CONCORDIA DELIVERS

INTRODUCTION

Nowadays, we are facing multiple crises that impressively demonstrate the dependency of our modern digital society on secure and trustworthy ICT (information and communication technology). Technologies like big data, artificial intelligence, quantum, or biotechnologies – emerging and disruptive technologies (EDT) – are advancing rapidly and present risks and opportunities. Developing responsible, innovative, and agile EDTs reflecting our core values is critical. Europe today stands for a high level of data security and data protection. The EU is probably the most trusted area in the world regarding these issues. This is a significant competitive advantage that must be maintained and built upon.

Speeding up innovation, reducing dependencies (not only gas and oil), increasing risk-tolerant investment strategies, and taking a visionary and courageous step towards European digital sovereignty or strategic autonomy, accompanied by appropriate regulation, are objectives that need to be faced. Ultimately, it is a value decision, but one that must be realized against the backdrop of technology with a power developing exponentially. Thus, strengthening technological capabilities and developing digital infrastructures are topics that need to be addressed as well.

Cybersecurity is fundamental for our digital society. The threat landscape is evolving, however, with tremendous speed. We are facing an extremely fast-growing attack surface with a diversity of attack vectors, an apparent asymmetry between attackers and defenders, billions of connected IoT devices, primarily reactive detection and mitigation approaches, and finally, big data challenges. The clear asymmetry of attacks and the enormous amount of data demand to rethink cybersecurity approaches in terms of reducing the attack surface, to make the attack surface dynamic, to automate the detection, risk assessment and mitigation, and to investigate the prediction and prevention of attacks with the utilization of artificial intelligence and machine learning. Besides technological aspects, building multistakeholder ecosystems, strengthening cooperation, and avoiding fragmentation and silo thinking are other vital issues.

The CONCORDIA results are contributing to mentioned objectives such as building with leading research, technology, industrial and public competences a European Secure, Resilient and Trusted Ecosystem.

We structured our 20 outcomes into five categories – Policy, Tools, Education, Pilots, and Certification. The sixth category is focused on Research and contains 28 selected publications.

The contribution of the CONCORDIA project is not limited to these highlighted outcomes. Please check the official deliverables (*concordia-h2020.eu/deliverables/*) to understand what we delivered in the CONCORDIA project.

Gabi Dreo,
CONCORDIA Project Coordinator

I. POLICY

1. CONCORDIA ROADMAP FOR EUROPE

What is it and what is it intended for?

What action should Europe take to build and sustain resilience and digital sovereignty?

CONCORDIA devised the Cybersecurity Roadmap for the EU, which defined fundamental challenges and recommendations in nine dimensions.

- → Threat Landscape
- → Research and Innovation
- → Education and Skills
- → Economics
- → Investments
- → Legal and Policy
- → Certification
- → Standardization
- → Community Building

Why is it important/what are the benefits?

Europe is challenged by the US and China. To avoid the fate of a digital colony, we must act now and build, achieve, and sustain European Resilience and Digital Sovereignty.

The purpose of this Roadmap is to both identify and jointly work to addressing, mitigating (and even resolving) the challenges regarding European digital sovereignty while identifying and joining European brainpower and forces to build, boost and amplify the gains of (the road towards) building, achieving and sustaining European digital sovereignty.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/roadmap

2. WOMEN IN CYBERSECURITY INITIATIVE

What is it, and what is it intended for?

Women in Cybersecurity initiative is a CONCORDIA task implementing actions to incentivise women to join the field of cybersecurity. We created a Women in Cyber – A Manifesto for TODAY, a document stating CONCORDIA's objectives for women's inclusion. To **achieve these goals, we focused on three types of actions**, which are Diversity&Cybersecurity webinars, Awards for Women in Cyber or Women in Cyber role models gallery of postcards.

Why is it important/what are the benefits?

Gender diversity brings benefits, such as obtaining a different perspective on the workplace or attitude towards risk. The cybersecurity field is often perceived as male-dominated. Therefore it doesn't encourage women to join in. Our initiative attempts to reverse this, motivate women, and support them.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/womenincyber

3. CONCORDIA NETWORK

What is it, and what is it intended for?

While working on the project, we were able to build a community and establish a liaison with stakeholders. Different institutions represent different competencies and, with their different levels of involvement, that's why we introduced three stakeholders groups involved parties could join: National Cybersecurity Competence Centers and Agencies Stakeholders Group (NSG), Observer Stakeholders Group (OSG) and Liaisons Stakeholders Group (LSG). We reached more than 500 people in 300 European organizations that relied on us to inform them. We did so, for example, by sending a newsletter every three months, providing security expertise, doing cybersecurity research, joining discussions in European institutions or organizing the CONCORDIA Open Door event every October.

Why is it important/what are the benefits?

Cooperation is essential to achieve the sustainability of the outcomes and for the collecting integration of concrete feedback. Provided tools have strengthened European Digital Sovereignty. It also helped to manage cybersecurity activities and propose a direction for cybersecurity action in Europe.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/network

II. TOOLS

4. KYPO CYBER RANGE PLATFORM

What is it and what is it intended for?

KYPO Cyber Range Platform is a flexible, scalable, and sophisticated virtual environment.

It has been developed by Masaryk University since 2013. The platform represents several years of experience using cyber ranges in education, cyber defense exercises, and training.

The CONCORDIA project released KYPO CRP as open-source in 2020. This activity aims to help solve the high amount of missing cybersecurity experts by providing a platform for the development, and execution of cybersecurity training and exercises.

Why is it important/what are the benefits?

We believe that KYPO Cyber Range Platform is a significant contribution to the cybersecurity community. The open-source cyber range makes hands-on cybersecurity education widely available for universities and organizations in Europe and around the world.

We perceive the release of an open-source cyber range as part of CONCORDIA strategy to build and sustain European resilience and digital sovereignty.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/kypo

5. CYBERTEA

What is it, and what is it intended for?

To build a comprehensive European cybersecurity ecosystem, we focus on cybersecurity's technical and economic aspects. Our proposed CyberTEA defines a clear methodology for cybersecurity planning and investments. For that, it integrates a set of tools to help decision-makers during the different planning steps. Examples of these tools include (i) SECAdvisor, a tool to calculate the optimal investment in cybersecurity based on different economic models like Gordon-Loeb and ROSI, (ii) MENTOR, a system that supports cybersecurity management to recommend services for the prevention and mitigation of cyberattacks, and (iii) SecBot, which is a conversational agent that focuses on helping non-experts users to make informed and efficient cybersecurity decisions.

Why is it important?

CyberTEA was created to guide decision-makers in cybersecurity planning and investment, especially in scenarios where there are limitations of budget and a lack of in-house technical expertise. CyberTEA defines all of the steps and artifacts needed for each step in order to achieve a cost-efficient cybersecurity plan. The tools available as part of the CyberTEA make the applications of cybersecurity economic modes less complex, the decision of cybersecurity actions more effective and faster, and cheaper to implement an adequate level of cybersecurity in companies. Also, CyberTEA highlights opportunities and challenges for the next generation of cybersecurity solutions, showing the direction for the development of solutions that simplifies and helps the massive cybersecurity adoption within companies.

Where can we find more information about it?

https://www.concordia-h2020.eu/delivers/cybertea

6. GORILLA CYBER DETECT

What is it, and what is it intended for?

Gorille is an innovative malware detection tool developed by the start-up Cyber-Detect in collaboration with the University of Lorraine. Gorille can identify the most sophisticated attacks that bypass traditional defence systems based on morphological analysis. It also allows precise identification of malware families and can address significant attack analysis and remediation tools.

Why is it important/what are the benefits?

Gorille can provide complete and instantaneous characterization to inform analysts about the attack. It guarantees relevant and fast analysis. Gorille helps to reduce risks and minimize exposure to future claims.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/gorilla

7. QUIC FLOWMON PROBE PLUG-IN

What is it?

Flowmon Probe QUIC plug-in – capability to identify QUIC traffic in the network, extract server name indication (SNI) from handshake and export the SNI as part of enriched metadata using IPFIX protocol.

Why is it important?

QUIC is a new and emerging protocol to deliver web content to users thus the ability to understand its usage patterns are essential for network operations and network security. Ability to decrypt and extract SNI will help security professional to fight attacks and cyber threats. The result as such was recognized among top CONCORDIA project results and will be published on the EU Innovation Radar Platform. Moreover, Flowmon Networks will prioritize this result and QUIC monitoring based on the result will be available to all Flowmon user and customer based as part of Flowmon 12.2 expected to be released till end of 2022.

Where can we find more information this?

https://www.concordia-h2020.eu/delivers/quic

III. EDUCATION

8. THE COURSE BECOMING A CYBERSECURITY CONSULTANT

What is it, and what is it intended for?

Based on desk research followed by a market validation, we identified a set of knowledge and skills a cybersecurity consultant should have. Accordingly, our partners and we created a course called Becoming a Cybersecurity Consultant, which is suitable for professionals, cybersecurity middle managers, and freelancers. After successfully finishing the course in full, the participants are eligible to apply for the C3 by CONCORDIA certification exam.

Why is it important/what are the benefits?

This course helped the participants to update their knowledge on cybersecurity related topics relevant to the cybersecurity consultant role profile. Over the 2 modules, the course covered topics such as anticipating new security threats, designing countermeasures, conducting capabilities and requirements analysis, or economics of cybersecurity.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/course

9. THE CONCORDIA GOVERNANCE MODEL FOR A EUROPEAN EDUCATION ECOSYSTEM IN CYBERSECURITY

What is it, and what is it intended for?

The CONCORDIA Governance model for a European Education Ecosystem in Cybersecurity is building on the experience and knowledge accumulated during the project, on several education related activities. After identifying the challenges of the ecosystem at the European and national level, and revising different cybersecurity /education related governance models, the document presents the ingredients of a possible governance model.

Why is it important/what are the benefits?

The Governance model proposed by CONCORDIA aims at supporting the European Cybersecurity Competence Centre endeavor in building and engaging with the Education related community, for the benefit of all the actors of the ecosystem.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/edugovmodel

10. THE METHODOLOGY FOR THE HIGH SCHOOL TEACHERS

What is it, and what is it intended for?

One of the outcomes of CONCORDIA is the Methodology and Guidelines to support high school teachers. The Methodology proposes an approach based on 3 steps, and suggests building a needs-based and knowledge-based modular portfolio of lessons. With more than 470 targeted resources, the Guidelines include 12 cybersafety modules, with topics such as hate speech or fake news, and 12 cybersecurity modules that can help to teach about cyber hygiene, protection of data or, for example, how a computer works. We are also pointing to related initiatives deployed in different European countries.

Why is it important/what are the benefits?

Cyberspace can be dangerous not only for adults but also children. Teaching pupils about cybersecurity and cybersafety is therefore necessary. Our methodology will make it easier for teachers to prepare to teach about these topics. We believe that its implementation in schools can decrease the risk of children being victims of cyber incidents and also can show them the importance of this topic or support their desire to work in the cybersecurity industry.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/highschools

IV. PILOTS

11. DDOS CLEARING HOUSE

What is it, and what is it intended for?

The DDoS Clearing House is a platform used for sharing measurements of DDoS (meta) data between organizations. By sharing data and expertise of DDoS attacks, organizations broaden their view of the DDoS landscape to an ecosystem wide one, which enables a more proactive and collaborative stance in fighting DDoS attacks. We piloted the system in the Netherlands and Italy, and it will be deployed in production in the Dutch anti-DDoS coalition.

Why is it important/what are the benefits?

DDoS attacks cost organizations tons of money and resources. DDoS Clearing House enables institutions to share the characteristics of the DDoS attacks they handle. With a broader scope on the DDoS landscape, organizations know better what kinds of DDoS attack are out there, and are able to better prepare for attack that have not yet hit them, in the end saving service downtime.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/ddosclearinghouse

12. FINANCIAL THREAT INTELLIGENCE PLATFORM

What is it, and what is it intended for?

CONCORDIA Financial Threat Intelligence Platform is adapted to the financial entities' needs. It provides a set of add-ons that work over MISP enhancing security and privacy when threat intelligence information between entities is being exchanged. The dashboard has several functionalities, such as defining concrete and fine-granular sharing groups to change the data and selecting encryption or anonymization details for specific IoC types and fields. It can also automate the anonymised information sharing process and score the incoming IoCs based on threats trends.

Why is it important/what are the benefits?

All the platform features allow entities to be much more flexible in the information-sharing process. We believe this solution will foster Europe's cyber threat intelligence sharing market growth. Information sharing is the key to managing and mitigating cyber risks.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/financialpilot

13. SECURITY OF VEHICULAR COMMUNICATION SYSTEMS PILOT

What is it, and what is it intended for?

In the secure communication pilot, we delivered three solutions contributing to the security of vehicular communication systems.

Firstly, we are providing lightweight, hardware-based post-quantum secure authentication as an enabler for all future interaction between vehicles.

Secondly, we developed a methodology for studying attack propagation in collaborative missions during mission design, planning and execution, and provided an implementation.

Thirdly, we delivered a fast and efficient routing algorithm to dynamically respond to communication needs.

Why is it important/what are the benefits?

These solutions help to improve the resilience of collaborative vehicles facing cyber attacks during missions by identifying potential threats early on. Also, they enable safe operation for more connected and collaborative vehicles.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/uaspilot

14. THREAT INTELLIGENCE FOR THE TELCO SECTOR

What is it, and what is it intended for?

CONCORDIA telecom sector pilot's main objective is to extend and enhance the CONCORDIA Threat Intelligence Platform with three use cases. They focus on automated processing of threat intelligence information, preventing flood attacks from IoT devices and handling privacy and anonymity with machine learning.

Why is it important/what are the benefits?

This pilot helps to reach the common goal of countering cyber-attacks towards Telecom networks. Several benefits come from each case, such as zero-day attack detection or detecting privacy violations on users' data. Overall this pilot and its specific tasks work on analyzing attack types targeting the Telco sector, collecting and sharing information about them and protecting the users and organizations from malicious cyber attacks.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/telcopilot

15. CONCORDIA MOBILE THREAT MODELLING FRAMEWORK

What is it, and what is it intended for?

Mobile Threat Modelling Framework is a compatible combination of the enterprise, mobile and ICS matrices of the MITRE ATT&CK framework. The first iteration of this framework intends to adapt and grow – as we see the need to accommodate more techniques as more attacks become known. Our perspective is to have this framework as a de-facto model for all members of the telco cybersecurity (& sharing) community.

Why is it important/what are the benefits?

CMTMF is a tool to enhance efforts and further extend the cyber threat intelligence paradigm in the telco sector. It can oversee the impact an attack or an exploit on a device connected to a mobile network can have on both surrounding devices and potentially the underlying infrastructure. The framework allows for better analyses of the ever-increasing and expanding attack types that target their infrastructures and connected devices.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/mtmframework

16. FEDERATED LEARNING AS A SERVICE: FLAAS

What is it, and what is it intended for?

FLaaS is a service that enables that enables SMEs and other third-party entities (e.g., mobile application owners) to build Machine Learning (ML) models that help their apps (e.g., for better recommendations, user modelling, etc.). Crucially the ML learning is performed on user devices, and not on the servers of the entities, using the principles of Federated Learning (FL). This means the entities do not need to collect user data at the backend (as they have been doing so far), with all the privacy implications this practice entails. Instead, they can select and train ML models on the user devices in a secure and privacy-preserving fashion. The target audience of this service are entities that may not have the resources (personnel, tech, etc.) to make this effort on their own. Interestingly, FLaaS can also enable 2 or more third-party entities to collaborate with each other to build joint ML models that serve all interested parties.

Why is it important/what are the benefits?

This service is important as it can push the ML era into the next step, which is decentralized and distributed ML. The step we have been living so far has been the ML-as-a-Service (MLaaS): companies collecting and analyzing data of users on their cloud servers and modelling their behavior. The next step is to do this using FL-as-a-Service (FLaaS): companies leaving the data at their owners (users) and using privacy-preserving ML techniques, they can build models that are still useful while protecting and respecting user privacy. We expect this market to pick-up in the next few years: there are already a dozen start-ups offering some sort of FL services for cross-silo training, and also big players such as Google, Facebook and Apple using FL inside their products, services and devices.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/flaas

17. REFERENCE ARCHITECTURE FOR E-HEALTH PILOTS

What is it, and what is it intended for?

E-health pilots work on digital transformation in the health service sector, and we mainly focus on capturing security and privacy. The first use-case is the medical devices at home that send data between home and the doctor/health care authorities via a secured communication channel. We saw it as essential to ensure digital identification of the patient, secure data storage, home infrastructure and communication – for today‘s Wifi world and the 5G near future. This use case as an open platform addresses mainly the EU citizen, as buyer and as user. Regarding intelligent and smart ambulance services, our goal was to describe reference architecture for secure real-time data and video exchange between the hospital and the vehicle along the 5G network. This use case addresses the first responder as a buyer of such a transport vehicle.

Why is it important/what are the benefits?

Healthcare is one of the most regulated areas in the European Economic Area. These pilots are focusing on securing identification, communication and infrastructure. Securing patient data and making it easier for doctors to get information on time is often crucial in this sector. The 510+ million EU citizens are not cybersecurity experts, but they are the decision maker on buying new medical edge products connected and used at or in the body of the citizen, mainly at home. CONCORDIA create guidelines for them. First responders use more connectivity in the ambulance services (helicopter, vehicle) to improve their services if the 5G network becomes more and more available. CONCORDIA collect awareness on cybersecurity for them.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/ehealthpilot

V. CERTIFICATION

18. A SECURITY CERTIFICATION SCHEME FOR INFORMATION-CENTRIC NETWORKS

What is it, and what is it intended for?

Information-centric networking is an emerging alternative to host-centric networking designed for large-scale content distribution and stricter privacy requirements. This research focused on protecting the network from attacks targeting the content delivery protocols while assuming genuine content can constantly be retrieved from trustworthy nodes.

Why is it important/what are the benefits?

In our work, we provided the security assurance methodology for information-centric networks supporting continuous security verification of non-functional properties.

We improve trustworthiness and transparency by proposing two certification processes balancing the impact on the network and the system performance.

It can be adapted for various applications, from Service Level Agreements to misbehaviour and attack monitoring.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/scsicn

19. THE C3 BY CONCORDIA SKILLS CERTIFICATION SCHEME

What is it, and what is it intended for?

C3 by CONCORDIA is a certification scheme for the cybersecurity consultant role. It is intended to be used by organizations wishing to provide evaluation and certification of the knowledge and skills of professionals based on the Cybersecurity Consultant role profile created by the CONCORDIA project. The scheme fulfils the requirements for cybersecurity skills schemes of ISO 17024.

Why is it important/what are the benefits?

C3 by the CONCORDIA certification scheme, together with the CONCORDIA Becoming a Cybersecurity Consultant course, attempt to address the lack of cybersecurity professionals by providing training and certification of cybersecurity skills. It is the first pilot of the CONCORDIA Cybersecurity Skills Certification framework. This certification scheme is the only existing following these best practices and addressing the role of the Cybersecurity Consultant.

Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/c3

20. MULTI-DIMENSIONAL CERTIFICATION OF MODERN DISTRIBUTED SYSTEMS

What is it, and what is it intended for?

The CONCORDIA participated through a number of partners in the consultation of the draft version of the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services). Certification scheme for (cloud) services awards a certificate to a service in case it holds a given non-functional property (e.g., confidentiality, integrity, availability). Services are then selected on the basis of the released certificates.

Why is it important/what are the benefits?

This scheme departs from the state of the art where services are evaluated and later certified according to their finalsoftware artifacts only (i.e., the executable service). For the first time, we extend the scope of certification to includeadditional aspects of the service to be evaluated, such as, for instance, the development process. We group these aspects in dimensions to be evaluated, certified, and managed according to the dimension's peculiarities. Our multi-dimensional certification scheme enables a new generation of service life cycle management, where services are provisioned and composed according to fine-grained certificates.

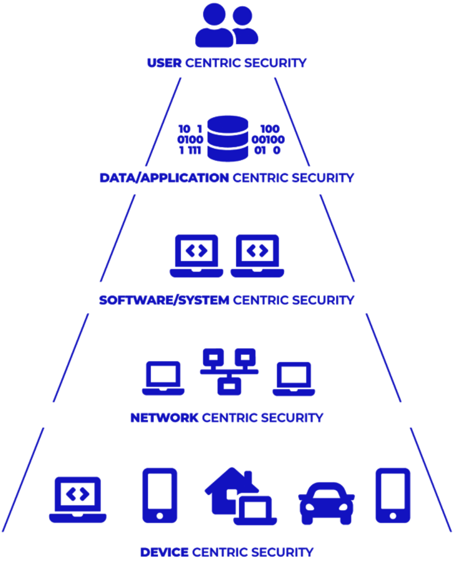
Where can we find more information about this?

https://www.concordia-h2020.eu/delivers/mdcmds

VI. RESEARCH

21. SELECTED PUBLICATIONS

Performing excellent academic research is the essential objective of the CONCORDIA project.



Our research activities are organized into five tasks, each focusing on a particular aspect of cybersecurity.

- → During the project's lifetime, we produced 324 publications. The total number of papers entered into the EU-ECAS system is even higher since white papers and papers without peer review are not counted. You can find all our publications on *our website*.
- → *concordia-h2020.eu/delivers/selectedpapers*

Security Aspects	2019	2020	2021	2022	Total
Device	10	23	19	25	77
Network	9	30	15	20	74
Software and system	8	13	4	7	32
Data and application	16	15	18	12	61
User security and privacy	16	26	20	18	80
Total	**59**	**107**	**76**	**82**	**324**

Here we present only our selection. Selected publications are all journal papers with SJR >= 2.0 and all CORE A* conference papers (excluding poster and demo papers).

DEVICE SECURITY

*1. P. Colombo, E. Ferrari, E.D. Tümer (UI): **Regulating data sharing across MQTT environments.** Elsevier Journal of Network and Computer Applications, 174, January 2021 https://doi.org/10.1016/j.jnca.2020.102907 [D1.2, SJR 2.19]*

*2. A.S. Lalos, E. Vlachos, K. Berberidis, A.P. Fournaris, C. Koulamas (ISI): **Privacy Preservation in Industrial IoT via Fast Adaptive Correlation Matrix Completion.** IEEE Transactions on Industrial Informatics 16(12), 2020 https://doi.org/10.1109/TII.2019.2960275 [D1.2, SJR 4.33]*

*3. I. Ahmed, M. Anisetti, A. Ahmad, G. Jeon (UMIL): **A Multilayer Deep Learning Approach for Malware Classification in 5G-Enabled IIoT.** IEEE Transactions on Industrial Informatics, 2022 https://doi.org/10.1109/TII.2022.3205366 [D1.4, SJR 4.33]*

*4. E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, B. Stiller (UZH): **Landscape of IoT Security.** Elsevier Computer Science Review 44, May 2022 https://doi.org/10.1016/j.cosrev.2022.100467 [D1.4, SJR 2.562]*

*5. A. Khurshid, S. D. Yalew, M. Aslam, S. Raza (RISE): **ShieLD: Shielding Cross-zone Communication within Limited-resourced IoT Devices running Vulnerable Software Stack** IEEE Transactions on Dependable and Secure Computing, 2022 https://doi.org/10.1109/TDSC.2022.3147262 [D1.4, SJR 2.265]*

*6. Y. Meidan, D. Avraham, H. Libhaber, A. Shabtai (BGU): **CADeSH: Collaborative Anomaly Detection for Smart Homes.** IEEE Internet of Things Journal, 2022 https://doi.org/10.1109/JIOT.2022.3194813 [D1.4, SJR 3.848]*

*7. Y. Sharon, D. Berend, Y. Liu, A. Shabtai, Y. Elovici (BGU): **TANTRA: Timing-Based Adversarial Network Traffic Reshaping Attack**. IEEE Transactions on Information Forensics and Security 17, 2022 https://doi.org/10.1109/TIFS.2022.3201377 [D1.4, SJR 3.299]*

*8. M. Hamad, A. Finkenzeller, H. Liu, J. Lauinger, V. Prevelakis, S. Steinhorst (TUBS): **Secure Endto-End MQTT-Based Communication for Mobile IoT Systems Using Secret Sharing and Trust Delegation**. IEEE Internet of Things Journal, November 2022 https://doi.org/10.1109/JIOT.2022.3221857 [D1.4, SJR 3.848]*

NETWORK SECURITY

*1. H. Lee, A. Gireesh, A.V. Vidyapeetham, R.v. Rijswijk-Deij, T. Kwon, T. Chung (UT): **A Longitudinal and Comprehensive Study of the DANE Ecosystem in Email**. Proceedings of the USENIX Security Symposium, 2020 USENIX Association [D1.2, CORE A*]*

2. E. Papadogiannaki, S. Ioannidis (FORTH): ***A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures****. ACM Computing Surveys 54(6), 2021 https://doi.org/10.1145/3457904 [D1.3, SJR 5.090]*

3. E.J. Scheid, B. Rodrigues, B. Stiller (UZH): ***Policy-Based Blockchain Selection****. IEEE Communications Magazine 59(10), October 2021 https://doi.org/10.1109/MCOM.100.2100120 [D1.3, SJR 5.147]*

4. A.S.M. Rizvi, L. Bertholdo, J. Ceron, J. Heidemann (UT, SIDN): ***Anycast Agility: Network Playbooks to Fight DDoS****. Proceedings of the 31st USENIX Security Symposium, August 2022 USENIX Association [D1.4, CORE A*]*

5. H. Lee, Md.I. Ashiq, M. Müller, R. van Rijswijk-Deij, T. Kwon, T. Chung (UT, SIDN): ***Under the Hood of DANE Mismanagement in SMTP****. Proceedings of the 31st USENIX Security Symposium, August 2022 USENIX Association [D1.4, CORE A*]*

SOFTWARE/SYSTEM SECURITY

1. T. Arnold, E. Gürmeri.liler, G. Essig, A. Gupta, M. Calder, V. Giotsas, E. Katz-Bassett (ULANC): ***(How Much) Does a Private WAN Improve Cloud Performance?*** *IEEE Conference on Computer Communications (INFOCOM), 2020 https://doi.org/10.1109/INFOCOM41043.2020.9155428 [D1.2, CORE A*]*

2. B. Cheng, J. Ming, E. Leal, H. Zhang, J. Fu, G. Peng, J.-Y. Marion (UL): ***Obfuscation-Resilient Executable Payload Extraction From Packed Malware****. Proceedings USENIX Security, February 2021 USENIX Association [D1.3, CORE A*]*

DATA/APPLICATION SECURITY

1. P. Colombo, E. Ferrari (UI): ***Evaluating the effects of access control policies within NoSQL systems****. Elsevier Future Generation Computer Systems 114, January 2021 https://doi.org/10.1016/j.future.2020.08.026 [D1.2, SJR 2.23]*

2. F. Daidone, B. Carminati, E. Ferrari (UI): ***Blockchain-based Privacy Enforcement in the IoT Domain****. IEEE Transactions on Dependable and Secure Computing, September 2021 https://doi.org/10.1109/TDSC.2021.3110181 [D1.3, SJR 2.265]*

3. M. Sestak, M. Hericko, T. Welzer Družovec, M. Turkanovic (UM): ***Applying k-vertex cardinalityconstraints on a neo4j graph database****. Elsevier Future Generation Computer Systems, February 2021 https://doi.org/10.1016/j.future.2020.09.036 [D1.3, SJR 2.233]*

4. M. Anisetti, C. A. Ardagna, N. Bena (UMIL): ***Multi-Dimensional Certification of Modern Distributed Systems****. IEEE Transactions on Services Computing, 2022 [D1.4, SJR 2.714]*

USER SECURITY

1. *P. Papadopoulos, N. Kourtellis, E. Markatos (FORTH, TID):* ***Cookie synchronization: Everything you always wanted to know but were afraid to ask****. Proceedings of the World Wide Web Conference (WWW). May 2019*
https://doi.org/10.1145/3308558.3313542 [D1.1, CORE A]*

2. *S. Zannettou, T. Caulfield, E. De Cristofaro, M. Sirivianos, G. Stringhini, J. Blackburn (CUT):* ***Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and their Influence on the Web****. Companion Proceedings of The 2019 World Wide Web Conference, May 2019*
https://doi.org/10.1145/3308560.3316495 [D1.1, CORE A]*

3. *P. Agarwal, S. Joglekar, P. Papadopoulos, N. Sastry, N. Kourtellis (TID):* ***Stop tracking me Bro! Differential Tracking of User Demographics on Hyper-Partisan Websites****. Proceedings of The Web Conference 2020, April 2020*
https://doi.org/10.1145/3366423.3380221 [D1.2, CORE A]*

4. *H. Herodotou, Despoina Chatzakou, N. Kourtellis (TID, CUT):* ***Catching them red-handed: Realtime Aggression Detection on Social Media****. Proceedings of the International Conference on Data Engineering (ICDE), June 2020*
https://doi.org/10.1109/ICDE51399.2021.00211 [D1.2, CORE A]*

5. *M. Diamantaris, S. Moustakas, L. Sun, S. Ioannidis, J. Polakis (FORTH):* ***This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration****. ACM SIGSAC Conference on Computer and Communications Security (CCS '21), November 2021*
https://doi.org/10.1145/3460120.3485366 [D1.3, CORE A]*

6. *A.-T. Hoang, B. Carminati, E. Ferrari (UI):* ***Privacy-Preserving Sequential Publishing of Knowledge Graphs****. Proceedings of the IEEE International Conference on Data Engineering (ICDE), 2021*
https://doi.org/10.1109/ICDE51399.2021.00194 [D1.3, CORE A]*

7. *E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, E.P. Markatos (TID):* ***User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users****. Proceedings of the Web Conference 2021, WWW '21, April 2021.*
https://doi.org/10.1145/3442381.3450056 [D1.3, CORE A]*

8. *C. Sandeepa, B. Siniarski, N. Kourtellis, S. Wang, M. Liyanage (TID):* ***A survey on privacy for B5G/6G: New privacy challenges, and research directions****. Journal of Industrial Information Integration 30, November 2022*
https://doi.org/10.1016/j.jii.2022.100405 [D1.4, SJR 2.745]

9. *E. Papadogiannakis, P. Papadopoulos, E.P. Markatos, N. Kourtellis (TID, FORTH):* ***Leveraging Google's Publisher-Specific IDs to Detect Website Administration****. Proceedings of the ACM Web Conference, April 2022*
https://doi.org/10.1145/3485447.3512124 [D1.4, CORE A]*

FINAL MESSAGE

Multiple crises, such as the pandemic, the war in Ukraine, and supply chain disruptions, underline the increasing importance of building a Resilient Europe. Being proactive, anticipating crises, avoiding fragmentation and silo thinking, and strengthening cooperation concerning building multistakeholder ecosystems are foundations of a European digital sovereignty resp. Strategic autonomy. In light of this effort, the results of CONCORDIA contribute to several objectives.

The proposed CONCORDIA Roadmap for Europe with the monitoring board to get feedback from the community about the priorities is an important approach to identifying research, investment, legal, and other development priorities. CONCORDIA's monitoring board will allow the ECCC to continuously get feedback on priorities from the cybersecurity community. Building the community with various stakeholder groups or developing tools for sharing security-relevant information in a trustworthy manner, such as the Cyber Threat Intelligence (CTIs) for the telco in the finance sector as well as for education such as the KYPO cyber range platform are other highlights, to name a few.

CONCORDIA has fully achieved its objective of building the foundation of the European Secure, Resilient, and Trusted Ecosystem. The results resp. the legacy of CONCORDIA will provide valuable input not only to the European Cybersecurity Center and the network of National Cybersecurity Centers, and with this, to the whole European cybersecurity community, but allow to build upon them to strengthen and speed-up research, development, and especially innovation. With this, CONCORDIA contributes to the objective of European digital sovereignty and building a resilient Europe.

Gabi Dreo, *CONCORDIA Project Coordinator*

About the project

CONCORDIA is operating a pilot for a Cybersecurity Competence Network to develop and implement a joint Cybersecurity Research & Innovation Roadmap. Consisting of more than 50 partners (universities, industries, and organizations), funded by the European Commission, CONCORDIA is part of a significant European-wide effort to accelerate cybersecurity research by drawing together leading experts across domains to boost the EU's resilience and digital sovereignty.

concordia-h2020.eu

twitter.com/concordiah2020

linkedin.com/in/concordia-h2020

This project has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement *No 830927*.