment further encouraged**. Here, one of the key issues remains to identify ways to effectively **share responsibility** across the supply chain, including discussing extending the chain of liability to the end user.

The EU should also investigate **defensive measures** such as screening companies and service providers, and blacklisting companies which introduce vulnerabilities into their systems.

While it may prove to be impossible to have regulatory control over all the components involved in critical and complicated **supply chains**, more efforts should be placed in **developing intelligence capabilities, early warning and rapid information exchange system about the vulnerabilities and risks**. In this regard, the regulatory incentives should be designed with the purpose of building and maintaining **trust** among various EU cybersecurity actors, without which the sharing mechanism that underlies successful cyber security protection will never become reality. As importantly, innovation and progress should be fully inserted in this control approach, to ensure that it is encouraged but avoiding its uptake to be done at the expense of increased risks.

Equally, there is a need for a **minimum set of standards** and a clear security by design approach in various interrelated domains such as critical infrastructure protection, supply chain management, as well as e-governance. To that end, the European cybersecurity **certification schemes** would serve the purpose of gaining confidence in the security of these technologies and ease carrying out business across borders.

[26] COM(2018) 237 Final. European Commission Communication on Artificial Intelligence for Europe? 25 April 2018.

The certification scheme should however be based on a component approach that takes into consideration a process approach – based on the feasibility of its effective uptake in terms of coverage, cost and impact.

The EU should continue to promote the **development and procurement of EU security technologies**, encouraging the development of new technologies such as AI, IoT, blockchain and others, and investing in research and development. **Foreign investments** in EU technologies should be carefully reviewed, with the proposed European framework for screening foreign direct investments serving as a welcome initiative.

Keeping in mind the above and with the aim to strive for further harmonisation, **EU should take a stronger role** in cybersecurity and aim for comprehensive policies such as promoting collective cybersecurity measures, e.g. sharing information on vulnerabilities, building circles of trusted stakeholders for more effective information sharing, encouraging volunteers to locate bugs in open source code and other critical systems.

The EU should move towards **greater coordination and coherence among Member States and other cybersecurity actors**, including industry stakeholders such as EOS and ECSO, in terms of strategic directions, investments as well as capacity building efforts, training and awareness raising. The emerging EU Competence Centre should provide this coordinating body for EU cyber capability development as there is the threat of fragmented domestic approaches having an impact on EU's overall position on the global cybersecurity arena. The role of industry in this coordination should be fully defined.

Finally, given the strategic importance of cybersecurity to ensure European digital autonomy to protect European values and promote them worldwide, EOS strongly recommends that the EU play a more prominent leading role in establish effective cybersecurity governance globally.

5. EOS CONCLUSIONS

For EU's leaders to successfully deliver on their 2017 ambition to transform the Union into a global leader in cyber-security by 2025, significant evolution of the European cybersecurity policy and collaborative environment needs to take place. At the forefront of this change must be the comprehensive and effective incorporation of initiatives to strengthen the Union's digital autonomy, ensuring independent, meaningful and future-proof capabilities to combat contemporary and emerging cyber-threats.

It should be highlighted that EU digital autonomy is not a binary state (of either having autonomy or not) but rather a spectrum that represents different degrees of autonomy and dependency. An autocratic European approach to cybersecurity is extremely difficult to achieve and is at risk of being counter-productive, and a structured global cooperation model will be more effective for the EU to mitigate cyber-threats that impact Europe but originate anywhere in the world (including in Europe). For European cybersecurity to reach the ambitious goals set out by EU policymakers, the balance of European digital and cybersecurity capacity and capabilities needs to shift away from its current reliance upon third countries, and develop more autonomous abilities to ensure the security of the EU cyber and physical environments.

EOS strongly supports the European Commission's initiatives to evolve the EU digital policy framework to ensure more autonomous cybersecurity capabilities. The question remains, **what are the practical measures to be incorporated or further developed within European policy?**

While the full series of EOS recommendations are explored in the chapters above, three key themes emerged for consideration by European policymakers, which are worth highlighting:

1. **An EU legal act to define priority investment areas and drive European Digital Autonomy forward is critical to overcoming current dependence on other regions' technologies and services.**
2. **Designing and implementing activities for achieving European Digital Autonomy requires a roadmap with concrete benchmarks keeping in mind the challenge of effective coordination between governmental and industry stakeholders on domestic and regional levels.**
3. **Further regulatory steps may be necessary for addressing Member States' fragmentation in implementing existing EU Digital policies, keeping in mind both the end-users and industry.**

As the voice of the security industry, EOS proposes to monitor the impact of the strategic choices made on the ethical, economical and sustainability domains and remains ready to share industry expertise; and, through the implementation of the recommendations elaborated in this position paper, we look forward to helping European policymakers to fully realise a successful outcome for the future of EU digital autonomy.

European Organisation for Security (EOS)
10 Rue Montoyer, 1000 Brussels, Belgium | www.eos-eu.com
EOS is registered at the EU Transparency: 32134385519-64