



Romanian Association
for **Information Security Assurance**

CONSIDERATIONS ON CHALLENGES AND FUTURE DIRECTIONS IN CYBERSECURITY

A project with the support of



romania2019.eu

ROMANIA
2019

CONSIDERATIONS ON CHALLENGES AND FUTURE DIRECTIONS IN CYBERSECURITY

A project by
the Romanian Association for Information Security Assurance (RAISA)
with the support of
the Romanian National Computer Security Incident Response Team (CERT-RO)
and
the National Cyberint Center



romania2019.eu

EDITORS

Ioan-Cosmin MIHAI, Costel CIUCHI, Gabriel PETRICĂ

ROMANIA
2019

The study expresses the opinion of the authors and does not necessary reflect the official opinions of their institutions, the Romanian Association for Information Security Assurance (RAISA), the Romanian National Computer Security Incident Response Team (CERT-RO) or the National Cyberint Center.

The correction belongs to the authors.

© 2019 Sitech Publishing, Craiova

All rights reserved. This book is protected by copyright. No part of this book may be reproduced in any form or by any means, including photocopying or utilized any information storage and retrieval system without written permission from the copyright owner.

SITECH Publishing is part of the list of prestigious Romanian publishing houses recognized by CNATDCU, for Panel 4, which includes the fields: legal sciences, sociological sciences, political and administrative sciences, communication sciences, military sciences, information and public order, economics sciences and business administration, psychological sciences, education sciences, physical education and sport.

SITECH Publishing, Craiova, Romania

Tel/Fax: 0251414003, Email: office@sitech.ro

ISBN 978-606-11-7004-3

eISBN 978-606-11-7005-0

TABLE OF CONTENTS

Foreword	7
Cătălin ARAMĂ, General Director, CERT-RO	
Foreword	9
Anton ROG, General Director, National Cyberint Center	
Introduction	11
Ioan C. BACIVAROV, President, RAISA	

PART I. CYBERSECURITY FRAMEWORK

EDUCATION AND AWARENESS

Cybersecurity Becomes from a Trend, a Fact	15
Viorel GAFTEA	
A Comparative Study on Security of E-learning Platforms in the Romanian Academic Field.....	21
Gabriel PETRICĂ, Sabina-Daniela AXINTE	
Learning Path for Gamified Cyber Training	29
Daria CĂTĂLUI	
How Botnets are Affecting Us and How to Protect Against Them.....	41
Mădălin VASILE	

INNOVATION AND RESEARCH

Cybersecurity in EU Framework Programmes for Research and Innovation	51
Claudiu CHIRIAC	

The Communications Future. 5G Between Benefits and Cybersecurity Challenges	59
Virgilius STĂNCIULESCU	

Innovation and Research - Current State, Trends and Challenges	79
Ioan CONSTANTIN	

Strategic Directions for Cybersecurity. A Bitdefender Perspective.....	85
Alexandru-Cătălin COSOI	

INTERNATIONAL COOPERATION

An Overview of the General Trends in Cybersecurity	95
Angela IONIȚĂ	

The Importance of Cooperation in Cybersecurity	117
Iulian ALECU	

A Cooperative Approach: the UK's Active Cyber Defence Programme.....	121
Jon BROWNING	

Collaboration: The Key to Disrupting Cyber Attacks.....	125
Matt LAVIGNA, Tara TRICKETT	

SELEC's Role in the Fight Against Cyber Crime.....	129
Robert PĂTRĂNCUȘ	

HUMAN LAYER

People and Machines: Dealing with Human Factor in Cyber Security	143
Ana BADEA-MIHALCEA	

The Importance of Human Resources.....	155
Iulian ALECU	

About the Real Value of Knowledge, Intellectual Capital and Resilience in the New Cognition Economy	159
Călin M. RANGU	

Filling the Cybersecurity Skills Gap.....	179
Liviu MORON	

PART II. CYBERSECURITY DIRECTIONS

NATIONAL CYBER SECURITY

Threats and Challenges. A National Cyber Security Perspective 187
Viorel SÎNPETRU, Cătălina PISARGIAC

CERT-EU: Contributing to a Cyber Secure European Union 201
Arthur DE LIEDEKERKE, Georgios PSYKAKOS

CYBER DEFENCE

**National Implications in Implementing NATO's Cyber Defence
Policy Concept 211**
Mihai-Ştefan DINU

Brief Overview over the Converged Security at the Enterprise Level 221
Andrei IANCU, Mircea BORCAN

CYBER RESILIENCE

Challenges in Cyber Resilience for Public Administration..... 229
Costel CIUCHI

**Cyber Resilience for the Special Telecommunications Services and
Systems from CERT/CSIRT Perspective..... 243**
Andrei-Sorin JERCA, Alexandru OZARCHEVICI

CYBER CRIME

Romanian Law Enforcement Involvement in Fighting Cyber Crime 253
Ioan-Cosmin MIHAI, Cătălin ZETU

Cyber Crime - Challenges and Evolution 263
Mircea-Constantin ŞCHEAU

Cybercrime - Legal and Strategic Elements 275
Virgil SPIRIDON

CYBER DIPLOMACY

Perspectives on Cyber Diplomacy 287
Carmen-Elena CÎRNU, Adrian-Victor VEVERA

Cyber (Security) Diplomacy 297
Mihai SEBE

DATA PROTECTION

GDPR - Enemy or Friend 311
Răzvan BĂRBIERU

Areas of Challenge in Data Protection for IT Systems 319
Larisa GĂBUDEANU

About the Authors 333

Foreword

Cătălin ARAMĂ

General Director of the Romanian National Computer
Security Incident Response Team (CERT-RO)

Cyber-attacks have become more complex and difficult to detect, some of them being classified as global epidemics due to spreading within cyberspace at high speed. Becoming prepared in the cybersecurity field is essential as these cyber-attacks can affect systems within critical digital infrastructure and, because the infrastructures are interconnected and transnational, any vulnerability exploited from a Member State could affect the whole of the European Union. For this reason, a high level of cybersecurity should be ensured through concerted action, both at the national and European level.

The study “*Considerations on challenges and future directions in cybersecurity*” focuses on the latest trends, challenges and future strategic directions of cybersecurity. The study was developed on the occasion of the *Romanian Presidency of the Council of the European Union* and represents an exercise in developing national cooperation among public, private and academic institutions for training, motivating and maintaining the human resource in the cyber ecosystem.

The Romanian Presidency Programme, conducted between January and June 2019, focused on four main pillars:

- Ensuring fair and sustainable development through an increased level of convergence, cohesion, innovation, digitalization and connectivity;
- Maintaining a safe Europe;
- Strengthening the EU’s global role;
- A Europe of shared values.

Regarding the second pillar, the Romanian Presidency aimed at consolidating a safer Europe through increased cohesion among European Union Member States in dealing with the new security challenges.

One of the objectives of the Romanian Presidency Programme during the second pillar was strengthening the internal security, by boosting cooperation among Member States and increasing the interoperability of the E.U. security systems, protecting the safety of citizens, companies and public institutions in cyberspace and improving the overall resilience of the European Union to cyber-attacks.

During its mandate as Presidency of the Council of the E.U., Romania has successfully implemented the *1911 Call Center* through the *Romanian National Computer Security Incident Response Team (CERT-RO)*, for reporting cybersecurity incidents. The *1911 Call Center* is unique in Europe and it represents a platform which facilitates the reporting of the cybersecurity incidents for operators of essential services and digital service providers, but also for all citizens and companies.

Founded in 2011 as an independent structure of expertise, research and development in the field of cyber infrastructure protection, CERT-RO activity consists in preventing, analyzing, identifying and responding to incidents within cyber infrastructures that provide functionality for public utilities or provide information society services. Since 2019, following the requirements of the NIS Directive, CERT-RO became the competent authority at the national level for network and information systems security, the national point of contact and the Computer Security Incident Response Team (CSIRT) for Romania. CERT-RO is actively involved in campaigns regarding awareness, projects and events in the field of cybersecurity.

In this context, CERT-RO supported the initiative of *the Romanian Association for Information Security Assurance (RAISA)* to elaborate the present study, which represents a joint effort of several entities from the public, private and academic sectors for developing a framework study regarding education, innovation, cooperation and human resources in cybersecurity and to present the challenges and the future strategic directions from this field.

Foreword

Anton ROG

General Director of the National Cyberint Center (CNC)

The rapid growth and widespread of technology turn the cyberspace into an environment characterized by excitement and opportunities and also by insecurity and challenges, considering that everything that can be used for good, can also be used towards gaining financial, ideological or strategic advantages.

The borderless Internet makes it difficult for the cyber security practitioners to counter the risks and threats that attackers pose to the security of national interest IT&C systems. For this reason, in this complex and expanding domain like cyberspace, any public or private institution can be at a higher risk today than it was years ago. While cyber attacks are based on more advanced techniques, organizations need to constantly integrate the latest technology. Businesses, modern life, societies, each individual - all rely and depend on technology, bringing opportunities and threats as well.

Therefore, improving cyber security resilience has become both a priority issue and a global need. The key for assuring cyber security is cooperation between governments and private institutions in order to create active defence strategies. It is important that all key parties have a good understanding of cyber attack methods and promote cyber security hygiene in order to continually strengthen cyber security and cyberspace.

The main manifestations of cyber threats to Romania's national security are cyber-attacks carried out by four categories of cyber criminals - states, cybercrime groups, extremist (hacktivist) groups and terrorist organizations.

Following its designation as national authority in the field of cyber intelligence by the Supreme Council of National Defense (CSAT), the Romanian Intelligence Service's *National Cyberint Center* has endeavored to identify, prevent and counter the vulnerabilities, risks and threats to Romania's cyber security.

Its main goal is to correlate technical defense systems with intelligence capabilities in order to identify and provide legal beneficiaries with the necessary information to prevent contain and/or preclude the consequences of any attack against the IT&C systems that are part of critical infrastructure.

Having a resilient digital environment can be achieved also through academic research by integrating insights from various sectors world-wide. In this context, the National Cyberint Center emphasizes the importance of efforts aimed at strengthening the cooperation among public, private and academic sectors, therefore closely supporting, alongside CERT-RO, the realization of the “*Considerations on challenges and future directions in cybersecurity*” study.

The present study represents a great initiative in regard to cyber security, gathering expert opinions on the main elements of this field such as national security concerns, human resources, cooperation, education, awareness, regulations and the main challenges.

Furthermore, the study “*Considerations on challenges and future directions in cybersecurity*” represents a statement for the importance of the cyber security field, by exploring its multidisciplinary nature, and of all the aspects the study addresses.

In order to ensure a high level of cyber security, future directions should include the creation of a framework based on cooperation, appropriate regulations and on the understanding of evolving challenges.

Only by gathering all our efforts and working together, strong cyber resilience can be achieved. Therefore, we would like to thank all participants to this study and encourage them to continue sharing their knowledge and research in cyber security in order to create a trusted digital environment.

Introduction

Professor **Ioan C. BACIVAROV**, PhD

President of the Romanian Association for Information Security Assurance (RAISA)

The accelerated evolution of technology generates many opportunities, but also many challenges for the information society. The number of newly discovered vulnerabilities, data breaches and cyber-attacks is increasing, making cybersecurity a major concern among countries and businesses.

The Romanian Presidency of the Council of the European Union focused on protecting safety in cyberspace and improving the overall resilience of the European Union to cyber-attacks. On this special occasion, due to the present importance of the cybersecurity issue, the *Romanian Association for Information Security Assurance (RAISA)* decided to elaborate the study “*Considerations on challenges and future directions in cybersecurity*”, which represents a cooperation exercise for raising the importance of cybersecurity.

The *Romanian Association for Information Security Assurance (RAISA)* is a professional, non-governmental and public benefit association, founded in 2012 as an initiative dedicated to disseminating the concept of cybersecurity and fighting against cybercrime. The aim of this association is to promote and support information security activities in compliance with applicable laws and to create a community for knowledge exchange between specialists, academia and the corporate environment. The vision of *RAISA* is to develop research and education in information security field, to contribute to the creation and dissemination of knowledge and technology in this domain and to create a strong “cybersecurity culture” at national level.

Among the notable activities developed by *RAISA*, we mention the *International Journal of Information Security and Cybercrime (IJISC)*, a scientific journal indexed in international databases, awareness websites, workshops, research projects and studies in the field of cybersecurity: the latest one is “*Current challenges in the field of*

cybersecurity - the impact and Romania's contribution to the field", elaborated in 2017 under the aegis of the *European Institute of Romania*.

The study "*Considerations on challenges and future directions in cybersecurity*" is a collection of papers organized in two sections: *Cybersecurity Framework* and *Cybersecurity Directions*. The first section contains 4 categories that play critical roles in the area of cybersecurity: *Education and Awareness*, *Innovation and Research*, *International Cooperation*, and *Human Layer*, all very important for developing a strong cybersecurity culture. The second section presents a vision of the future cybersecurity directions, categorized into *National Cyber Security*, *Cyber Defense*, *Cyber Resilience*, *Cyber Crime*, *Cyber Diplomacy* and *Data Protection*. This separation is not ideal, but it is a reality due to the complexity and diversity of cybersecurity, and it is necessary to define the roles and responsibilities of the institutions.

This study contains papers from specialists with a vast expertise, from different domains, presenting a systematic and integrated approach of the essential aspects specific to the field of cybersecurity. The added value of the study is given by the analysis of future cybersecurity directions from the perspective of the experts from the public, private and academic institutions.

RAISA is very grateful to all those who have contributed to this study, especially to the *Romanian National Computer Security Incident Response Team (CERT-RO)*, which has played a catalytic role in discussions with the authors, and to the *National Cyberint Center* for the support. We hope this study will underline the importance of cooperation in the field of cybersecurity, for all the countries, organizations and companies, to consolidate a powerful cybersecurity culture.

**PART I.
CYBERSECURITY
FRAMEWORK**

**EDUCATION AND
AWARENESS**

PART I. CYBERSECURITY FRAMEWORK

EDUCATION AND AWARENESS

Cybersecurity Becomes from a Trend, a Fact

Viorel GAFTEA
Romanian Academy
Information Science and Technology Section
viorel.gaftea@acad.ro

1. Introduction

Diverse specialties and backgrounds of specialists are today in context with cyber security due to the generalization of information and computer systems and electronic communications, in all branches of social and economic life. It should be divided into sections, each with a major emphasis on technology development, so that the reader can follow the temporal and logical development of the impact of cyber security in the surrounding technology and more recently in the whole spectrum of social economic life. We describe this evolutionary path for communications, computers, automation, robotics, medical medicine, mobile communications, internet networks, the Internet of things, Artificial Intelligence, 3D Printing technologies and Blockchain. It is not possible to forget about the electronic services in all social economic areas, financial, banking, orientation and geo-site services and, of course, social networks, which have a major impact and bring together the latest technologies. All these require and prioritize information security and cyber security from the simple components to the service level.

2. General strategic framework

Our goal is to capture this information technology evolution process and to identify some major requirements that address today's society. Starting from the author's multi-sectoral and multi-institutional experience, complemented by the strong current impact of science and information technology, we have defining several directions to be pursued in the future development.

Here are the main directions in which cybersecurity justifies its presence:

- Education and assimilation of 'digital skills';
- Evolution of communications (media, TV, mobile framework 3G, 4G, 5G);
- The evolution of computers and computer science;
- Robotics;
- Artificial Intelligence;
- Electronic services (e-Government, e-Health, e-Payments, e-Trade);
- Integrative technologies (as internet, eHealth, IoT, Blockchain).

2.1. Infrastructures

In all of these categories, the predominant role is played by hardware and software infrastructures; they are largely critical infrastructures and whose functionality depends on their security in operation, availability, security and access. These are, in fact, the cyber security criteria for information technology infrastructures.

2.2. Services

Attributes as mentioned below: availability, security and access, are essential for electronic services. Talking about the following type of electronic services specified in Table 1, as best you can know, we can identify the main Strategic Directions for Cyber security, oriented by the main and the more used digital services.

Table 1. Type of main public services

Type	Use for
G2C	Government to citizens
G2B	Government to business
B2C	citizens to Government
B2G	Business to Government
Mobile communication	Mobile, TV, Video, Internet
e-Health	Electronic health services, telemedicine
e-Payments	Electronic payments, financial services
e-Commerce	Electronic Trade platforms, Digital Market
Geo services	GPS, e-Maps, e-Driving
Social platforms	Social Media, e-mail, messenger

The list is not limiting and in the current environment of interoperability and synergy between technologies, the complexity is a current feature.

In June 27, 2019, the European Union introduces stricter security rules for identity papers to reduce counterfeiting. Electronic identity is a fundamental requirement for the implementation and deployment of electronic services. The impact of electronic identity occurs both in e-government public services offered to citizens and to firms but also correlated with the financial and commercial operations of the firms.

Robotics and Artificial Intelligence

Under the current mobility of labor, people, capital, production and assets, cyber security gets a new dimension, a global one, which cannot be provided only partially by national systems, on personalized services and private networks.

The processing of activities on global platforms is a matter of great importance that of national data protection. Accessing, ownership and processing of national data, especially economic and financial banking, is a newly informed issue that challenges cyber security systems.

In this context, the impact of robotics in industry and Artificial Intelligence in services becomes major and subject to cyber security criteria unattained to date. Adapting industrial policies, to a digital world for economic diversification and structural transformation, becomes in actual digital revolution more disruptive than previous technology waves, because advances in Artificial Intelligence and Robotics increasingly enable the substitution of cognitive, instead of just manual tasks.

If the actual trend in digital economy is generated by Robots and industrialization especially in developing countries, the Industrialization has historically been synonymous with development, while deindustrialization is a well-established trend in mature developed economies as they move towards services-based economies. Artificial Intelligence helps cyber security to be a service-based activity.

The combination of Artificial Intelligence, humanoid robots and intelligent or smart cities becomes a combination that defies the classical concepts of cyber security,

embracing, besides those mentioned, the electronic identity with the safety of utility applications besides financial banking.

Blockchain

Blockchain technology promises the integration and additional security of the complex services. It is not yet fully defined how integration of cyber security elements will be done by a component or by a new philosophical and technological approach.

The informatics technology gets a new property, less identified in previous technological stages and leaps. It is the ability to synthesize and interoperate technologies. This new attribute of technology raises cyber security issues, faces more complex issues than securing an email server or communications and information that feeds various forms of sub-applications such as viruses, computer worms, or spyware cookies.

In Romania was held in Bucharest, at the Palace of Parliament between June 21 and 22, and organized under the patronage of the Minister of Communications and Information Society in partnership with representatives of the Romanian Block Industry and with the participation of the Observatory EU Forum on Blockchain technology, one of the most important Conference in the subject (<https://www.romaniablockchainsummit.com/>).

Global References

Number of consecutively assumption of European or global institution regarding new technologies and new cyber security requirements are becoming more and more deeply embraced at the level of the European Commission, UN, ITU, UNCTAD, etc.

Digital Assembly from Bucharest 2019, June, after Romanian Presidency of European Council, has identified and set out a digital path for Romania and Europe.

The Digital Assembly 2019 has been a forum for stakeholders to review the achievements of the Digital Single Market Strategy, draw new lessons and to exchange views on a future digital policy (<https://ec.europa.eu/digital-single-market/en/events/digital-assembly-2019>).

UNCTAD's e-Commerce Week is held in conjunction with the Intergovernmental Group of Experts on e-Commerce and the Digital Economy between 01-05 Apr 2019 at Geneva, has had special sessions devoted to cyber security, Blockchain and new global trends in e-Commerce and digital economy.

European Digital Single Market continues to be strategically sustained by the European Commission and support also materializes in enhancing electronic security support.

Conference “Europe of Convergence: growth, competitiveness, connectivity” had the main objective to discuss different issues related to the reform of the next EU Cohesion Policy (after 2021) through cohesion or competitiveness, urban dimension or rural dimension, transition regions or lagging regions, support of jobs and innovation or infrastructure, cyber security and digital markets.

3. Paper conclusion

The new political trend and its economic philosophy are generating antagonistic approaches and actions of various actors, leading to numerous clashes of interest, intention and outcomes. All of these issues have a direct reflection on cyber security, all the more so that this area has to cope with actions ranging from social, economic to defense.

The specific objective is to unify the vision of understanding cyber security implications, in the digital economy and society. The paper has two main conclusions:

- First is that the digital economy is present and conceives the educational, economic and development prospects of a nation;
- Second, Cyber security is a fact, it is no longer a trend, and it becomes an obligation in education, in the implementation from the device in the household and the industrial products to the institutional or private information services.

For this purpose, the European Commission is aware of the need to educate the European citizens in digital skills, building initiatives like the skills agenda for Europe, to help Europe's growth in an increasingly digital society.

Other initiatives like EU e-Health Action Plan and Telemedicine, bring other requirements to Cyber security, to digital tools that allow access to better social care, health monitoring and recording through e-Health and ageing. Smart digital technologies for life are being supported by the Commission. It also encourages smart energy use in homes and for transport in order to have a positive environmental impact in a safe environment.

References

- [1] Ioan-Cosmin MIHAI (coord.), Costel CIUCHI, Gabriel-Marius PETRICĂ, SPOS 2017 - Provocări actuale în domeniul securității cibernetice - impact și contribuția României în domeniu, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf.
- [2] Viorel-Nicolae GAFTEA (coord.), Angela IONIȚĂ, Ionel NIȚU, Iulian-Florentin POPA; SPOS 2017 - România și Piața Unică Digitală a Uniunii Europene. Oportunități și provocări, http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_3_FINAL.pdf.
- [3] Academia Română, STRATEGIA DE DEZVOLTARE A ROMÂNIEI ÎN URMĂTORII 20 DE ANI, <https://acad.ro/strategiaAR/strategiaAR.htm>.
- [4] UNCTAD eCommerce Week 2019, April 1-5, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-eWeek.aspx.
- [5] UNCTAD, UNCTAD HANDBOOK OF STATISTICS, https://unctad.org/en/PublicationsLibrary/tdstat41_en.pdf.

A Comparative Study on Security of E-learning Platforms in the Romanian Academic Field

Gabriel PETRICĂ, Sabina-Daniela AXINTE

Faculty of Electronics, Telecommunications and Information Technology,
University Politehnica of Bucharest, Romania
gabriel.petrica@upb.ro, axinte_sabina@yahoo.com

1. Introduction

With the explosive growth of the Internet environment, Web content management technologies have also evolved. Information can no longer be published online through a manual process (page by page) but must be permanently supervised and updated by content editors, so other consumers - individual users, customers, websites or search engines - have access to the most up-to-date version of that Web page.

Information and communication technologies are used today at all levels - from regular users to organizations or government entities - for information, business development, communication, cooperation and global collaboration. In this context, individual education and employee training are facilitated by e-learning, a modern solution chosen by more and more companies or educational entities to support and improve learning as a complement or alternative to traditional classrooms and standard teaching techniques.

Since the second half of the '80s, digital communications and computer networks have begun to evolve in the education field as well. First-generation LMS (Learning Management Systems) applications ("E-learning 1.0") ensured a unidirectional distribution of information, from instructor to student, unlike the "E-learning 2.0" concept, introduced by Stephen Downes in 2005 [1]. The latter integrates with the new Web 2.0 specific technologies (wiki, podcast, or RSS) and promotes a new term, CSCL (Computer-supported Collaborative Learning) - an

interactive and cooperative learning method. Starting with 2010, the 3rd generation e-learning uses modern technologies such as cloud computing, artificial intelligence, data mining, or machine learning in information sharing and collaboration between users [2].

In the beginning of 2019, Web Courseworks made the predictions presented in Figure 1 on frequently used keywords related to e-learning technologies [3]: virtual reality, blockchain, gamification, MOOCs (Massive Open Online Course), mobile learning and xAPI (Experience API).

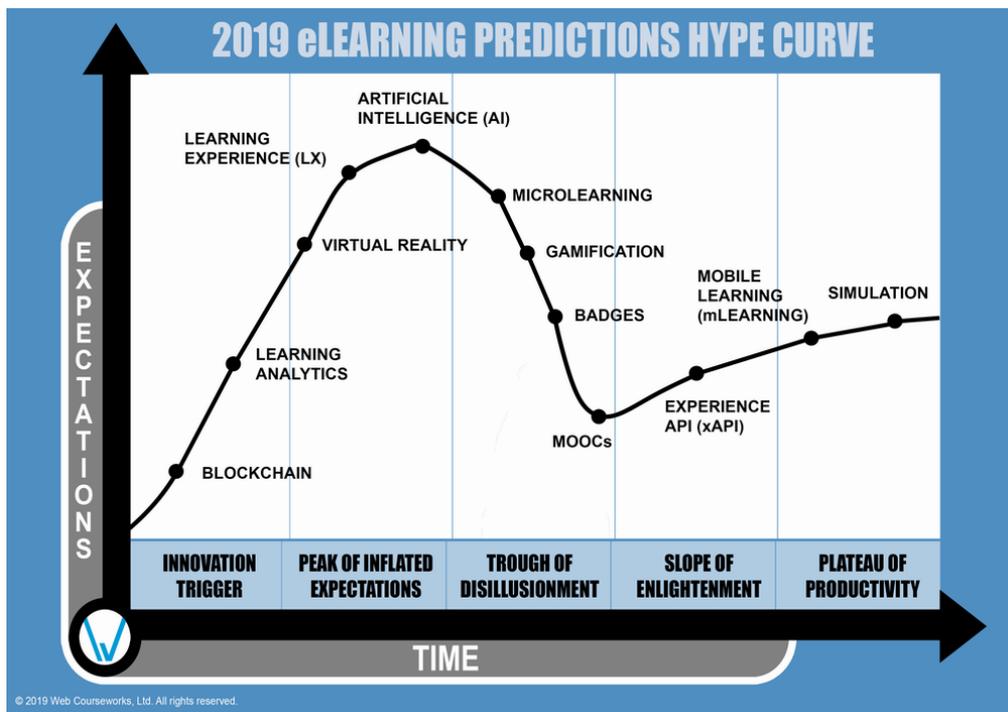


Fig. 1. eLearning predictions for 2019 [3]

2. Advantages and disadvantages of e-learning platforms

The emergence of LMS applications has offered certain advantages. It helps increase student motivation by facilitating interactions and obtaining feedback from the trainer. Access to electronic materials with no time and space constraints, learning media offered in various formats (text, audio and video) and online assessments are other important advantages of this technology [4]. In August 2018, Moodle (more than 132 M registered users [5]), Edmodo (85 M members), and SuccessFactors (over 45 M users) ranked as the top 3 LMS applications according to the number of global users. Other popular LMS applications include Blackboard and Cornerstone [6].

However, there are some disadvantages of e-learning platforms, among which:

- the need for an infrastructure for the implementation and development of LMS at the school or university level. This involves both Internet access and/or a server providing specific e-learning services, as well as audio-video support for the dissemination of information in the classrooms (when adopting a hybrid e-learning model).
- adaptation of the course content to the online teaching format requires specific knowledge from the instructor, as well as additional time allocated to translating information from the existing format to that required by the e-learning platform.

These disadvantages may somewhat justify the results of the survey on the degree of implementation and use of e-learning platforms in Romanian higher education (a survey designed by the authors and publicly available in 2018): although the absolute majority of respondents offer course support in electronic form (90%), only 30% use an e-learning platform (usually Moodle), the rest preferring to send documents by e-mail (70%), individual Web pages (50%) or cloud storage (20%).

Another disadvantage is the software vulnerabilities encountered in all types of applications (operating systems, programming languages and environments, utility programs and Web applications). Thus, for the Moodle platform (which will be analyzed in this work), the vulnerabilities identified between 2009 and 2018 are distributed according to the Table 1 [7]:

Table 1. Statistics on Moodle vulnerabilities identified between 2009 - 2018

Vulnerability type	No. of vulnerabilities
Denial of Service	8
Code Execution	16
SQL Injection	15
XSS (Cross-Site Scripting)	79
Directory Traversal	3
HTTP Response Splitting	2
Bypass Something	46
Gain Information	81
Gain Privileges	4
CSRF (Cross-Site Request Forgery)	21
File Inclusion	1

Obtaining confidential information (user names, encrypted passwords or other sensitive information) is the most common type of vulnerability (“*Gain Information*”) identified during the specified period. The second most common are XSS (Cross-Site Scripting) vulnerabilities, which allow attackers arbitrary code injection (HTML or Web scripts) through various parameters passed to the server. The third place is occupied by those that allow a bypass of a specific security mechanism (“*Bypass something*”); this type of vulnerability would allow an attacker to access, for example, a protected directory or the source code of the platform or Web application.

3. E-learning support in representative universities at the national level

We analyzed the e-learning platforms made available to users (students) of universities from the top 5 positions of the University Metaranking-2018 (“*Metarankingul Universitar-2018*” [8]), a ranking aimed at identifying Romanian universities with international visibility and impact in the academic area corresponding to the university profile (see Table 2). Thus, in the University Metaranking-2018, out of 54 public universities (47 civil and 7 military) and 47 private universities (of which 38 accredited and 9 provisionally authorized), the first five positions are occupied, in order, by: Babeş-Bolyai University of Cluj-Napoca (UBB), University of Bucharest (UB), University Politehnica of Bucharest (UPB), Alexandru Ioan Cuza University of Iaşi (UAIC) and Iuliu Haţieganu University of Medicine and Pharmacy from Cluj-Napoca (UMF).

Table 2. E-learning platforms analysis

University	E-learning Web address	Default protocol	Platform	Version	No. of vulnerabilities*
UBB	cursuri.elearning.ubbcluj.ro	HTTPS	Moodle	3.6.4	-
UB	moodle.fmi.unibuc.ro	HTTP	Moodle	2.0	90
	claroline.faa.ro	HTTP	Claroline	1.11.8	1
	dreptonline.unibuc.ro	HTTP	Moodle	3.7	-
	edocemus.ro	HTTPS	Moodle	2.8.2	62
UPB	curs.pub.ro	HTTPS	Moodle	3.5.2	3
UAIC	elearning.law.uaic.ro	HTTPS	Moodle	3.1.6	18
UMF	web.umfcluj.ro/moodle	HTTPS	Moodle	3.7	-

* according to CVE Details [9]; “-” means *data not yet available*

The analysis consists of identifying e-learning platforms within these 5 universities, the default protocol used, platform type and version, and specific number of vulnerabilities.

The Babeş-Bolyai University of Cluj-Napoca offers two portals centralizing information on the programs developed within the university: UBB Online (curricula, subjects, teaching materials, discussion groups, document sharing) and an e-learning system offered by the Center of Continuous Education, Distance and Part Time Learning.

At the University of Bucharest, we identified e-learning platforms developed within the Faculty of Mathematics and Computer Science, Faculty of Business Administration, Faculty of Journalism and Communication Studies and Faculty of Law (a platform for Distance Learning programs).

The University Politehnica of Bucharest has implemented and made available, since 2010, the project “E-learning platform and e-content curriculum for technical higher education” [10], which consisted of the following milestones:

- a physical infrastructure (servers, connections, storage space) to support the implementation of the e-learning solution;
- an application that provides on-line support for teaching and for presenting digital content;
- the digital content of the subjects in the undergraduate and postgraduate programs, initially for the students of the University Politehnica of Bucharest, which will be extended to the whole technical education at the national level or interested companies.

Within Alexandru Ioan Cuza University of Iaşi, the Faculty of Law offers an e-learning solution for subjects taught in the Bachelor's degree and Master's degree programs, full time, distance and part time learning.

At the Iuliu Hațieganu University of Medicine and Pharmacy of Cluj-Napoca we identified a Moodle platform with information for courses taught within the Department of Medical Informatics and Biostatistics at the Faculty of Medicine.

Analyzing the versions of Moodle platforms and their specific vulnerabilities, we find that most vulnerabilities identified are “Gain Information”, XSS and “Bypass something”. The distribution of these vulnerabilities by Moodle version is shown in Figure 2.

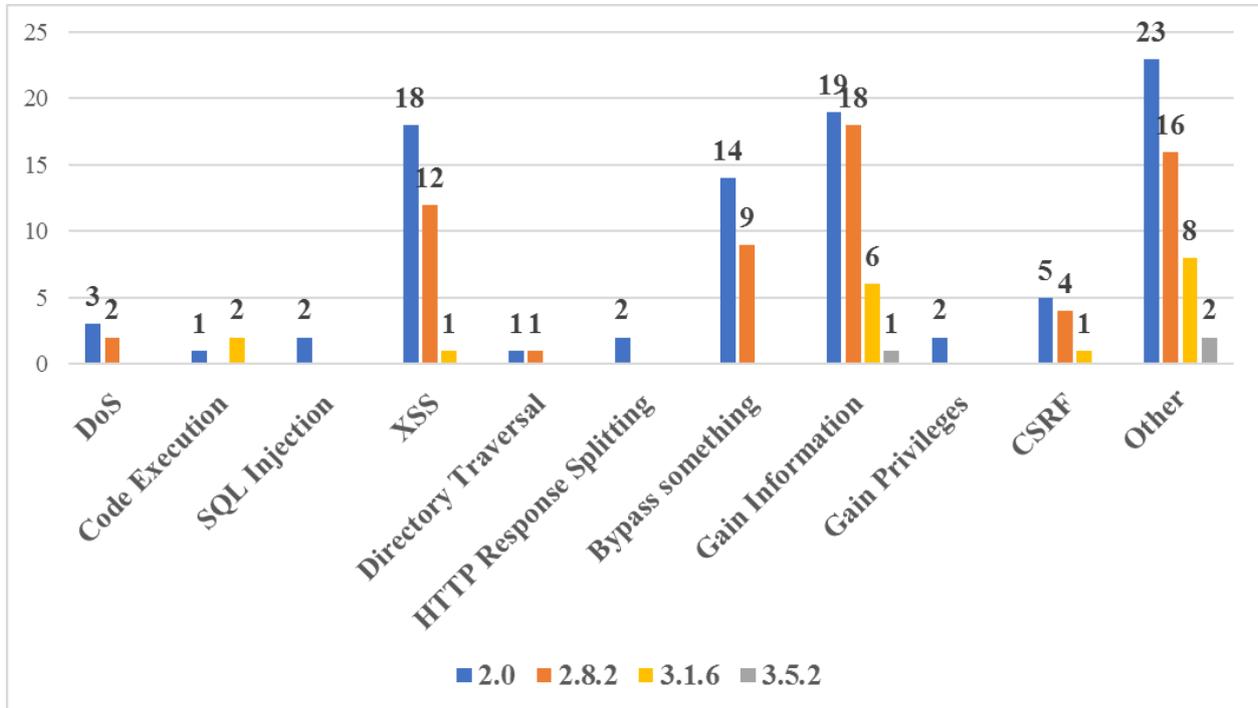


Fig. 2. Distribution of Moodle vulnerabilities

After analyzing the data, we can make the following remarks:

- compared to a study conducted by the authors in 2018, the websites of the universities align with the general trend of using the HTTPS protocol for securing access to Web resources;
- the most widely used e-learning platform is Moodle, with alternatives being Claroline (an open source, collaborative e-learning and e-working platform for Windows, MacOS, Linux [11]) or resource distribution through static Web pages;
- the Moodle versions in use vary between very old, with various known vulnerabilities (e.g. v.2.0 of 2010 or v.2.8.2 of 2015), other outdated versions (v.3.1.6 of 2017 or v.3.5.2 of 2018), to updated ones, with no identified vulnerabilities so far (very recent versions, like v.3.6.4 or v.3.7 of May 2019) [12].

4. Conclusions

In a more and more dynamic, global and European context, with increasing threats and a major impact on cyber security, it is noticed that the Romanian information society is experiencing a sustained technical development (at the hardware and software level) and harmonization of legislation to adapt to the requirements of the European Union.

In the 2018 Country Report on DESI (Digital Economy and Society Index), Romania ranked on the same last place among the EU Member States (28th place), but still scores higher than in 2017 (37.5 vs. 33.7), while at the EU level the average score in 2018 was 54 (rising from 50.8 in 2017). Romania's slow progress is due to the increase in performance in 4 of the 5 chapters (Connectivity, Human Capital, Use of Internet Services and Digital Public Services); the only area where the score has fallen was the Integration of Digital Technology [13].

Education and training are aspects which should be given maximum attention. An area in which action should be taken is the dissemination of ICT (Information and Communications Technology) and cyber security subjects in educational programs from the youngest ages, given the intense use of computers and mobile devices among children [14].

Setting up computer networks in schools (especially in rural areas), providing access to the Internet and introducing new, modern, competitive, and market-oriented programs into the curriculum, using beneficial technologies such as online courses and e-learning platforms, will increase the number of IT specialists and improve the level of knowledge, country-wide, in the cybersecurity field.

References

- [1] S. Downes, E-Learning 2.0, eLearn Magazine, 2005, <https://www.downes.ca/cgi-bin/page.cgi?post=31741>.
- [2] G. Petrică, I.D. Barbu, S.D. Axinte, I. Bacivarov, I.C. Mihai, E-learning platforms identity using digital certificates, Proceedings of the 13th

- International Scientific Conference „eLearning and Software for Education”, Bucharest, 2017, vol. 3, pp. 366-373, doi: 10.12753/2066-026X-17-228.
- [3] A. Hicken, 2019 eLearning Predictions - Hype Curve, www.elearninglearning.com/2018/market/statistics/?open-article-id=9516267.
- [4] A. Sharma, S. Vatta, Role of Learning Management Systems in Education, International Journal of Advanced Research in Computer Science and Software Engineering, 3, 6, 2013, <https://pdfs.semanticscholar.org/3d19/dc963e7fb8ce49bb6bcc9329aa03e22a6075.pdf>.
- [5] Moodle statistics, <https://moodle.net/stats/>.
- [6] Capterra - The Top 20 Most Popular LMS Software, <https://www.capterra.com/learning-management-system-software/#infographic>.
- [7] CVE Details - Vulnerability datasource, <https://www.cvedetails.com>.
- [8] D. David, O. Andronesi, D. Banabic, C. Buzea, B. Florian, S. Matu, A. Miroiu, A. Prisăcariu, L. Vlăsceanu, University Metaranking-2018. Romanian Universities Ranking, http://ad-astra.ro/wp-content/uploads/2018/12/Metarankingul_Universitar_2018.pdf.
- [9] CVE Details - Moodle: All Versions, <https://www.cvedetails.com/version-list/2105/3590/1/Moodle-Moodle.html>.
- [10] Project „E-learning platform and e-content curriculum for technical higher education”, <http://curs.pub.ro/index.php/cursuri-upb-despre-proiect>.
- [11] Claroline - Votre Learning Management System, <https://claroline.net/>.
- [12] Moodle Releases, <https://docs.moodle.org/dev/Releases>.
- [13] Digital Single Market - Romania, DESI country profile, http://ec.europa.eu/information_society/newsroom/image/document/2018-20/ro-desi_2018-country-profile_eng_199394CB-B93B-4B85-C789C5D6A54B83FC_52230.pdf.
- [14] I.C. Mihai, C. Ciuchi, G. Petrică, Current challenges in the field of cybersecurity - the impact and Romania’s contribution to the field, Sitech, Craiova, 2018, ISBN 978-606-11-6575-9.

Learning Path for Gamified Cyber Training

Daria CĂTĂLUI

Lancaster University, United Kingdom

daria.catalui@protonmail.com

1. Abstract

This article is part of a larger working paper and represents a pilot or small-scale empirical research on the topic of gamified cyber training. It has as conceptual framework network learning theory and community of practice approach, with data collection gathered from 3 emailed interviews and one face-to-face collective interview. The data trail based on convenience sampling is further presented by subtopics for a clear interpretation and analysis. The researcher was interested to know if gamified solutions are integrated in the learning path of cyber professionals. The final conclusion is that the training professionals interviewed consider that we are not yet at that stage of integrating gamified solutions in the learning path of cyber professionals. Rather, we work on a year-by-year basis in terms of taking part in specific cyber training but not delving enough into educational results and planning.

2. Introduction

What is the Learning path for gamified cyber training?

In the cyber security world, highly skilled human resource is scarce (Harvard Business Review- HBR, 2017). Good training for on-the-job professionals is essential according to HBR. In my opinion, this is not such a different reality compared with other fields. However, when European governments pin cyber education as top priority on the strategy map, it is possible to understand that the focus switches to this particular topic (ENISA, 2018). I believe that from a practitioner viewpoint, this is an important subject of concern. Specifically, I am interested to know more about learning path

understood for the purpose of this research as a wide variety of educational experiences in diverse settings (Education Glossary, 2013).

For use within this work, cyber education refers to face-to-face training, demos, quizzes, educational articles, but particularly game-based learning. An exemplification for gaining a wider understanding can be found in references like CyberReadyGame (European Commission, 2018), the Network and Information Security quiz (ENISA, 2016), and the Network and Information Security Education map (ENISA, 2017). But gamification is introduced in cyber education also in the form of table-top cyber exercises like Cyber Europe (ENISA, 2018) and different other facilitated exercise games.

This research builds upon some initial ideas and work of other scholars. The first paper, 'Serious games experience in teaching cloud security' (Ruboczki, 2016), argues that by employing role-based games it can improve both the knowledge and awareness of the user. It is stated that by playing, the gamer gets a higher awareness than if it is practiced; game-experience engagement gives feedback and offers a sense of control. Ruboczki's paper concludes there are benefits and advantages of using gamification in teaching cloud security in particular. In the same line, there is recent work (Elizondo et al., 2016) that reviewed existing serious games for general cyber security awareness this time in teaching and training, showing that these games have a great pedagogical potential. The authors concluded that their use is most often limited to formal contexts and ideally these limitations could be overcome if serious games were released in informal contexts, without degrading their pedagogical advantages. They also tackle gamification by developing on the serious games concept (Abt, 1970; Zyda, 2005; Sawyer, 2002) as a human-computer rule-based contest using entertainment to communicate and pass learning objectives.

At this point, I would like to put into context an explanation of gamification (Deterding et al., 2011) and give more technical details, since it is important to understand some specific details for this paper that relate to the study. Accordingly, gamification reflects the use of game thinking, including progress mechanics (such as points systems), player control (such as avatar use), rewards, collaborative problem

solving, stories and quizzes, and competition in non-game situations (Deterding et al., 2011; Kapp, 2012).

Underlying gamification is an understanding of motivation as significantly correlated with and predictive of desirable human outcomes such as achievement, success, and the attainment of distinction and rewards (Kapp, 2012). The gamification of learning is an educational approach to motivate students to learn by using video game design and game elements in learning environments. Maybe it is worth underlining that this article looks into the educational approach to gamification and not to the entertainment angle that is mostly advertised worldwide. It is important to note that recent developments in gaming for entertainment make clear that this can evolve into addiction (WHO, 2019).

Furthermore, in a piece of work (Mackenzie et al., 2015) focusing on cyber security skills, I found an interesting idea that combined gamification and entrepreneurial perspectives with the objective in mind to understand how to best build cyber security skills in a cost-effective manner. For the purpose of building cyber security skills there is an emphasising of a third stream, attacker types, to create training scenarios for lifelong learning. According to the authors, the use of such methods would enable employees and leaders to use role-play scenarios in an effort to build skills and awareness. Moreover, we are encouraged to think like a hacker in a business school article (Esteves et al., 2017) that advocates for gamification in cyber security education.

By using the term cyber security, we refer to the international standard (International Telecommunications Union- ITU recommendation -T X.1205, 2008). Cyber security strives to ensure the attainment and maintenance of the security properties of the assets against relevant security risks in the cyber environment. Of course, the interesting part in the current work is the training and education subtopic in cyber security.

For the purpose of this research, the focus is on being connected as part of networked learning. However, I am also interested to frame the theory around networked learning in order to emphasise the dimension of this. It is seen as ‘Learning

in which ICT is used to promote connections: between one versus other learners, between learners and tutors; between a learning community and its learning resources' (Dirckinck-Holmfeld et. al., 2012). Regarding the theory of CoP - communities of practice are groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly (Wenger et al., 2015). A CoP approach and engaging with peers offers a diverse test bed of exploring the research questions and eventually reaching novel findings. I have used networked learning as theoretical background, but at the same time included CoP in the interview phase since the relationship between the two puts light on an interesting combined approach offering richer results in my view.

3. Findings

What news arises about the Learning path for gamified cyber training?

The purpose of this research takes into account my interests as a researcher and professional, namely integrating cyber training in a learning path. Perhaps it is useful to indicate my own awareness of the debate since my positionality in this article may be considered at the same time to class me as an 'insider research'.

My professional path has included, for a couple of years now, work in IT security training and education, so I am very much interested in researching and applying the findings on cyber research.

For this research, I employed 3 written interviews filled in by 3 very experienced training professionals that have a good overview of the topic and its evolution in the last 10 years.

The interview request together with the research presentation was sent via e-mail, with a follow-up call if needed. I also set up a face-to-face collective interview with the cyber training team of a global company.

This data trail was conducted in several phases as presented in Figure 1 below.

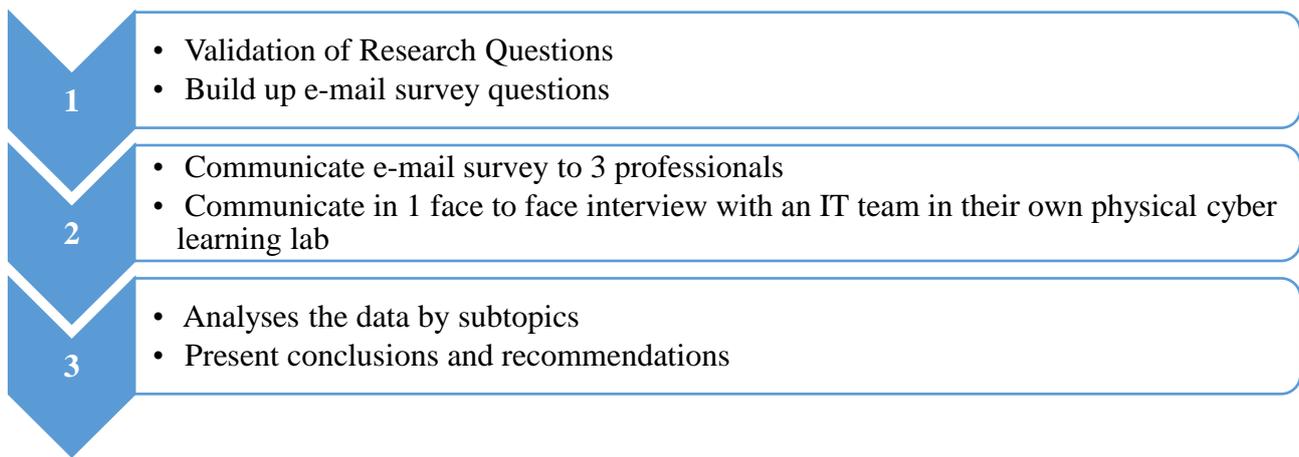


Fig. 1. Data Trail structure

Hereby I present the findings by grouping them according to the research questions (Figure 2) and further detail them with supporting survey questions and then referencing some patterns.

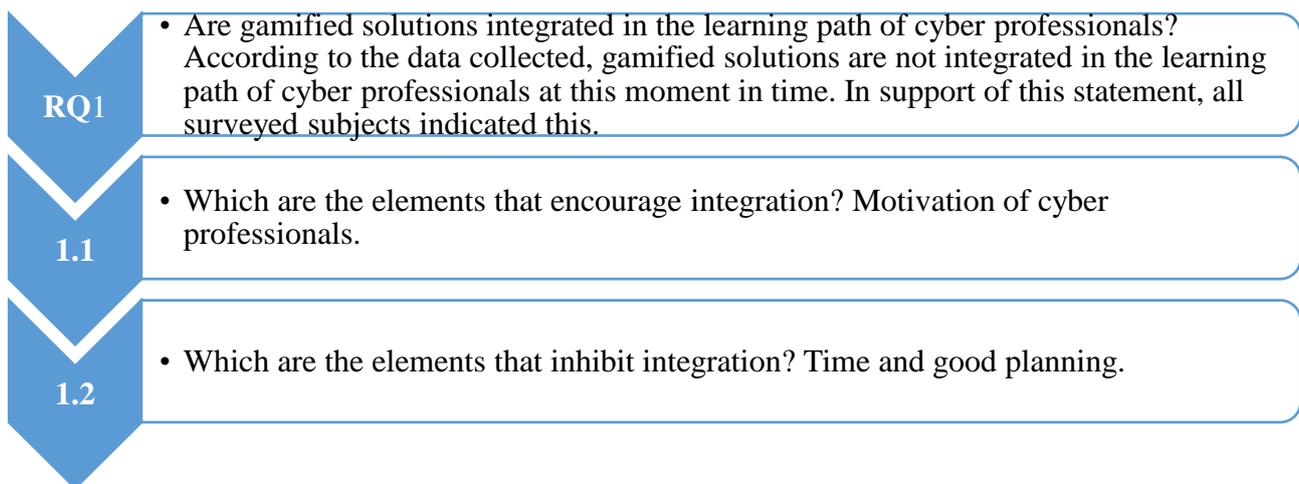


Fig. 2. Research questions

The survey questions below aligned with the research questions, enriching the findings on several subtopics.

1. What are the **3 essential elements of designing learning** for cyber professionals?

Among three essential elements that emerge as common for respondents are: *know your audience and focus on it; what do you want them to know as a result of your training; how will you engage and train them.* These findings drawn from practitioners' experiences reinforce the conclusions from an academic article

mentioned early on (Douglas et al., 2010). The authors have provided a tool for students and instructors to understand and pay attention to the relationship between knowing the system, knowing the people, and knowing the methods, since they are considered as key concepts for engaging in a praxis of change.

Other nuances gathered from the respondents related to these questions refer to:

- **Content of the training:** adding hands-on activities to cyber training; introducing apprenticeships after the learning process; knowing what the current and future threats are and include examples; also, besides technical knowledge, the soft skills cannot be neglected along with managerial skills, so cyber professionals have an overall understanding of what they are actually defending; the channels for delivering the knowledge should involve a simulation environment, so participants can have first-hand experience from the very first moment; and setting up a learning space like a laboratory for hands-on training.
- **Generalising:** one mentioned that learning theory should not be different for cyber security; cyber security is really not that different than any other topic.
- **Tailor the process for career path:** 1. Know what the learner will be doing, what the job title will be and what can be expected from that position; 2. Logical clear career-pathways should be mapped out where organisations are aware of the skills they need and professionals can plan their career advancing accordingly; 3. Having a corporate strategy; 4. Keeping track on the motivation of people.

1.1. What is the role of community of practice in design of learning for cyber security?

When asked about the role of the community of practice the training professionals replied that:

- It plays a central role; however, the management of it can be cumbersome.
- It is a great mobiliser and benchmarking element.
- It is both consumer and creator of knowledge.

Regarding the role of community of practice one respondent mentioned *‘Community serves as a good audience and influencer in regards of directions. Cyber education and training should be agile and be able to adapt to the changing environment where cyber operates. Learning materials can come from various sources along with the simulation challenges that are created by community based on their real life experiences. So community both serves as a measure for what is required and also as a creator of learning material.’*

Furthermore, another significant quote about communities of practice from the interviews: *‘We clearly won our first and only played high level cyber exercise till now for the following reasons: we set up a working team communicating effectively and knowing the split of tasks. Also because we shared the same space, our cyber lab where we could feel the pressure of the competition and learn as a team. When we realized at the end that we won, we could not believe it. The entire way we were emerged in the cyber exercise focusing on solving the challenges, not on the winning.’*

These quotes add qualitative examples to this research analysis and show that CoP is very much appreciated at a micro level, by practitioners or professionals.

1.2. How did design of learning adapt in a networked world compared to 10 years ago?

When asked on the difference from 10 years ago, professionals added that:

- Learning is very much online now, such as interactive training, knowledge assessments and gamification.
- Learning is very slow. The premise here is that the education system is a very slowly- moving system where there are too many conflicts of interests among the different stakeholders compared to training organisations that adapt faster and participate more in knowledge sharing. There are more resources available; however, many of these resources are focusing on different silos of the cyber domain, and not having a horizontal layer or holistic approaches taking into account all the different aspects.
- Learning is very much a collective discovery and offering team solutions is very important.

These findings tell me as a researcher that the learning changes at a high pace but not necessarily the procedures behind it, where those procedures support and should enable the learning to happen. Also, once again, I find validation of the CoP role in the learning process.

2. How do they rate the use of gamification in designing learning in cyber security on a scale from 1 minimum to 5 maximum?

When asked in rating the current use of gamification in design learning in cyber training **professionals average rate was 3.**

Some other details mentioned here for the purpose of contextual understanding were:

- There is a preference for it in awareness where it fits versus cyber security professionals that need lots of hands-on skills.
- Usually new training companies integrate gamification solutions from the start; however, the majority of organisations do not use it.
- There is a clear preference for its interactivity and learning by doing solutions like cyber exercises.

2.1 How important is physical space on a scale from 1 minimum to 5 maximum in designing learning in a gamified approach?

When asked on the importance of physical space for designing learning with a gamified approach, for example, work environment versus on the move versus at home, **professionals reported an average of 4** (on a scale from 1 minimum - 5 maximum).

However, we should also take into account several distinctions as follows:

- If well done, then the learner should be able to do it from anywhere.
- Any gamified environment makes learning faster.
- In this case, the team could see better outcomes in using specially designed learning spaces or in any way of getting the staff off their normal working desk/environment.

2.1.1 From the game-based learning approach do you recommend more online, e.g. platform based and CTF games, or offline facilitated, e.g. cardboard games game solutions?

When asked for recommendations between more online (platform based and CTF-capture the flag games) or offline facilitated training (cardboard games), **the preference was on online solutions since these could scale better, faster and fit to more audiences.**

Also, there were further mentions giving details about question 2.1.2 *Which is the reason of this choice/preference?*

- That cyber security is in a big part about using technology to secure technology. As such, so the focus should be on the interaction.
- Advantages of a mixed approach or hybrid solution should be explored. The premise being that not all trainings are suitable for platform-based solutions, so the tools should be used according to the audience and the availability. The aim should justify the tool. For example, cyber security training for management could be well done with the help of offline materials, while a technical challenge would be hard to carry out in a gamified environment without a supporting platform.
- The preference for online and cyber exercises in order to have a competitive ecosystem.

The findings analysed from the data collected from the respondents support a better understanding of ‘*What news arises about the Learning path for gamified cyber training?*’ At the same time, the data support the work presented in academic articles (Douglas et al., 2010; Catalui, 2018) giving impactful details from practitioners’ experiences. This pilot small-scale research succeeded in presenting a better understanding on the status of gamified cyber training and its use for learning paths. For example, it offers a better understanding on the role of CoP in the learning process, the importance of hybrid or blended learning between online and offline channels, the importance of engagement methods and keeping curating good relevant content.

However, this is surely a small contribution of what is needed to describe the entire phenomenon regarding cyber learning.

4. Conclusions and recommendations

What recommendations are there for the Learning path for gamified cyber training?

The final interpretation is that the training professionals I interviewed consider that we have not yet reached the final objective in integrating gamified solutions in the learning path of cyber professionals. Rather, we work on a year-by-year basis, namely, taking part in cyber exercises and drills, but not delving into educational results and planning. The practitioners were quite eager to share details about the elements that encourage integration like enjoyment of learning and the dynamic design of the learning space.

As we are reaching the final part of this article, I would like to summarise the process with an insider story. Many times, when I experience a new gamification solution demonstration, my questions are: Do you have educational objectives embedded? Do you apply a competence framework to match the tasks and deliver at the end a token of learning impact? Do you follow a user education path? Sometimes these questions receive a blunt YES or a NO answer but it happens that they open long conversations too. These long conversations are very useful in my professional life since they help me understand that using gamification elements can happen for very different reasons, but ultimately one should know how to use them to benchmark.

This research is limited in scope. Nevertheless, it has been possible to present the practitioners' view together with some insider points. The implications of this research can help better understand the potential of considering applying more seriously- design learning for professionals in cyber careers. Of course, there is a need for more research data to advance this work and hereby once more, I join the call for further analysis and gathering of data. I hope the results of this research are valuable for the following stakeholder groups: decision-makers in the higher education sector and training providers, and professionals in cyber security, to request a clearer

education path using gamified cyber training for their careers as this is a finding from the focus of the study.

References

- [1] Catalui D. (2017). *Cyber security education in public administration. Case study on gamification methods used in Europe*. The EDULEARN conference proceedings.
- [2] Deterding, S. & Dixon, D. & Khaled, R. & Nacke, L. 2011. *From Game Design Elements to Gamefulness: Defining Gamification*. The 15th International Academic MindTrek Conference proceedings: 9-15. New York, NY: Association for Computing Machinery, <http://dx.doi.org/10.1145/2181037.2181040>.
- [3] Dirckinck-Holmfeld, L. & Hodgson, V. & McConnell, D. (2012). *Exploring the Theory, Pedagogy and Practice of Networked Learning*. New York. Springer.
- [4] Education Glossary (2013). Retrieved May 2019 from <https://www.edglossary.org/learning-pathway/>.
- [5] Elizondo, D. & Le Compte, A. & Watson, T. (2016). *A Renewed Approach to Serious Games for Cyber Security*. The 7th International Conference on Cyber Conflict: Architectures in Cyberspace Proceedings.
- [6] Esteves, J. & Ramalho, E. & De Haro, G. (2017). *To Improve Cybersecurity, Think Like a Hacker*. MIT Sloan Management Review. Cambridge 58.3, 71-77.
- [7] EU Agency - ENISA. *NCSS map*. Retrieved April 2019 from <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map>.
- [8] EU Agency -ENISA. *Network and Information Security quiz*. Retrieved April 2019 from www.enisa.europa.eu.
- [9] EU Agency -ENISA. *Network and Information Security Education map*. Retrieved April 2019 from www.enisa.europa.eu.

- [10] EU Agency -ENISA. *Cyber Europe exercise*. Retrieved April 2019 from www.enisa.europa.eu.
- [11] European Commission. *CyberReadyGame*. Retrieved April 2019 from <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3296029>.
- [12] Harvard Business Review (2017). *Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It, 2017*. Retrieved April 2019 from <https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it>.
- [13] International Telecommunication Union- ITU (2017). Retrieved April 2019 from <http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx>.
- [14] Kapp, K. M. (2012). *The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education*. San Francisco, CA. Pfeiffer (Wiley).
- [15] Mackenzie A. & Makramalla M. (2015). *Cybersecurity Skills Training: An Attacker-Centric Gamified Approach*. Technology Innovation Management Review.
- [16] Ruboczki E.S. (2016). *Serious games experience in teaching cloud security*. Obuda University, Hungary. Retrieved April 2019 from <https://library.iated.org/view/RUBOCZKI2016SER>.
- [17] Zyda M., (2005). *From visual simulation to virtual reality to games*. Computer, vol. 38, no. 9, pp. 25-32.
- [18] Wenger, E. (2006). *Communities of practice: A brief introduction*. Retrieved April 2019 https://link.springer.com/referenceworkentry/10.1007/978-3-642-28036-8_644.
- [19] World Health Organisation - WHO (2019). Retrieved April 2019 <https://www.who.int/features/qa/gaming-disorder/en/>.

How Botnets are Affecting Us and How to Protect Against Them

Mădălin VASILE
Fortinet, Romania
mvasile@fortinet.com

Have you ever asked yourself if someone else has access to your gadgets without your approval and your knowledge? Do you have any tools to verify if your device was compromised or not?

In this article, I will give you insights on what a botnet is and how to protect yourself and make sure that you minimize the risk for your device to be part of a botnet.

Technology is under constant evolution and we are using more and more Internet connected gadgets in order to optimize our time, improve our productivity, ease the communication, improve our fitness results, automate processes at home and office and, why not, share easier our experiences and thoughts.

With so much technology and the benefits derived from it, it comes also a great risk in exposing our resources without our explicit consent and awareness, because most of the people are not considering securing these gadgets, but they are more focused on the benefits that come out of using them.

What is a botnet? With so much technology being exposed unprotected on the Internet, a malicious user can build an enormous network of processing devices that he can use and exploit for his own agenda, like gathering data that he can later sell, deploy malware, steal confidential information, launch attacks on others, rent by the hour the processing power of the distributed network that he just built.

A simple definition for Botnet is: an army of intelligent devices that can be centrally controlled to achieve a certain purpose, without the approval or knowledge of the legitimate owner.

How a botnet can be created? The term Botnet is a general name, but there are specific botnets like Mirai, Reaper, OMG (Oh my God) and in order to understand the term better, we will analyze the specifics of the mentioned Botnets and how they can be built.

Mirai - this botnet is built after scanning the internet for gadgets and smart devices that run on ARC processors. The idea behind is to try to access the smart devices, that run on a Linux version, via the default credentials and try to infect them with malicious software (malware).

What kind of smart devices can be a target? Any Internet connected device can become a bot, if compromised, and the list of devices can include home wireless routers, fitness gadgets, smart TVs, smart home appliances (fridge, air conditioning, and coffee machines), smart cameras, digital video recorders, baby monitors, environmental monitoring devices, medical devices and the list can continue.

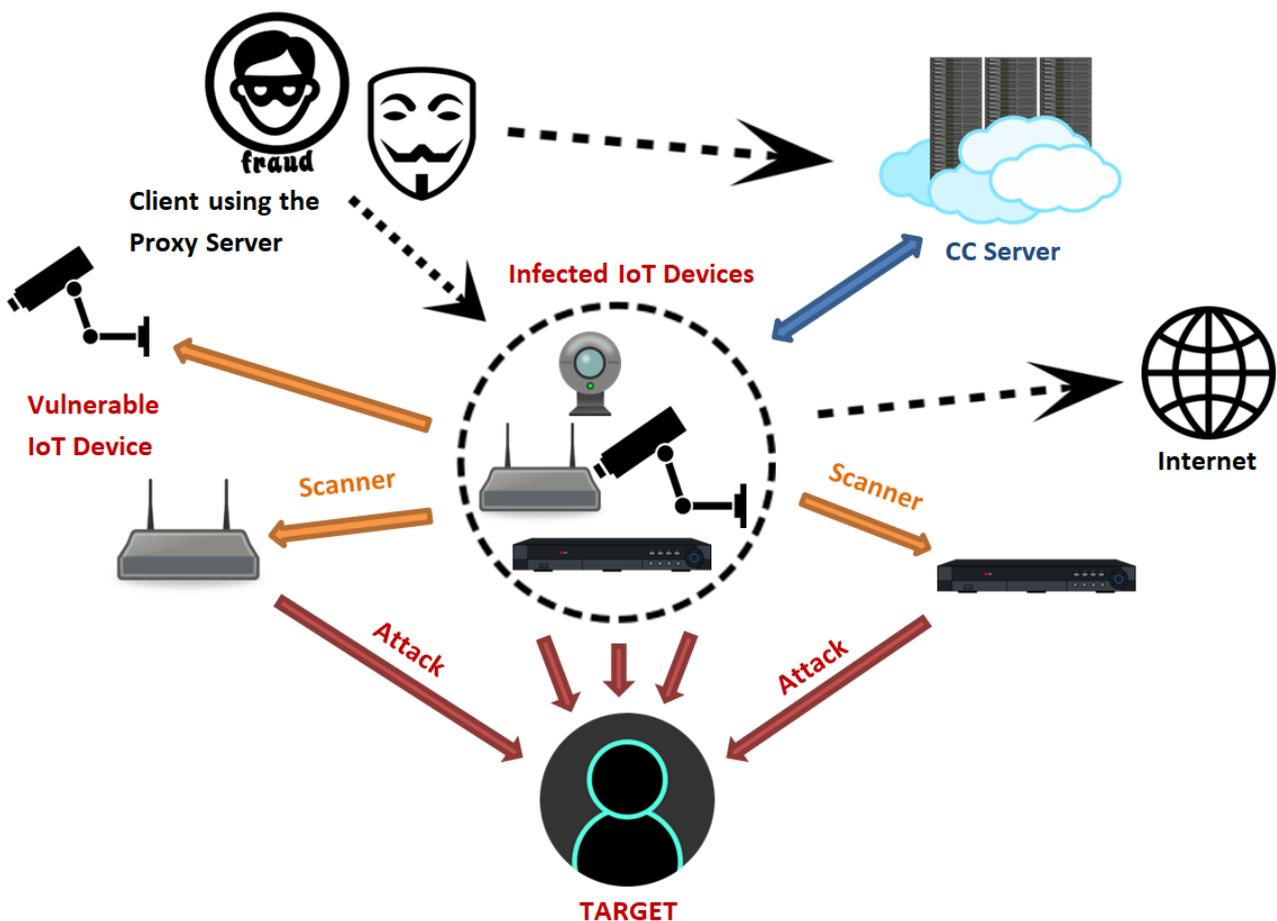


Fig. 1. The Botnet Ecosystem and workflow [1]

The **Mirai** botnet was originally created in 2016 and reached 500 000 devices shortly, with an estimated total of 2.5 Million devices at the end of 2016. Mirai was used to launch DDoS attacks (distributed denial of service) on the DNS providers and affected Github, BBC, Spotify, Xbox Live.

Dyn, a DNS service provider, was targeted by 1.1 Terrabyte DDoS attack launched using the Mirai botnet and affected completely its services. Although the services were reachable, the legitimate DNS queries could not be completed due to the high number of malicious requests.

The same botnet was also involved in taking down the Internet in Liberia, an African country with a population of about 4 Million people. The largest communication provider in the country, Lonestar MTN was targeted by 500 Gbps DDoS attack that affected the cross-country communications.

Another botnet that leverages Mirai is **OMG (Oh My God)**, an improved version that can kill processes (telnet, ssh, http and more), can brute-force login in order to spread itself, can launch DDoS attacks, and then can also transform the vulnerable devices into proxy servers. This means that virtually, an infected device can be used as proxy to mask malicious activities for attackers around the world or it can be used as anonymous proxy even for legitimate traffic, but without the consent of the legitimate owner or user.

The Mirai evolution doesn't stop here and continues with **Wicked, Sara, Owari and Omni**, and in the future with many other versions as any payload (malicious code) can be updated to the exploited devices. Most of the latest Mirai versions are using the scanner to identify the potential devices to be infected and are using as infection point the exploit of known vulnerabilities, although most of them are quite old.

Now, that we've seen different versions of Botnets and how they are spreading, let's see how actually a Botnet can be used.

Once a device is compromised using their specific method, the bot has to register to the **Command and Control server (CNC)**. The address of the server is coded into the payload downloaded on the compromised device. The payload can load different versions of malware which can build different Botnets. Once the CNC servers receive

the new bot registration from the infected device, it can reply with the action for this new bot. Some examples of possible actions, which represent also the bot purpose, are: proxy, launch attacks or even teardown the connection.

By renting the army of botnets, a malicious user can launch **distributed denial of service attack (DDoS)** from real devices, with spoofed origin or real source and take down the targeted service, which can be a bank website or service, webhosting infrastructures, service providers networks, government agencies infrastructure, online gaming platforms, online casinos, universities infrastructure or, in summary, any service that is publicly available on the Internet.

Another use for botnets is **data exfiltration**. Once a hacker or malicious user has gained access to personal records or information, he/she needs to extract that data to an external location so it can use it or sell it later. Usually data exfiltration and DDoS attacks come together, and the attacks purpose is to mask the data exfiltration while the Networking and Security professionals are trying to mitigate the attack and restore the targeted service. Usually the attackers are not extracting the entire databases at once, but they are pacing their effort and extract just a small amount of data, so the outgoing internet bandwidth will keep the normal value range and will seem like being just the legitimate traffic. Personal data records are targeted because they can be sold in bulk for lots of money. The data records that have value and can be a target for attackers are: social security information, health and medical records, tax information, salary information, education records, bank records, home and work address, pictures, location, phone agenda, contacts, credentials - usernames and passwords, confidential files, emails and more.

In order to steal some of the mentioned records, sometimes there is a need for additional malware to help extract this data, and even this **malware will be distributed** by using the botnet. Among the malware variants distributed by botnets, the most recent types are used for **crypto currency mining, crypto jacking and ransomware**.

After understanding how the botnets can be used, the results of using them are easy to summarize:

- Botnets can help to steal important records that will be sold and can be further used for identity theft, unauthorized payments and more;
- They can help to take down completely or partially an Internet Service Provider or more providers in the same region in order to limit the access to Internet. It is possible to take down the Internet service in an entire country
- They can block or restrict online legitimate business and ask for ransom in order to stop the attack and restore the service.
- Botnets can also help in malware distribution and automate a large-scale attack. Ransomware can be distributed in this way and legitimate users can lose access to their important files, to business and personal information.
- Malicious attackers will be hard or impossible to identify while using anonymous proxies over the distributed botnet.

So who is really affected by botnets? The answer is quite simple: everyone using or needing internet service - a person, a company, an Internet Service provider, government agencies, shipping companies, entire countries. While the botnet itself is not malicious, I can say that by exploiting these vast networks of Internet exposed devices, virtually, nobody is safe from botnets.

Who can rent the botnet? Anybody with a purpose and a grudge and with some money can rent the botnets, the cost depending on the resources needed like the number of hosts, type of hosts, Internet bandwidth, time interval and tools to control these entire networks and take down the targeted service. The profile of the botnet rental person can be a student taking down an online exam platform, it can be an employee that was fired, it can be a bored kid on the Internet, hacktivists and political activists that are trying to prove a point, hackers trying to monetize their activity, companies trying to take down or slow their competition, and the list can continue.

At this point we understand what a botnet is, how it is built, how it can be used and why, but the remaining open question is: **Why someone can build a botnet?** While the question seems complex, the answer can be summarized by the lack of security knowledge and discipline and unfollowed best practices. The easiest way to start building such a botnet is by exploiting weak or unchanged passwords or by

targeting unpatched operating systems on the Internet connected devices. Once the access is granted to the device, this can be enrolled in different botnets and start working for the botnet master or renter.

How can we protect our devices against botnets or against enrollment in botnets? Depending on our skills, knowledge and available tools, we can start protecting our devices by following few simple rules:

Each individual can make sure that is following few basic ground rules at home:

- Make sure that you change the administrative passwords for your home wireless routers. Each vendor has a well-known default administrative username and password, that is publicly available and anyone can use these credentials to log remotely or locally to your router.
- Make sure you are using a strong password, by using more characters, combine big and small caps, numbers, special characters and change this password regularly;
- Disable administrative access from Internet or from wireless; restrict it to specific IP addresses if possible;
- Make sure your router is up to date with its software by doing regular updates. If the software is out of support, consider replacing the device, even if it is properly functioning.
- Make sure that your laptops and PCs are up to date with operating systems and with the 3rd party software like Internet browsers, media players, Java, Flash, document processing tools and more;
- Use endpoint protection software that can block viruses and malware and potentially help maintain an up to date and patched system;
- Use software that is blocking access to malicious websites;
- Update your smart devices to the latest software and update the installed application as well. Don't install software on smart devices unless you trust the source and programmer. Use only validated applications from legitimate application stores. Never root your device in order to install an application. A

routed device is the most vulnerable and can be controlled or programmed with persisting software even after reboot.

- If you are using smart home appliances that can be controlled or programmed from a portal, make sure that this is not available on the Internet, but through a VPN and use two factor authentication (token) in order to secure the login. In this environment use a dedicated SSID only for these devices and use strong password on the SSID.

While at home we can rely on our expertise, **at work** we can have at our disposal more advanced tools and dedicated people who can help us in protecting our devices, by applying all best practices listed above and enhanced them with few more:

Implement Next Generation Firewall and filter out the connections from and to known botnets; implement a virtual patching system (IPS) in order to protect the devices that can't be patched or don't have software patches available;

- Implement a centralized and automated patch management system;
- Implement a sandbox solution in order to detect advanced or zero-day malware;
- Segment your network in order to contain a vulnerable segment in case it happens;
- Implement a network access control system in order to limit or to profile the devices that are trying to connect to your network;
- Advanced malware like crypto miners and crypto lockers can be detected by using behavior detection at endpoint level;
- Moving further, our Internet Service Provider or webhosting provider can help us protect against botnets by deploying advanced systems or technics that can help filter out connections:
 - from botnets by using IP reputation databases;
 - to botnet domains by using filtering at DNS requests level;
 - to malicious websites by using website reputation databases and Indicators of Compromise for legitimate but exploited websites.

Botnet spread and monetization is possible due to collaboration amongst malicious actors, but in the same way, the network and security vendors developed strong collaboration for cyber intelligence and information sharing in order to detect faster the malicious activity and to deliver better protection for their customers. Such collaboration is possible amongst the Cyber Threat Alliance members who share the knowledge, resources, discovered zero-day vulnerabilities and threat feeds.

For an efficient protection it is necessary a collaboration with the Internet Service Provider that can help mitigate earlier some of the risks by blocking the connection to and from botnets, and also it is mandatory that the network and security vendors to collaborate in order to identify early different type of botnets, disclose them and start protecting against them depending on their specifics.

Even if attackers have automated tools at their disposal and virtually enough time to build and maintain the botnets, we, as individuals, can protect ourselves against the negative effects that they create. How do we do that? By implementing security best practices and by maintaining a good security discipline.

Botnets are becoming more and more complex, which makes their detection harder, but by deploying security solutions that are using Artificial Intelligence and Machine Learning, we can prevent and detect future botnet activity and protect against the illegitimate use of our devices.

Be aware and start protecting yourself!

References

- [1] Jasper Manuel, Rommel Joven, Dario Durando, “OMG: Mirai-based Bot Turns IoT Devices into Proxy Servers.” Available: <https://www.fortinet.com/blog/threat-research>.
- [2] Rommel Joven, Kenny Yang, “A Wicked Family of Bots”. Available: <https://www.fortinet.com/blog/threat-research>.



INNOVATION AND RESEARCH



INNOVATION AND RESEARCH

Cybersecurity in EU Framework Programmes for Research and Innovation

Claudiu CHIRIAC

Directorate General Logistics, Ministry of Internal Affairs, Romania
claudiu.chiriac@mai.gov.ro

1. Horizon 2020 - a brief introduction

Information and communication technology has always been a priority for R&D framework programmes. H2020 - EU's 8th Framework Programme for Research and Innovation - is no exception, having two main pillars dedicated to ICT - Societal Challenges and Industrial Leadership. Between 2014 - the launching year of the calls funded under H2020 - and 2018, the financed projects totaled over €3 B, which represents 7.88% of the general budget. According to Horizon 2020 - work programme 2018-2020 for secure societies, the majority of Member States rely entirely on the 8th Framework Programme to cover their needs for innovative security solutions, and it represents 50% of the overall public funding for security research in EU. Starting with April 2016, a new priority arose on the Commission Agenda - to boost the effectiveness of the Security Union (SU). In order to foster the implementation of the SU, a focus area was set up with 6 priorities, 3 of them being centered on cybersecurity. The 2018-2020 working programme also underlines that the expected impacts are the following:

- key infrastructure better protected against natural and man-made threats, including cyber-attacks;
- new products that meet the needs of security practitioners in the EU, including for investigating and prosecuting crime (including cybercrime) and terrorism;
- ensuring a secure and trusted networked environment for the governments, businesses, and individuals, thus positioning the EU as a world leader in building a more secure digital economy.

According to H2020 Qlik Sense portal [1], between 2014 and 2018 there were 843 signed grants in information and communications technology (ICT) and digital security (DS) topics altogether, distributed as presented in Figure 1.

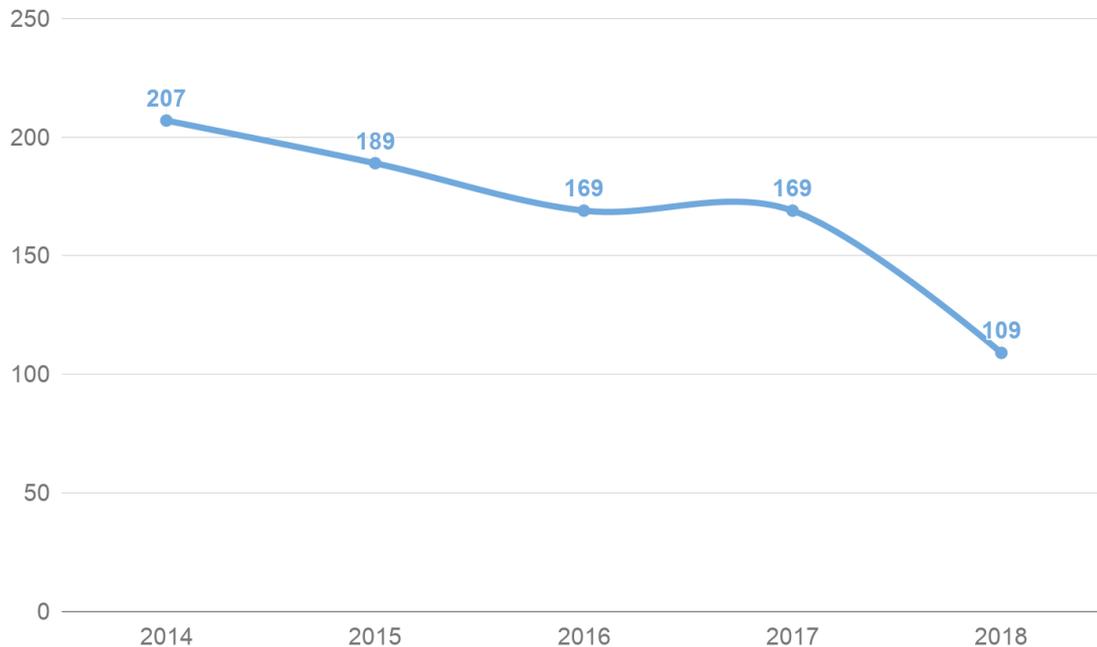


Fig. 1. H2020 signed grants in ICT and DS topics

The trending line is descending in this timeframe, being constant only in 2017. What is not presented in this graphic is the evolution of the funding scheme. If in 2014 there were 207 funded projects totaling € 659M, in 2018 the total number halved but the top 5 projects funded under Horizon 2020 were financed in 2018 - 5G-MOBIX (€ 21.5 M), AI4EU (€ 20 M), 5G-VINNI (€ 20 M), 5GENESIS (€ 15,7 M), 5G EVE (€ 15,7 M), but the funding remained almost constant.

What it can be observed when running the numbers is that European Commission managed to shift the trends in research and development by reducing the number of relatively small, peculiar projects while increasing the financing for the mainstream topics like 5G.

2. Cybersecurity-related projects funded under H2020

According to Community Research and Development Information Service Portal (CORDIS) [2], since the beginning of the 8th framework programme - 2014 -

the total number of the projects funded under Horizon 2020 was 23143, out of which 928 were related to ICT and DS.

Among these, there are projects such as CS-AWARE - A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis. According to CORDIS factsheet, the project benefits from an EU contribution consisting of € 3.7M, spread over three years, starting with 2017, and it is in the implementation phase with the grant agreement number 740723 [3]. CS-AWARE is funded under the digital security topic (DS-02-2016 Cyber Security for SMEs, local public administration and Individuals), using an innovation action (IA) funding scheme. As opposed to a research and innovation action (RIA) where the EU contribution can be up to 100% of eligible costs, in the case of IA, the EU contribution is maximum 70% of eligible costs [4].

CS-AWARE is about helping the local public administration to deal with red tape when it comes to the legal framework in the field of cybersecurity. According to the project website, what the consortium proposes is a situational awareness solution for small-medium IT infrastructures at the level of local public administrations that will detect incidents and facilitate information exchange with relevant national and EU level network and information security authorities such as computer emergency response teams [5].

In the deliverable D2.1 of the project, the main threats identified for the local public administration were cyber criminals, insiders, hacktivists and script kiddies [6]. The threats have been identified by applying the ENISA model to local public administration, as presented in Table 1.

Table 1. ENISA model applied to local public authorities

	Threats							
	Cyber-criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber-fighters	Cyber-terrorists	Script kiddies
Malware								
Web-based attacks								

	Threats							
	Cyber-criminals	Insiders	Nation states	Corporations	Hacktivists	Cyber-fighters	Cyber-terrorists	Script kiddies
Web application attacks								
Denial of Service								
Botnets								
Phishing								
Spam								
Ransomware								
Insider threat								
Physical manipulation / damage / theft / loss								
Exploit kits								
Data breaches								
Identity theft								
Information leakage								
Cyber espionage								
Primary group for threat Secondary group for threat								

GHOST project intends to bring corporate level security to citizens’ smart homes. Basically, with this solution, the residents will be able to monitor and avoid different threats that occur with their own IoT devices [7]. According to CORDIS factsheet, the project benefits from an EU contribution consisting of € 3.6M, spread over three years, starting with 2017, and it is in the implementation phase with the grant agreement number 740923 [8]. GHOST is funded under DS-02-2016, with 30% co-financing from the project consortium. The project will be tested smart homes throughout Europe, including Romania, using different networks such as the Red Cross, and the network of the project coordinator.

REACT project (grant agreement ID 786669) proposes another approach to cybersecurity - instead of concentrating all efforts to a cyber-attack that just occurred another perspective is to use the advanced and modern tools in order to anticipate where and when the attackers will strike again [9]. The project benefits of 100% non-refundable budget via a research and innovation action, under DS-07-2017 topic (Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors). The expected end date of the project is May 2021 and it has as coordinator the Foundation for Research and Technology Hellas.

The CANVAS project (grant agreement ID 700540) is built around EU core values - equality, fairness, and privacy - in order to outline problems related to value-driven cybersecurity [10]. This is an ongoing project started in September 2016, funded under DS-07-2015 - Value-sensitive technological innovation in Cybersecurity with a € 1M budget from EC. According to the projects' website, in 2019 the CANVAS consortium will publish a book on ethics related to cybersecurity - CANVAS book, together with a massive open online course containing case studies from health, business, and national security domains [11].

While the main general objective continues to be the strengthening of the cybersecurity, there are also projects like Cyberwatching.eu and EUNITY that focus on the bottom-up approach by monitoring research initiatives on cybersecurity or fostering the dialogue in the cybersecurity area between EU and different countries such as Japan.

3. The next programming period - Horizon Europe

Horizon Europe is the next Framework Programme, the Commission proposal for a € 100 billion research and innovation funding instrument for seven years (2021-2027) [12]. The programme will have a three-pillar structure. The first pillar will ensure the proper cohesion with Horizon 2020 - open science - this will comprise the European Research Council (ERC), Marie Skłodowska-Curie Actions (MSCA) as well as research infrastructures. The second pillar - Global Challenges and Industrial Competitiveness - will deal with a more in-depth approach of societal challenges and

industrial technologies while the last one - open innovation - will settle the European Innovation Council that will bring ideas from lab to real world [13]. The cybersecurity-related topics from Horizon 2020 - DS and ICT - topics will be integrated into the second pillar, within the second cluster - Inclusive and Secure Society - and considered as distinct areas of intervention, with a budget consisting of € 2.8B [14]. Specifically, according to the Commission proposal for Horizon Europe, the term of digital security (DS) seems to be included in the cybersecurity area of intervention for the 2021-2027 multiannual financial framework (MFF) while the ICT probably will be distributed in the digital and industry cluster, within areas of intervention such as key digital technologies, artificial intelligence and robotics, next generation internet, and advanced computing and Big Data.

The Horizon Europe programme is still in beta version but the major decisions have been already taken and cybersecurity seems to be on the right track with its own area of intervention, unlike in the current framework programme where is dispersed in two main pillars - Societal Challenges and Industrial Leadership.

References

- [1] QlikTech International AB, "H2020 projects," QlikTech International AB, 12 April 2019. [Online]. Available: <https://webgate.ec.europa.eu/dashboard/sense/app/93297a69-09fd-4ef5-889f-b83c4e21d33e/sheet/erUXRa/state/analysis>. [Accessed 14 May 2019].
- [2] European Commission, "CORDIS - EU research projects under Horizon 2020 (2014-2020)," Community Research and Development Information Service, 13 May 2019. [Online]. Available: <https://data.europa.eu/euodp/en/data/dataset/cordisH2020projects>. [Accessed 30 May 2019].
- [3] European Commission, "A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis," 4 May 2017. [Online]. Available: <https://cordis.europa.eu/project/rcn/210224/factsheet/en>. [Accessed 6 May 2019].

- [4] European Commission, "Horizon 2020 Factsheets - Grants," 26 December 2016. [Online]. Available: http://ec.europa.eu/research/participants/data/ref/h2020/other/gm/h2020-grant-factsheet_en.pdf. [Accessed 2 May 2019].
- [5] CS-AWARE Consortium, "CS-AWARE Project Objectives," CS-AWARE Consortium, 2 December 2017. [Online]. Available: <https://cs-aware.eu/objectives/>. [Accessed 4 May 2019].
- [6] S. Thomas, W. Chris, K. Veronika and P. Alex, "D2.1 System and dependency analysis (first iteration) - Cybersecurity requirements for local public administrations," 28 February 2018. [Online]. Available: https://cs-aware.eu/wp-content/uploads/2019/03/D_2_1.pdf. [Accessed 7 May 2019].
- [7] Televés, "About GHOST," Televés, 3 June 2017. [Online]. Available: <https://www.ghost-iot.eu/ghost-project>. [Accessed 16 May 2019].
- [8] European Commission, "Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control," 23 June 2017. [Online]. Available: <https://cordis.europa.eu/project/rcn/210233/factsheet/en>. [Accessed 12 May 2019].
- [9] European Commission, "REactively Defending against Advanced Cybersecurity Threats," 6 June 2018. [Online]. Available: <https://cordis.europa.eu/project/rcn/214838/factsheet/en>. [Accessed 3 May 2019].
- [10] European Commission, "Constructing an Alliance for Value-driven Cybersecurity," 14 July 2017. [Online]. Available: <https://cordis.europa.eu/project/rcn/202697/factsheet/en>. [Accessed 5 May 2019].
- [11] CANVAS consortium, "Constructing an Alliance for Value-driven Cybersecurity," 2 February 2017. [Online]. Available: <https://canvas-project.eu/>. [Accessed 9 May 2019].
- [12] European Commission, "Commission proposal for Horizon Europe," 25 June 2018. [Online]. Available: https://ec.europa.eu/info/sites/info/files/horizon-europe-presentation_2018_en.pdf. [Accessed 20 March 2019].
- [13] European Commission, "Proposal for a regulation of the European Parliament and of the Council Establishing Horizon Europe," 7 June 2018.

[Online]. Available: https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-horizon-europe-regulation_en.pdf. [Accessed 2 May 2019].

[14] European Commission, "Commission proposal for Horizon Europe," 25 June 2018. [Online]. Available: https://ec.europa.eu/info/sites/info/files/horizon-europe-presentation_2018_en.pdf. [Accessed 9 May 2019].

The Communications Future. 5G Between Benefits and Cybersecurity Challenges

Virgilius STĂNCIULESCU

National Authority for Management and Regulation in
Communications of Romania (ANCOM)
virgilius.stanciulescu@ancom.org.ro

Approaching the days and more exactly daily habits will change substantially with the development of technology that will connect everything that surrounds us. With 5G networks, connections will be faster, things that play a role in day-to-day comfort will be connected, with benefits little understood or known to each of us.



For telecommunication network operators, the fiber optic network and fixed-to-mobile integration work together to open the way to 5G and beyond, or to keep up with the speeds needed to transport huge amounts of data, with minimal delay (milliseconds) and a massive number of connected elements.

It is not long before we have access to services supported by this technology, and in this article I will briefly review both the benefits and the vulnerabilities that we will have to take into account as IT & C security specialists.

1. Background info

The following bands have been identified at European level as priority bands for the early introduction of 5G mobile communications systems in the Union: the 700

MHz (694-790 MHz) band, the 3400-3800 MHz band and the 26 GHz (24.25-27.5 GHz).

The 700 MHz (694-790 MHz) band is very important for providing extended coverage, especially in economically challenging areas, such as rural, mountainous or other remote areas. The band is adequate for ensuring efficient coverage over wide areas and improved indoor coverage, being suited both for enhancing and improving the quality of mobile communications services offered by 4G technologies, and for the deployment of next-generation mobile communications technologies known as 5G or IMT-2020. The frequencies in the 700 MHz band will expand the spectrum resources below 1 GHz already used for the provision of broadband mobile communications services through LTE technology and will facilitate the deployment of 5G networks, and the widespread introduction of innovative digital services.

The 3400-3800 MHz band is deemed an appropriate primary band for the introduction of 5G services before 2020, as it offers large radio channel bandwidths and a good coverage/capacity balance, ensuring significant capacity growth and supporting enhanced broadband communications, as well as applications requiring low latency and high reliability, such as mission critical applications (industrial automation and robotics).

The 26 GHz band is considered to be a “pioneer” band for early 5G harmonization in the EU by 2020, as it offers more than 3 GHz of contiguous spectrum and enables the provision of ultra-high-density and very high-capacity networks over short distances, as well as revolutionary 5G applications and services, which involve very high data transfer rates, increased capacity and very low latency.

Here are the steps taken or in progress to implement the next generation of communications networks in Romania: ANCOM has debated and adopted, in a Consultative Council session together with the industry, the national action plan and schedule for the allotment of the 470-790 MHz frequency band as well as the associated regulatory options, in the form of a National Roadmap for the Allotment and Future Use of the 470-790 MHz band. "In the consultation on the 700 MHz band, we actually agreed on the schedule for making available the radio spectrum needed to implement

5G technology in Romania. We will complete the whole documentation of this auction, including reserve prices, by July 2019 and we will finalise the spectrum auction no later than December 2019," said Sorin Grindeanu, president of ANCOM (www.ancom.org.ro English version).

Schedule of actions on the allotment and future use of the 470-790 MHz band

An essential first step is the timely release of appropriate radio spectrum for the future development of mobile broadband systems. In order for the 700 MHz band to be available, ANCOM will propose amendments to the NTFA (National Table of Radio Frequency Allocations) and the allocation of the 790 MHz band to the land mobile service, as the band is allocated to digital terrestrial television services at the moment.

By the end of this year, ANCOM will develop and adopt a national position on the allotment and future use of radio frequencies available in the 700 MHz, 800 MHz, 1500 MHz, 2600 MHz, 3400-3600 MHz and 26 GHz frequency bands for broadband wireless electronic communications systems.

Another action with impact on the implementation of 5G technologies is the conclusion of bilateral co-ordination agreements with the neighboring countries, by 30 June 2019. Moreover, ANCOM will carry out a radio spectrum monitoring campaign in the frequency bands to be auctioned out and will make available to the bidders a report on the status of the radio signals identified on the territory of Romania in these bands, coming from the territory of other states.

By 31 July 2019, ANCOM will adopt the decision on the organization of the licensing procedure, namely the establishment of the conditions for awarding the frequency use rights and other necessary normative acts.

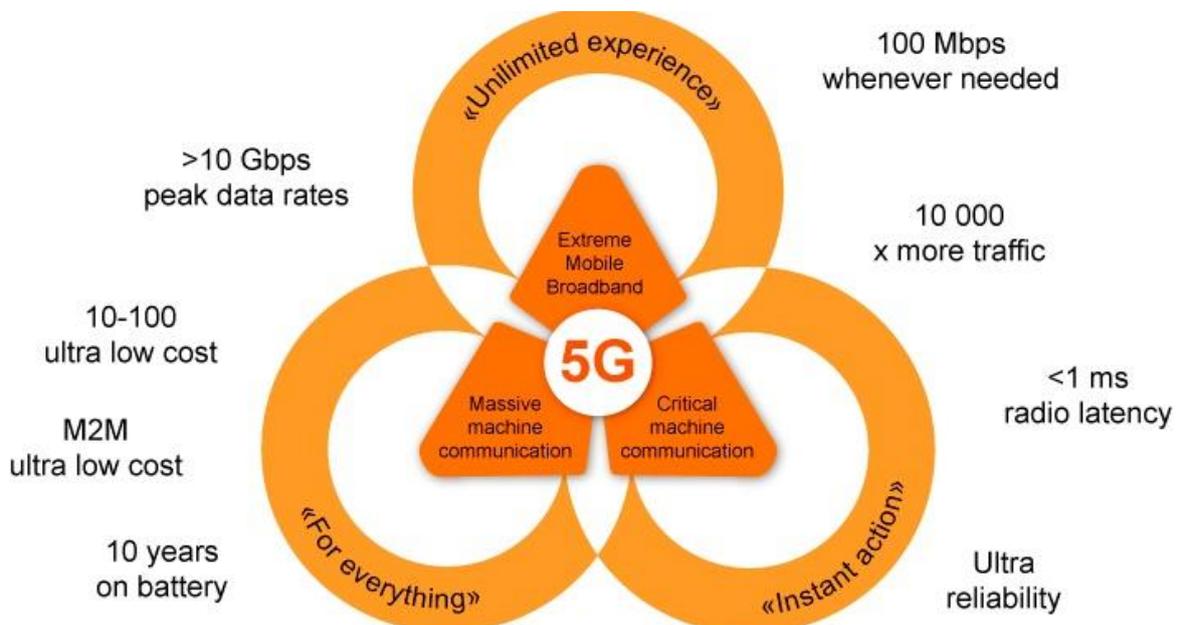
According to the Authority's proposal and following debates with industry representatives, the auction for awarding frequency use rights in the 700 MHz band and in the other frequency bands envisaged for the provision of fixed and mobile communications within the scope of 5G technology will be finalized by 15 December 2019.

The National Roadmap for the Allotment and Future Use of the 470-790 MHz Frequency Band is available on www.ancom.org.ro

2. 5G will bring to us benefits and opportunities

The experts announced amazing performance:

- The number of interconnected devices will increase becoming multiplied with hundreds compared to now. This is also in conjunction with IPv6 adoption.
- The volume of data can increase in the future multiplied by thousands compared to the actual moment
- Data processing speed: 10Gbps, but experts estimates that will be even higher.
- Reduced latency: Latency, known as "lag", is the time it takes for data to arrive from the transmitter to the receiver. Obviously, the smaller it is, the faster the connection will be. At the level of a regular user who uses a device connected to the Internet, the values of this feature via 4G is quite difficult to see, but for the Internet of Things, a lower latency is a very important aspect. The 5G latency is expected to be 1 millisecond (ms), much lower than the human audio perceptual capacity, and for comparison, the 4G latency is between 20 and 50 ms.
- Reduced energy consumption.



We've all heard about the exciting new services that 5G will bring, from connected vehicles to smart manufacturing. While some advanced industrial services will take five to ten years to emerge fully, 5G offers plenty of near-term value. However, this is not well known. According to a recent survey by GSMA, consumers think 5G is just a faster version of 4G. In fact, only 25% of people understand the true value that 5G can bring. They're in for a pleasant surprise.

Applications in: industry, entertainment, safety, medicine

5G will greatly enhance mobile user experience. It will enable new services such as cloud-based virtual reality (no more clunky headsets), cloud PC (it gives your phone the same processing capabilities as a laptop) and ultra-high definition video, wherever you go.

5G will improve the efficiency of spectrum use tenfold and network capacity by 20 to 30 times, allowing operators to provide consumers with better service at a lower price. There is no doubt that 5G is already delivering economic value for consumers, telecoms operators and vertical industries. 5G will be deployed in about 110 markets by 2025, according to GSMA.

ENTERTAINMENT

The listed technical features will make it possible to access high-speed mobile internet even in crowded areas: concerts, festivals, sports events without being affected by speed limitations, interference, or signal instability. For example, a download of 4K resolution movies will be a matter of seconds.

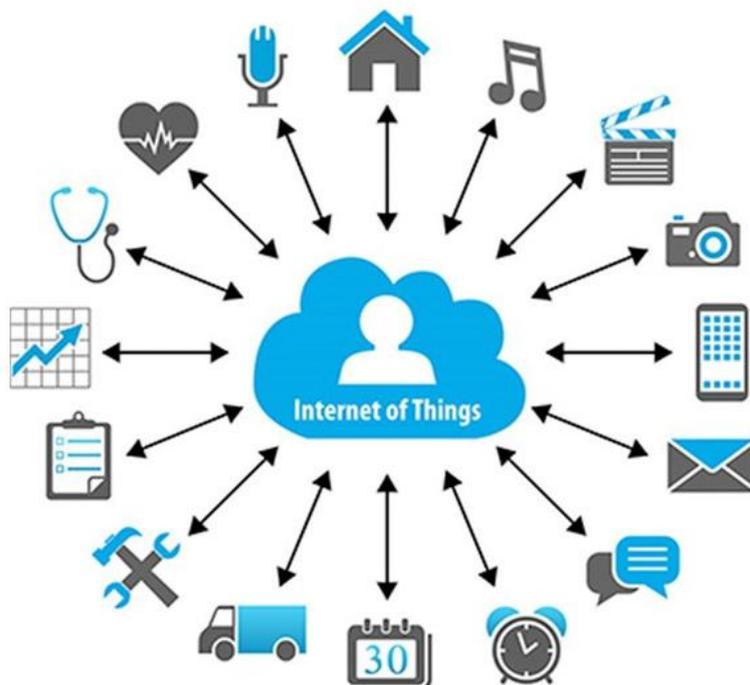
On the other hand, live TV shows and sports events will become real immersive, augmented or virtual visual experiences, even for those who will not personally participate in real life, offering the possibility of virtual, sensory participation in real events. Sounds good, right? Well experiments and demonstrations have shown that it is possible, and the penetration of these experiences in everyday life will also depend on the absorption and consumption capacity of end users. In the testing period, an operator from Romania made an experiment with a rock concert with a hologram!

In November 2018, the UK's largest operator BT/EE broadcast the Wembley Cup Final live in high definition over a commercial 5G network. Because 5G is so fast and experiences so little delay in signal transmission, BT was able to produce complex effects that made the game more interesting to viewers, but it could do all the production remotely, without having to drag heavy equipment to the game site.

Going beyond the TV screen, 5G-enabled virtual reality (VR) applications will also let sports fans watch games from the perspective of their favorites players - or that of the ball itself. This will completely change how we experience sports, while opening up new revenue streams for telecoms operators and other companies along the value chain.

INTERNET OF THINGS and INTERNET OF EYES

Dynamic traffic monitoring, traffic management, and public security (so-called Internet of Eyes concept) will be possible or expanded: object detection and positioning in real-time, and we will also witness an explosion of applications and frameworks dedicated to smart city, smart home, smart building, because technology will be the backbone of IoT (Internet of Things), connecting objects around us in ways that we would not have thought possible.



We will assimilate technologies of the future that will allow independent vehicles to interact with traffic lights, infrastructure, communicate with each other, based on systems with Artificial Intelligence or Augmented. In addition, sensors integrated into roads, railways and flight paths will communicate with each other and intelligent vehicles to improve infrastructure control and critical services.

New generation of network will produce another revolution in business processes. High speeds and a short response time will ensure the mass deployment of robots and the Internet of Things. Modern business has long been digitized and needs a new round of productivity.

And the 5G has all the chances to do it. Despite the whole hype about the Internet of Things, it is not yet possible to combine wireless objects into a single network. The lack of a single IoT standard prevents this. Wearable devices work through Bluetooth, smart homes - via Wi-Fi, in other segments several protocols are used at once.

Especially the 5G is useful in those IOT segments where the objects are heavily removed (for example, in agriculture) or a fast reaction is required (for example, for driverless vehicles). There are also applications in the field of agriculture where moisture sensors, automatic fertilizer distributors, artificial intelligence entities specializing in predictions will intervene for the regulation, control and maximization of results.

Moving, self-contained, remote-controlled flying vehicles and their traffic management will also be driven by systems that communicate large amounts of data, but especially in real time.

We can say that 5G will multiply the known advantages of the Internet of Things and will bring its widespread.

The high data transfer rate in 5G networks will sharply increase the load on the infrastructure. This will require significant efforts and investments from mobile operators. Mass introduction of IoT will enrich the suppliers of cloud technologies: smart devices will produce huge amounts of data and they will need to be stored somewhere.

How 5G will change our lives

Sphere	Effect
Driverless vehicles	elimination of dangerous signal delay at high speed
Industry	speed of industrial robots and the unification of infrastructure
Agriculture	remote management of agricultural machinery, monitoring of fields and herds
Education	visual training through VR-translation of the process from the point of view of the master
Telemedicine	real time remote operations
Communication	interactive virtuality: users will be able to interact at a distance as they are nearby
Entertainment	fast wireless video transmission of ultra-high definition (4K, 8K), broadcast events with the VR effect
Computer games	multiplayer VR-games without signal delay

INTERNET OF SKILLS

Expansion could exist according to tests and applications in the field of cloud-controlled robotics, more precisely the control of a remote robot.

Tests and demonstrations of medical operations, combined with virtual reality, have been carried out to create touch-based internet, such as remote and real-time transmission of touch sensation. Doctors will operate patients at a distance. They will use virtual reality helmets and special gloves, which will give them the feeling of grabbing the patient, but they can also act.



Using 5G, China Mobile has helped turn ambulances into mobile hospitals. Doctors at Zhejiang University School of Medicine in China can operate ultrasound equipment remotely through VR glasses, using a robotic arm to examine patients in ambulances as well as other locations. 5G is crucial here, as any delay in signal transmission can be disastrous for the patient, and only 5G networks are stable enough to allow doctors to perform such delicate procedures remotely.

In January 2019, doctors in the southeastern Chinese province of Fujian performed the world's first remote operation using a 5G network transmission. The successful operation (performed on a pig) marks the advent of 5G remote surgery, laying the groundwork for a wealth of innovative new clinical applications in the future.

One day, 5G networks will connect patients in remote areas with doctors around the world. People in the Gobi Desert and Arctic Circle will have access to the same level of care they could get in London or Dubai.

Carriers are also launching 5G pilot projects that connect students in poorer regions with some of the world's best teachers. Although high-definition video and VR can't be reliably delivered through 4G networks, high-powered 5G connections could benefit the children in underdeveloped regions, giving also to students a chance to receive a good education.

EXPANSION

It is estimated that by 2023, 20% of the world's population will have 5G coverage and 5G technology will generate \$ 1,200 billion worth of business by 2026

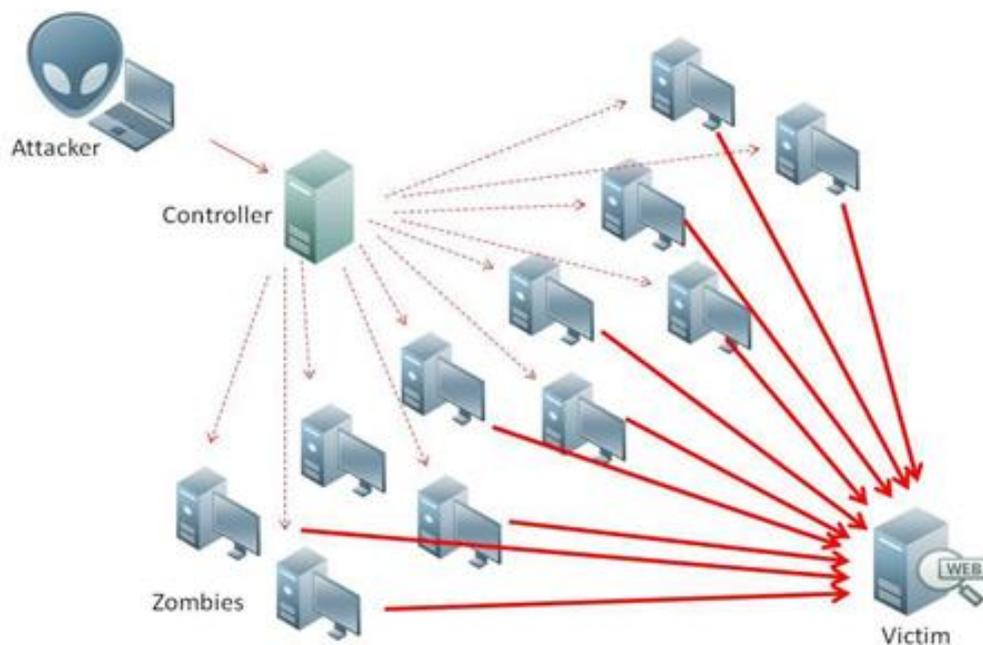
3. Vulnerabilities

Talking about vulnerabilities and associated risks, I identify at least two of their origins:

- one related to the application level, vulnerabilities associated with new types of services and applications;
- one related to the technical aspects of the technologies themselves, management modules or protocols.

Thus, linked to the first category:

- It can easily extrapolate the current known situation of malware infection of multiple IP devices or networks for DDoS (Distributed Denial of Service) attacks: increasing the number of interconnected devices will increase the critical mass of potential devices taken over in a Botnet network to initiate stronger attacks from even greater than present targets or potential targets, and attentively at a speed perhaps thousands times higher! From a technological point of view, attack-rejection equipment will have to keep pace, and physical detection, either based on artificial intelligence, will need to have an adapted response capacity.



- Information theft can reach immense levels: if we are talking about extortion of information and theft of personal data, traffic intercepts for password decryption or confidential information, in the case of the 4.0 industrial revolution that brings virtual prototyping and sending the online model directly on the manufacturing line, a man-in-the-middle attack could mean the theft of the model (intellectual property, industrial espionage) or worse, its distortion or replacement, the change of features before the physical execution begins. The results and negative effects can be immeasurable.

- Real-time intercepting / modifying data from traffic sensors, smart building, autonomous vehicle or flight controls would bring disasters and crimes to catastrophic or compromising critical infrastructure and endangering many lives.

- The real-time intercepting / modifying of data traffic associated with a remote operation is easy to imagine as effects, and unfortunately not very difficult to achieve, given the technology offers huge speed and response time close to zero.

Linked to the second category: ENISA already studied and made it public in a study “Signalling Security in Telecom SS7/Diameter/5G” (<https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g>):

- SS7 attacks can be complex as attackers are gaining more and more knowledge and as they had the time to develop effective attack scenarios. A basic protection will cover probably the majority of the attacks but will leave room for the complex or targeted attacks that can really cause damage at social, economic or political level (e.g. espionage etc.). As a conclusion, we can mention that in terms of SS7 minimum security measures are adopted by the majority of the providers. This conclusion is also reinforced by industry, through different industry papers, findings or other materials. Nonetheless, one problem arises from the fact that basic security measures are providing only a basic level of security. Also, SS7 infrastructure is quite old in some cases and not all equipment supports the adoption of security measures, not even the basic ones. This is also confirmed by the technical and cost related constraints explained in the study.
- Industry’s focus on Diameter security has come later than in the SS7 case, and has certainly not reached maturity yet. Diameter is derived from RADIUS (Remote Authentication Dial-In User Service) and provides an authentication, authorization, and accounting protocol for computer networks. In terms of design, it has borrowed many concepts from SS7, along with its vulnerabilities. Being a purely IP based protocol, there is an increased risk in the possibility of an intruder gaining access through hacking. The more knowledge the attacker has on Internet related protocols the more chances they have to succeed. This makes it in theory, simpler to exploit than SS7.

Considering the above, the conclusion might be that special attention must be granted to 5G security. As mobile plays a huge role in our digital society, assuring our

everyday digital infrastructure in support of the economy itself, the stakes are high. Older mobile generations have proven their drawbacks in terms security and the same approaches cannot be repeated anymore. As Diameter related vulnerabilities are beginning to be publicly uncovered the future use of this protocol or similar approached should be avoided. Carriers will need a new signaling architecture that can address the impact of introducing billions of roaming and static devices, the subscriber behavior and bandwidth requirements, and new applications.

ENISA recommendations are: “while work is being done in addressing SS7 and Diameter attacks, only a small portion of the protocols has been studied. It is expected that new vulnerabilities shall be discovered. In addition, tools to scan and potentially attack mobile networks are now freely available. 5G, the new mobile generation, is still under development. Early releases from some manufacturers are available but the standards are still in their infancy. Nevertheless, there is a certain risk of repeating history. Given the improvements that 5G will bring (more users, more bandwidth etc.) having the same security risks can be extremely dangerous.”

Security Challenges in SDN and NFV

SDN centralizes the network control platforms and enables programmability in communication networks. These two disruptive features, however, create opportunities for cracking and hacking the network. For example, the centralized control will be a favorable choice for DoS attacks, and exposing the critical Application Programming Interfaces (APIs) to unintended software can render the whole network down.

The SDN controller modifies flow rules in the data path, hence the controller traffic can be easily identified. This makes the controller a visible entity in the network rendering it a favorite choice for DoS attacks. The centralization of network control can also make the controller a bottleneck for the whole network due to saturation attacks.

Even though NFV is highly important for future communication networks, it has basic security challenges such as confidentiality, integrity, authenticity and non-repudiation. From the point of view of its use in mobile networks, the current NFV

platforms do not provide proper security and isolation to virtualized telecommunication services. One of the main challenges persistent to the use of NFV in mobile networks is the dynamic nature of Virtual Network Functions (VNFs) that leads to configuration errors and thus security lapses.

The main challenge that need immediate attention is that the whole network can be compromised if the hypervisor is hijacked.

Security solutions for SDN and NFV

Due to the logically centralized control plane with global network view and programmability, SDN facilitates quick threat identification through a cycle of harvesting intelligence from the network resources, states and flows. Therefore, the SDN architecture supports highly reactive and proactive security monitoring, traffic analysis and response systems to facilitate network forensics, the alteration of security policies and security service insertion.

Consistent network security policies can be deployed across the network due to global network visibility, whereas security systems such as firewalls and Intrusion Detection Systems (IDS) can be used for specific traffic by updating the flow tables of SDN switches.

The security of VNFs through a security orchestrator in correspondence with the architecture that provides security not only to the virtual functions in a multi-tenant environment, but also to the physical entities of a telecommunication network. Using trusted computing, remote verification and integrity checking of virtual systems and hypervisors is proposed to provide hardware-based protection to private information and detect corrupt software in virtualized environments.

Security Challenges in Communication Channels

Before 5G networks, mobile networks had dedicated communication channels based on GTP and IPsec tunnels. The communication interfaces, such as X2, S1, S6, S7, which are used only in mobile networks, require significant level of expertise to attack these interfaces.

However, SDN-based 5G networks will not have such dedicated interfaces but rather common SDN interfaces. The openness of these interfaces will increase the possible set of attackers. The communication in SDN based 5G mobile networks can be categorized in to three communication channels i.e. data channel, control channel and inter-controller channel. In current SDN system, these channels are protected by using TLS (Transport Layer Security) / SSL (Secure Sockets Layer) sessions. However, TLS/SSL sessions are highly vulnerable to IP layer attacks, SDN Scanner attacks and lack strong authentication mechanisms.

Security Solutions for Communication Channels

5G needs proper communication channels security not only to prevent the identified security threats but also to maintain the additional advantages of SDN such as centralized policy management, programmability and global network state visibility. IPsec is the most commonly used security protocol to secure the communication channels in present day telecommunication networks such as 4G-LTE.

It is possible to use IPsec tunneling to secure 5G communication channels with slight modifications. Moreover, the security for LTE communications is provided by integrating various security algorithms, such as authentication, integrity and encryption. However, the main challenges in such existing security schemes are high resource consumption, high overhead and lack of coordination. Therefore, these solutions are not viable for critical infrastructure communication in 5G.

Thus a higher level of security for critical communication is achievable by utilizing new security mechanisms such as physical layer security adopting Radio-Frequency (RF) fingerprinting, using asymmetric security schemes and dynamically changing security parameters according to the situation.

Similarly, end-to-end user communication can be secured by using cryptographic protocols like HIP.

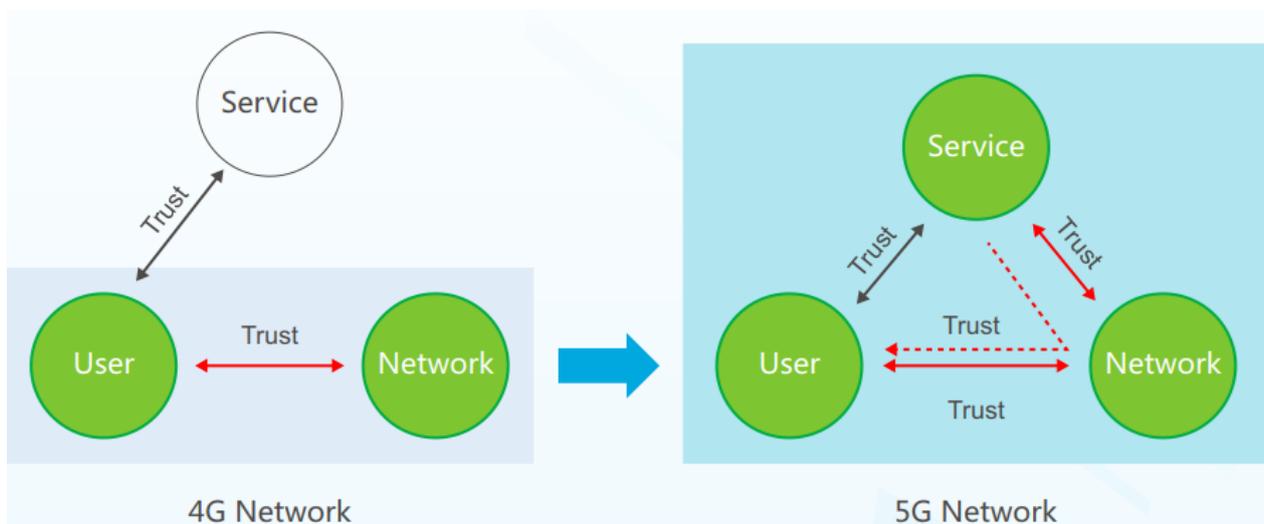
Here are a table with the security challenges in 5G technologies:

Security Threat	Target Point/Network Element	Effected Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS attack	Centralized control elements	✓	✓		✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			✓	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓		✓	
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds		✓		✓	
User identity theft	User information data bases				✓	✓
TCP level attacks	SDN controller-switch communication	✓		✓		
Man-in-the-middle attack	SDN controller-communication	✓		✓		✓
Reset and IP spoofing	Control channels			✓		
Scanning attacks	Open air interfaces			✓		✓
Security keys exposure	Unencrypted channels			✓		
Semantic information attacks	Subscriber location			✓		✓
Timing attacks	Subscriber location				✓	✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Subscriber identity			✓		✓

New Trust Model and Identity Management

In legacy mobile communications networks, Telecom networks are responsible for authenticating user for network access only. A trust model with two elements, between users and networks, is formed. The authentication between user and services are not covered by the networks.

However, in 5G networks, a trust model with an additional element, the vertical service provider, is favored possible design. Networks may cooperate with service providers to carry out an even secure and more efficient identity management.



Hybrid Authentication Management Challenges

5G networks are open platforms with a plenth of services. Smart transport, smart grid, industrial IoT are some of them. Both networks and service providers face

challenges in making access & service authentication simpler and less costly. Three authentication models would possibly co-exist in 5G to address needs of different businesses.

- Authentication by networks only

Service authentication incurs significant amount of costs to service providers. Service providers can pay networks for service authentication so users will be able to access multiple services once they complete a single authentication. This frees users from the cumbersome task of getting service grant repeatedly when accessing different services.

- Authentication by service providers only

On the other hand, networks may rely on the proven authentication capabilities from vertical industries and exempt devices from radio network access authentication, which can help the networks lower down operating cost.

- Authentication by both networks and service providers

For some of the services, a legacy model might be adopted. Networks take care of network access, and service providers deal with service access.

4. New 5G vulnerabilities discovered and made public in February 2019

A group of researchers from Purdue University and the University of Iowa presented their findings Tuesday at the Network and Distributed System Security Symposium in San Diego. They note that their discoveries, first reported by TechCrunch, are particularly concerning since the 5G standard was specifically developed to better protect against these types of attacks.

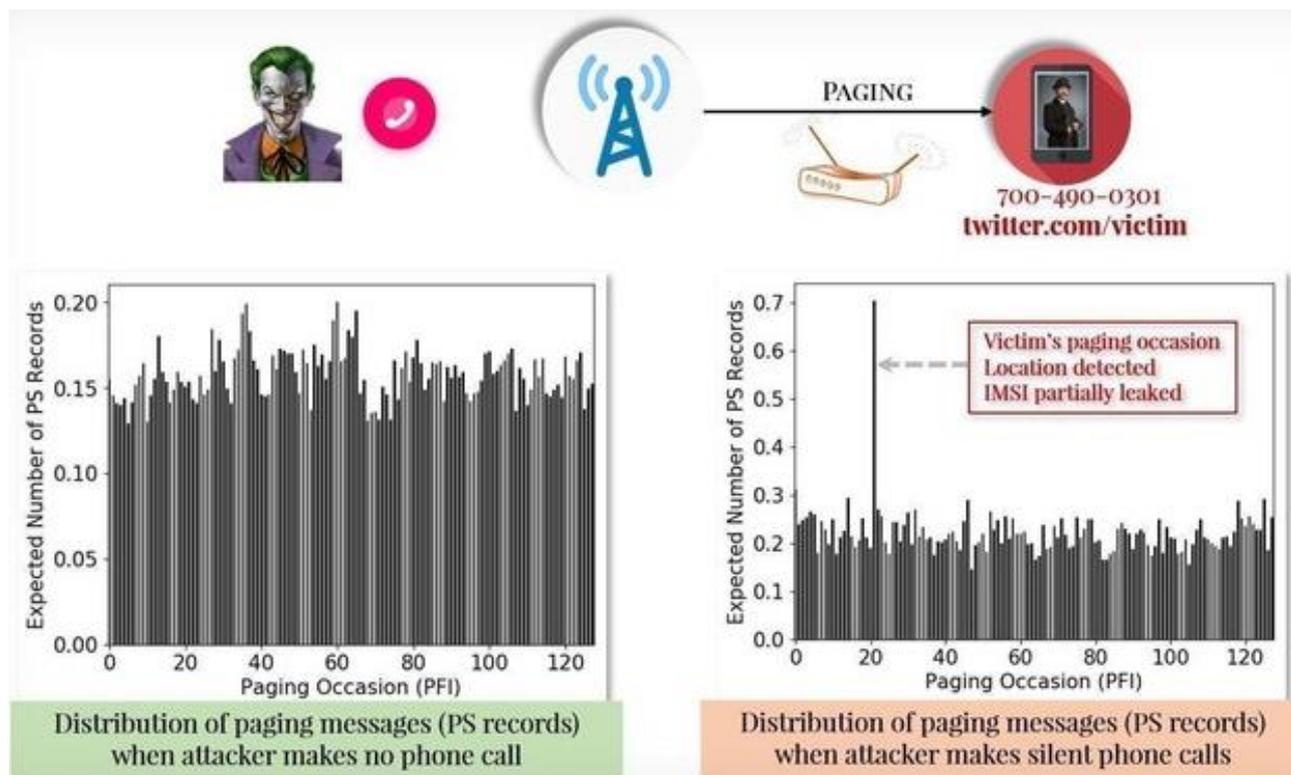
"We were really surprised that though 5G promises enhanced security and privacy, it cannot guarantee that level, because it inherits many security policies and subprotocols from the previous generations, which are more error-prone," says Purdue's Syed Rafiul Hussain, one of the paper's authors. "It opens the door for an adversary to exploit these weaknesses."

The researchers, who also uncovered other vulnerabilities in the 4G network last year, describe a series of new protocol weaknesses that could be used in a variety of

attacks. An exploit the researchers call Torpedo underlies the others; it preys on flaws in the "paging protocol" used to notify devices about incoming communications.

"Once a user's IMSI is exposed, an adversary can carry out more sophisticated attacks." [Syed Rafiul Hussain, Purdue University]

An idle device checks in with the nearest cellular base station for these pages at set increments, so it isn't killing battery life by checking constantly. But the researchers found that this predictability can be exploited. If an attacker wants to determine if a target is nearby, they can initiate a quick series of phone calls to a victim's device to "sniff," or evaluate, the paging protocol communications. Both 4G and 5G have built-in protections against this type of surveillance, but researchers found that these obfuscation efforts fall short. An attacker can spot patterns in the paging messages that reveal which base station the device is closest to, and confirm that the victim is in the area.



Torpedo attacks could also allow a hacker to manipulate a target's paging channel to add or block paging messages, resulting in victims missing messages and calls. A hacker could also use the technique to spoof certain kinds of messages, like a fabricated Amber Alert message.

But an attacker can use Torpedo as a stepping stone in an "IMSI-cracking attack" that could allow a hacker to ascertain a victim's "international mobile subscriber identity" number. The smartphone's subscriber identity number can be used to track a device more precisely, or monitor communications through rogue devices that impersonate cellphone towers—often called stingrays or "IMSI catchers." While stingrays have been a known privacy threat for years now, they are still prevalent around the US, deployed by law enforcement and attackers alike.

IMSI numbers are encrypted in 4G and 5G networks to protect them from such attacks, but the researchers again found that the protections are inadequate. They also found a carrier implementation issue, dubbed Piercer, that could expose IMSI numbers another way on the 4G network. They say that one US carrier, which they're not making public, is currently vulnerable to Piercer attacks.

"Once a user's IMSI is exposed, an adversary can carry out more sophisticated attacks including tracking the location and intercepting phone calls and SMS messages of the user," Purdue's Hussain says. "Average consumers are at the risk of exposing their privacy to malicious third parties who sell location data and other private information."

With the exception of the Piercer flaws, the vulnerabilities the researchers discovered would need to be fixed above the individual carrier level by the industry group GSMA, which oversees development of mobile data standards including 4G and 5G.

GSMA is aware of the research and is considering fixes for some of the issues, but disputes the practicality of the attacks. According to GSMA: "The findings suggest that a hacker could theoretically target a subscriber's IMSI or unique identifier on a 4G network by sending multiple messages in quick succession and then monitoring the network to identify increased traffic against a specific subscriber."

"However, this approach in reality would have to be performed in a specific time slot and be based on trial and error, which would be an exhaustive and time-consuming process in order to be successful.

The GSMA is working with 3GPP to consider attack detection options, if the threat level warrants and whether modifications could be made to the standards."

The statement also disputes that the 5G network would be vulnerable to the researchers' attacks. GSMA says the work is "based on an early version of the standard that has since changed. This security enhancement illustrates how security levels continue to evolve and improve through standardization."

The researchers say that the improvements still do not resolve the problem, though. "We checked the change requests and it seems that even the new change is vulnerable to Torpedo attack in 5G."

All of this isn't to say that the 5G standard should just be scrapped. It still has many benefits, including security benefits, that make the arrival of the network an important and productive thing. But security flaws in telephony standards need to be taken seriously and resolved, and there's a mixed record of that in the telecom industry. Fundamental protocol flaws, like those in the historic SS7 backbone standard, have remained unresolved for decades and led to increasing risk to end users.

The more pressure telecoms feel to resolve these flaws, the better.

References

- [1] Official ANCOM website: www.ancom.org.ro.
- [2] Virgilius Stanciulescu - Cybersecurity Forum: 5G beneficii și vulnerabilități.
- [3] Virgilius Stanciulescu - Cybersecurity Congress, Sibiu & Porentruy, 2018: 5G vulnerabilities and new attack strategies and countermeasures.
- [4] Virgilius Stanciulescu - Cybersecurity Congress, Firenze 2019: 5G vulnerabilities and new attack strategies and countermeasures.
- [5] 5G Security: Forward Thinking Huawei White Paper.
- [6] 5G Security: Analysis of Threats and Solutions.
- [7] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtovk, Centre for Wireless Communications, University of Oulu, Finland.

- [8] <https://www.go4it.ro/telefoane-mobile/au-fost-descoperite-noi-vulnerabilitati-in-retelele-4g-si-5g.-toate-dispozitivele-pot-fi-accesate-de-catre-hackeri-17890274/>.
- [9] World Economic Forum: <https://www.weforum.org/agenda/2019/01/heres-how-5g-will-revolutionize-the-digital-world>.
- [10] World Economic Forum: <https://www.weforum.org/agenda/2019/02/heres-what-5g-will-bring-in-2019/>.
- [11] New Line Technologies: <https://newline.tech/blog/what-will-the-era-of-5g-bring-us/>.
- [12] ENISA: <https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g>.
- [13] WIRED: <https://www.wired.com/story/torpedo-4g-5g-network-attack-stingray/>.
- [14] TECHCRUNCH: <https://techcrunch.com/2019/02/24/new-4g-5g-security-flaws/>.
- [15] Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information, Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li and Elisa Bertino, Purdue University, The University of Iowa.

Innovation and Research - Current State, Trends and Challenges

Ioan CONSTANTIN

Development and Innovation, Orange Romania
ioan.constantin@orange.com

1. Innovation and research

The specific objective of this paper is to present the current state in the field of Research and Innovation, the emerging trends, needs, challenges and best practices used to solve specific issues along with recommendations for improving the current state.

1.1. Overview of the current state in the field of innovation and research

According to the European Commission's scoreboard [1] Romania has EU's poorest track record in research and innovation along with the lowest R&D expenditure, the lowest number of patents per capita and the lowest rate of employment in research - oriented activities out of all member states.

Based on the analysis conducted by the European Commission of the EU innovation potential, an index was calculated [2] as a composite of 25 indicators used to measure innovation performance, dividing the Member States into four groups in terms of performance:

- *Innovation leaders* - includes countries with performance above the EU average;

- *Innovation followers* - includes countries with performance in the 90-th percentile of the EU average;

- *Moderate innovators* - including countries with performance in the 50% to 90% range of the EU's performance and

- *Modest innovators* - having a level of performance less than 50% of the EU average.

As the Commission ranks Romania as a ‘modest innovator’ challenges arise as to determine the needs and the best practices required to drive progress in this specific field. A summary innovation index presents an overview of the principal indicators and Romania’s performance relative the EU averages.

Table 1. Innovation Union Scoreboard 2018[1] uses the most recent available data from Eurostat and other international sources. All indicators are from 2011 and 2018

Romania	Relative to EU 2018 in 2018	Relative to EU 2011	
		In 2011	In 2018
Summary Innovation Index	31.4	44.8	34.1
Human resources	13.7	40.3	16.7
New doctorate graduates	28.1	107.7	40.8
Population with tertiary education	8.1	11.9	9.7
Lifelong learning	0.0	3.1	0.0
Attractive research systems	24.2	14.3	27.2
International scientific co-publications	18.8	15.7	27.3
Most cited publications	29.1	14.7	31.9
Foreign doctorate students	20.7	12.8	19.8
Innovation-friendly environment	76.9	75.4	121.6
Broadband penetration	116.7	111.1	233.3
Opportunity-driven entrepreneurship	35.2	51.0	45.5
Finance and support	26.9	31.7	29.4
R&D expenditure in the public sector	5.1	23.4	4.8
Venture capital expenditures	45.4	41.6	58.7
Firm investments	9.1	61.9	10.9
R&D expenditure in the business sector	19.9	13.3	22.8
Non-R&D innovation expenditures	3.1	163.3	3.6
Enterprises providing ICT training	5.3	0.0	6.7
Innovators	0.0	42.5	0.0
Innovative SMEs collaborating with others	4.8	10.7	5.1
Public-private co-publications	20.8	19.9	24.5
Private co-funding of public R&D expenditures	77.0	99.7	73.9
Intellectual assets	23.0	13.2	22.3
PCT patent applications	6.5	4.2	5.9
Trademark applications	31.2	27.1	34.8
Design applications	31.6	11.2	29.1
Employment impacts	46.3	18.7	48.4

Romania	Relative to EU 2018 in 2018	Relative to EU 2011	
		In 2011	In 2018
Employment in knowledge-intensive activities	23.5	3.8	25.6
Employment in fast-growing enterprises	64.1	29.4	64.8

The available data listed in the table above, which is used to determine the E.C. country ranking, scales across multiple research, development and innovation domains including Cyber Security.

It is our assessment that the current state in the field of innovation and research in Cyber Security is impacted by several important factors such as the migration of human resources, the downwards trend in the number of population with secondary and tertiary education and the lackluster R&D expenditure from the public sector.

In regards to the beneficial factors that impact this field, our assessment highlights the noticeable rise of opportunity driven entrepreneurships and the dynamic start-up environment which - although immature compared to other E.U. member states - provides a friendly environment for innovation, in some of the developed urban areas of Romania such as Bucuresti, Cluj-Napoca, Iasi or Timisoara.

1.2. Emerging trends in innovation and research

Innovation and Research in Romania is responding to the changing landscape of the global economic conditions that affect how various nations, corporations and agencies prioritize investment in research and innovation. In respect Horizon 2020, a multinational research program, launched by the E.U., we are noticing a shift toward funding innovation, research and development activities with a greater market potential.

A substantial approach to funding and supporting innovation that tackle societal challenges is noticeable in the Horizon 2020 program, with Consortiums of private organizations and public institutions developing platforms and frameworks in various areas for consolidating security. A focus of activities can be found in *improving cyber security for citizens and organizations, protecting and improving the resilience of critical infrastructures, supply chains and transport modes, fighting crime, illegal trafficking and terrorism.*

Development and innovation are key factors in driving growth and addressing challenges and nations and organizations are developing new policies, ecosystems and strategies promoting these factors. A National Strategy for Research, Development and Innovation exists in Romania [3] as it establishes a set of general objectives for economic, societal and technological growth by the means of supporting innovations in both public and private sectors.

Whilst lagging behind the European Average in terms of maturity, Romania's Start-ups ecosystem is dynamic, with several corporate accelerators managing a growing number of start-ups, in various tracks. The Cyber Security tracks of some of local accelerators are keeping pace with global trends in research, with innovators focusing on developing future-proof solutions for current and future challenges such as the advent of A.I.-driven technologies, the 5G paradigm shift towards IoT deployments, Machine to Machine and low-latency communications, block-chain based authentication, validation and access control. This pace is well maintained in emerging fields that supplement 'traditional' cyber-security technologies with noticeable efforts in the cloud-native security solutions and Managed Security Services.

1.3. Challenges, needs and best practices for solving issues

A distinct challenge in today's Development and Innovation programs, across its domains including Cyber Security is the complexity of the on-boarding phase of most research programs. Programs such as Horizon 2020 will benefit from a simplification of the rules, grant instruments and funding models with simpler application procedures being a key factor in increasing reach.

Another challenge for Innovation and Research in Cyber Security and related areas is the rapid developments in the underlying technological layers of most business oriented and consumer technologies -such as 5G, Internet of Things, Cloud Services, Artificial Intelligence-, as this dynamic environment brings forward new needs for technologies, tools and methods for Cyber Security protection. As privacy and security of data become important pillars for most business, innovative cyber security products and services must answer today's threats such as Advanced and Persistent Threats

(APTs) and targeted attacks, fake news and deep fake image and audio/video manipulations, Operational Technology and Industrial malware or A.I.-coordinated Botnets.

One important challenge to achieving cyber security is critical infrastructure exposure to IT networks vulnerabilities, with OT and IT becoming increasingly interdependent. Romania's critical infrastructure, including electric power grids, communications networks, traffic control systems and financial systems can be susceptible to cyberattacks and as these concerns begin to be addressed by stakeholders, research and innovation in the field of cyber security gains recognition of its importance.

In this regard, responding to these challenges requires a sustained support for research and from innovation that will address today's needs and those on the horizon by collaborative and inter-disciplinary work.

One approach to developing best practices for research and innovation activities is innovation management - the systematic learning process aspiring to identify, create, refine and implement value creating ideas as to address the perceived challenges in cyber security and to exploit the opportunities that have risen.

This approach can be implemented as a practice in the development and innovation ecosystem as a whole, at a national level, through a strategy or guide published by the state-level stakeholders and disseminated by public and private organizations, academia, research and development centers and groups and corporate accelerators alike. Having a systematic approach to innovation can drive better results and focus on specific challenges such as those in the cyber security domain.

A distinct approach to innovation in cyber security, addressing the needs for faster response to new threats in the cyber space is the crowdsourcing of ideas by involving a large number of people, from different academic and business backgrounds, in project such as *themed hackathons* in which the participants work in teams to tackle a specific challenge, following a set of specifications, within a pre-determined timeline. It is this author's opinion that events such as *hackathons*, *capture the flag competitions*

or *builder / maker fairs* are key components for a systematic development of a framework for innovation, applicable to Romania's societal needs in cyber security.

2. Recommendations and Conclusions

As the dynamic threat landscape challenges current cyber security technologies, an engaging and supportive innovation and research environment can lead the development of new tools and methods needed to achieve cyber security. Although Romania's innovation environment is lagging behind the E.U.s averages terms of human resources, financial support and academia involvement, the systematic, strategic development of an open innovation framework could be beneficial to all parties involved, private, public and academia.

A coordination and collaboration between research centers and start-up corporate accelerators, on one side and public and private organizations on the other side, could bridge the gap between the perceived societal needs in cyber security and the identification of innovative approaches that tackle those needs.

References

- [1] European innovation scoreboard 2018 - Main report, <https://ec.europa.eu/docsroom/documents/35918>. [Accessed: July 10, 2019].
- [2] European innovation scoreboard 2018 - Methodology report, <https://ec.europa.eu/docsroom/documents/35644>. [Accessed: July 9, 2019].
- [3] Ministerul Cercetării și Inovării “Strategia Națională de Cercetare, Dezvoltare și Inovare 2014-2020” [Online]. Available: https://www.edu.ro/sites/default/files/_fi%C8%99iere/Minister/2016/strategii/strategia-cdi-2020_-proiect-hg.pdf. [Accessed: July 12, 2019].

Strategic Directions for Cybersecurity. A Bitdefender Perspective

Alexandru-Cătălin COSOI
Bitdefender, Romania
acosoi@bitdefender.com

1. Introduction

Two years have passed since the WannaCry ransomware attack, a large-scale, global security incident that spread through the EternalBlue exploit targeting computers operating on outdated Windows systems. It affected over 300,000 computers that were still using vulnerable software such as Windows Vista and Windows 7. Similarly, powerful was 2017's NotPetya, encrypting ransomware that also went after Windows computers and propagated via the same EternalBlue, affecting companies in Ukraine, France, Germany, Poland, the UK and US. After months of investigations, both cases unfolded to be very interesting, however, the general public remembers them just as an incident that slowed down their productivity.

Studies show that the business sector is maturing in terms of cyber-resilience, but organizations with weak cybersecurity sometimes prefer to pay up when hit by ransomware, especially since most of the time, it's not their money that they are giving away; their insurance companies are the ones paying. High-profile examples include the healthcare industry, professional services, and the financial sector.

Also, playing into the hackers' game also creates a vicious circle. Firstly, paying the ransom encourages adversaries to strike again. Second, an organization like a healthcare facility may have to close its doors until it recovers critical scheduling and patient EMR servers, leading to disruption and lost business - not to mention risk to lives. And, as others have shown, the cost of downtime can devastate businesses.

In this article we will briefly touch the state of security today, enumerate some predictions, draw some conclusions and then issue some recommendations.

2. State of security

The total amount of malware has significantly increased year over year, both on Windows-based systems as well as on Android and MacOS.

But what motivates malware developers to constantly develop new malware? Since no one does anything - especially invest time and effort in developing malware - without getting some sort of return on investment on their work, the main motivation for cybercriminals for developing malware is MONEY. Most of today's malware is financially motivated. Whether it's data stealing malware (e.g. Trojans or APTs), money making malware (e.g. ransomware or cryptocurrency miners), or even malware designed to aid in infiltrating organizations and exfiltrate funds, the main motivation behind this rampant malware growth over the past decade is financial.

If we are to look at how malware has evolved over the past decade, we can clearly see how it has evolved strictly from a financial perspective. Ten years ago, we used to have Trojans, mostly designed at getting e-banking credentials and transferring funds from their victims' bank accounts. While this type of threat was mostly aimed at the average user, shortly after, a new piece of malware emerged that was designed at simply extorting victims: ransomware. Ransomware also marks the evolution from cyber-criminals targeting the average user to cybercriminals targeting organizations. While at first the average user was mostly extorted for up to \$600, going after organizations was far more profitable for cybercriminals as they could ask for ransom notes as high as \$700,000, depending on how valuable the encrypted data was for ensuring business continuity for the victim. Ransomware has even evolved to the point where ransomware developers have created an affiliation-based business models, enabling their "clients" to handle the distribution and infection part while the ransomware developers got a cut of the profit and focused only on improving the malware and their customer services.

Another financial motivated group is the Carbanak group, famous for going after banking organizations, successfully infiltrating their infrastructures and exfiltrating funds either by compromising banking applications or ATM networks.

Other cybercriminal gangs, such as APT10, have been focusing on MSP, as these service providers often represent a far more valuable target because they have direct access into various client infrastructures. This means that by successfully compromising an MPS, attackers can instantly have access into dozens of organizations that are managed by that MSP.

Cryptojacking, or the process of illicitly using someone's computing power to mine cryptocurrency, has become popular ever since the browser-based cryptocurrency mining script (CoinHive) picked up traction, in late 2017 and early 2018. While cryptojacking was mostly targeted at consumers at first, by going after popular websites and using the computing power of unsuspecting victims to mine cryptocurrency on behalf of the attacker, they have later started going after business infrastructures as they had more computing power. As a result, cybercriminals have used infrastructures ranging from a water utility in Europe all the way to several Amazon cloud instances belonging to Tesla. While this is considered a somewhat benign threat, in the sense that it's not as disruptive as the other types of financially motivated threats, the presence of a cryptojacker within an infrastructure is still considered a data breach.

Microsoft Office "Macros", PowerShell, and WMI scripts embedded inside documents, will increase in number and scope. Fileless malware and macros have become a low hanging fruit for threat actors in terms of using it to deliver ransomware, cryptocurrency miners, and even advanced persistent threats. In some instances, this type of threat allows attackers to first assess the victim's system and validate whether or not it could be a potential target, before actually delivering the final malicious payload.

Which brings us to GandCrab, a type of ransomware that encrypts important files and asks for a ransom to decrypt them. In January 2017, it started spiking on the global threat map, spreading through e-mail attachments and exploit kits. The new contender in the ransomware underworld managed to take more than 50,000 computers and servers hostage, demanding varying sums of money for the decryption key. What made it interesting and special at the same time is that its developers have adopted an as-a-

service business model in terms of distribution. Basically, using this model the cybercriminals behind GandCrab concentrate on development and then take a cut of the paid ransom notes (usually between 600 and 2000 USD), letting others with lesser technical skills run the campaigns.

Since its January arrival, new versions of the ransomware have been released and in late September, the Australian Cyber Security Centre stated the need for Australian businesses to remain vigilant of ransomware and the damage it can cause, both in terms of reputation and financial impact.

As for WHERE are these ransomware-as-service offerings hosted, the answer is the dark web and other illicit marketplaces. Because GandCrab ransomware campaigns can be managed using a simple - and intuitive web console - these services are usually hosted on *.onion* websites that can easily be taken offline or moved to another location. What's interesting about GandCrab is that potential clients can even estimate earnings before signing up for the service. Also, *.onion* websites, also names hidden services, can easily be anonymously hosted on a laptop behind a NAT in a coffee shop.

Also, GandCrab won't infect a Russian-based system. In fact, it actually scans for regional settings and keyboard layouts to determine if the victim is Russian-based and won't engage the encryption mechanism.

In terms of how victims get infected, the most spectacular development in the way affiliates target victims is the targeting of SMBs through stolen or brute force remote desktop credentials. Of course, other attack vectors for GandCrab distribution involve DOC files with macro inside or laced PDF files, Zipped JS downloaders attached to malspam, cracks and exploit kits.

Now, no law enforcement agency nor security companies actually encourage victims to pay the ransom, but some victims sometimes have no choice but to give in. Either because they lack backups or because the downtime and financial costs associated with manually restoring the affected infrastructure might be higher than the ransom note. However, the amount of time at your disposal in which you can pay the ransom is usually limited. For example, if in this case the victim fails to give in within a week, the ransom note will double from the \$10,000 to \$20,000 in 7 days.

3. 5G deserves its own chapter

Organizations and consumers alike are eagerly anticipating the arrival of 5G, the latest generation of cellular mobile communications. But perhaps IT and security executives need to be thinking about the potential security implications.

This technology is designed to provide benefits such as increased performance made possible by much higher data rates than offered by previous cellular networks.

Other possible benefits of 5G include reduced latency, energy savings, cost reduction, higher system capacity, and massive device connectivity—an important consideration for the growing Internet of Things.

In addition to IoT, the high data rates and low latency of 5G are expected to support newer applications such as virtual reality (VR) and augmented (AR), as well as accommodate the huge amount of data consumption needed for autonomous vehicles to operate safely.

The first phase of 5G specifications was scheduled for completion by April 2019 to accommodate early commercial deployment. The second phase is due to be completed by April 2020.

One 2018 study [1], by a team from ETH Zurich, the University of Lorraine/INRIA, and the University of Dundee, described some of the concerns with the next generation of mobile communication.

The researchers subjected the 5G mobile communication standard to a comprehensive security analysis. And while they concluded that data protection is improved in comparison with the previous standards 3G and 4G, security gaps are still present.

With the aid of a security protocol verification tool designed for analyzing cryptographic protocols, the researchers systematically examined the 5G Authentication and Key Agreement (AKA) security protocol, taking the specified security aims into account.

The tool automatically identifies the minimum-security assumptions needed in order to achieve the security objectives set by the 3rd Generation Partnership Project (3GPP), a collaboration between groups of telecommunications standards associations.

The analysis showed that the standard is not sufficient to achieve all the critical security aims of the 5G AKA protocol.

The researchers also determined that the protocol permits certain types of traceability attacks, in which a mobile phone does not send the user's full identity to the tracking device but still indicates the phone's presence in the immediate vicinity.

4. Tendencies and challenges

- Ransomware - The most profitable form of malware, ransomware remains a constant threat. We still record copious numbers of infections daily, but the good news is ransomware is no longer growing - it's plateauing. One reason is already well documented: ransomware has taken a back seat to cryptojacking in the past year as bad actors developed a taste for stealing computing power to generate digital currency while flying under the radar. But an even heftier factor behind ransomware's stagnation is the emergence of dedicated solutions aimed directly at thwarting this form of malware. There will always be new versions of ransomware, some more complex than others and some harder to detect, but we don't expect ransomware to take on much bigger proportions. At least not bigger than in the past year.
- Internet of Things (IoT) - We expect more attacks leveraging Internet of Things (IoT) / smart / connected devices. As lawmakers scramble to come up with a way to regulate the IoT space, attackers will continue to capitalize on their inherent weaknesses. Hackers are becoming better at hijacking IoT products like baby monitors, surveillance cams and other home appliances. And connected medical devices are far from safe either. In fact, body implants that support wireless connectivity may lead to the first ransomware attacks where you need to pay or die. In 2013, former US Vice President Dick Cheney asked his doctors to disable the wireless function in his pacemaker to thwart the potential of terrorists hacking it.
- In another noteworthy trend in the IoT landscape, manufacturers are jumping on the cellular bandwagon, gradually moving their IoTs from WiFi to LTE

and from ipv4 to ipv6. While this shift promises increased security, it will likely open up a new can of worms since it's relatively new ground for the IoT ecosystem.

- macOS attacks on the rise - Apple's share of the desktop market is rising, and malware designed to infect Macs is growing along with it. We project an increase in the number of attacks targeting Mac users, something we are already beginning to see in our internal telemetry. Our data shows not just new macOS-specific malware, but also macOS-specific mechanisms and tools designed to capitalize on Macs post-breach. We've already seen this in past APTs that housed Mac-specific components.
- MACROs and fileless attacks - Attacks leveraging Microsoft Office MACROs will also increase in number and scope. MACROs are a feature, not a bug, as the old adage goes. Which makes it the perfect bait for victims prone to social engineering scams - where the attacker convinces the victim to essentially partake in their own abuse. We expect fileless attacks - such as those leveraging powershell and other system-bound tools like gen reg, mshta, etc. - to also increase in scope in the year to come.
- Potentially unwanted applications (PUA) and cryptojacking - Potentially unwanted applications (PUA), including adware, don't pose a tremendous threat of themselves, but they're not innocent either. For example, you could download a seemingly legitimate application not knowing it's bundled with crypto miners or even malware.
- We forecast an increase in JavaScript-based miners embedded in webpages - like the YouTube cryptojacking incident where attackers conducted a malvertising campaign and injected miners within ads displayed on YouTube.
- Finally, we can expect a shift from drive-by-downloads of malware to full blown drive-by-mining. In other words, the use of web-mining APIs that perform crypto-mining, directly in the user's browser, instead of exploit-kits to download malware onto the victim's computer.

- Combating invisible threats - Network-level exploits will enter the limelight next year, and they will likely be hyped by social media, if history is any indication. And researchers will have to devote considerable resources to analyzing hardware-based implants, hardware backdoors, and hardware design flaws, as well as supply chain compromises in software.
- APTs targeting banks - We expect advanced persistent threats to continue emerging, with a renewed focus on the banking sector, reminiscent of the Carbanak group making headlines in 2014 for using an APT-style campaign to steal money from banks. The malware was reportedly introduced via phishing emails, with the hackers said to have stolen hundreds of million dollars not only from banks, but from more than a thousand private customers as well.
- GDPR to show its fangs - Here's a positive prediction for a change: Thanks to the EU's renewed effort to protect personally identifiable information - in the form of the General Data Protection Regulation that took effect in May this year - we should expect fewer "credential leaks" to occur, or at the very least make headlines. Security incidents will be more thoroughly contained at an organization level in an effort to avoid penalties that could force a business into bankruptcy. Remember that the GDPR can dish out fines of up to 4% of the victim's annual turnover, which can translate into hundreds of millions and even billions of dollars in the case of large enterprises and corporations.
- A shift towards mobile attacks - Fintech services are paving the way to a very profitable new trend for hackers. The more money and integration with traditional banking systems, the more attention they will get from cybercrooks who will likely develop new threats targeting these specific services in the next years.

References

- [1] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirović, Ralf Sasse, Vincent Stettler, A Formal Analysis of 5G Authentication.



INTERNATIONAL COOPERATION



INTERNATIONAL COOPERATION

An Overview of the General Trends in Cybersecurity

Angela IONIȚĂ

Institute for Artificial Intelligence, Romanian Academy
aionita@racai.ro

1. Introduction: The general framework in Europe and Worldwide

“One observation consistently made about the digital era is that when people and technology mix, the results are surprisingly hard to anticipate. This kind of uncertainty puts cybersecurity professionals at a structural disadvantage because it favors attackers over defenders and protectors. Looking to the future, at the intersection of people and digital technology, there is a gulf between the operational security on the agenda today and the range of cybersecurity issues and challenges that will emerge in a decision-relevant future time frame.” [26]

The number of people using the internet under different hypostases: from every citizen at different ages to specialist in different domain, employed by different companies, supposed to be subjected to cyber attacks in one or another form has surged over the past year, with more than one million people coming online for the first time each day since January 2018 reveals new collection of Digital 2019 reports¹ from Hootsuite² and We Are Social³ (Figure 1).

The reported aspects suggest that an average of almost 1 million people came online for the first time each day over the past year, continuing the strong growth that we saw in recent Digital 2019 reports¹.

Every year, cyber-attacks on both business and individuals seem to break new ground. And in 2019, with threat vectors growing and cybercriminals leveraging new hacking tools and techniques, Information Technology (IT) security departments will

¹ <https://datareportal.com/library>

² <https://hootsuite.com/>

³ <https://wearesocial.com/blog/2019/04/the-state-of-digital-in-april-2019-all-the-numbers-you-need-to-know>

have their work cut out for them. The good news is that the field of cyber security is rising to the challenge and will put up a noble fight in the coming year.



Fig. 1. Digital around the world in July 2019

(Source: Simon Kemp, 2019)

It should come as no surprise that data breaches have become more commonplace as cyber crime becomes big business. A recent survey of 1,200 companies reported that 71% [13] suffered at least one data breach at some time, with 46 percent reporting a breach in the last year (up from 26% the year before). Many of these attacks exploit employees' and people's lack of awareness of phishing and other social engineering tactics that are designed to steal corporate login credentials, giving cyber criminals backdoor access to network infrastructure.

2. The Facts and the initiatives in European Union

“The European Commission has proposed to significantly boost investment in cybersecurity and advanced digital technologies in the EU in the next EU budget period, notably through its proposal for a Digital Europe Programme⁴. It has

⁴ https://europa.eu/rapid/press-release_IP-18-4043_en.htm

also proposed a new European Cybersecurity Competence Centre and network⁵ to pool resources and coordinate on priorities with Member States and to implement relevant projects in the area of cybersecurity. The proposal also aims at creating a Network of National Coordination Centres and a Cybersecurity Competence Community in order to ensure better cooperation and synergies among the existing experts and specialist structures in the Member States. This goes hand-in-hand with the key objective to increase the competitiveness of the EU's cybersecurity industry and to turn cybersecurity into a competitive advantage for other European industries.” [30]

The existence of problems created by the definitions in special in cyber security and, above all, their harmonization, brings shortcomings in the different aspects of sectoral management, especially in the production of normative, countermeasures and law enforcement. This implies a great complexity with a multiplier effect on the domain and its implication for geographic and functional reasons [25]. Geographic, because infrastructures or critical infrastructure systems are mostly transnational and require the involvement of more states. Functionality, because modern network interconnections involve interdependence where vulnerabilities are transmitted from one system to another and are often amplified. These domino, geographic and functionality effects of system vulnerabilities have a very high potential impact and may involve both public and private sector targets that are fundamental to infrastructure owners and / or security managers.

Because in cyber space one operates on many different levels and one of the functions of the strategy should be to address coherently all the different levels of cyber space needs, ENISA decided to publish his overview of cybersecurity and related terminology, Version 1 in September 2017 in order to offer a common language of understanding the complexity of the cybersecurity domain.

A reading of the relevant strategic documents adopted by the European Union (EU) and the United States of America (US) in recent years provides interesting

⁵ https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1598442_en

indications that cyber related terms are being used in a fairly heterogeneous and ambiguous manner at international level without a common definition of threats cybernetics [4].

At one point, it was found [2] that a time has passed since the ambiguity of the definitions of official EU-US documents characterizing the perception of cyber security has contributed to the fact that threat assessment analyzes have been concentrated almost exclusively on high-performance events, but low probability, thus significantly diverting resources from ordinary administration, but also from urgent problems.

In its effort to adapt to digital and data-driven environments while minimizing the negative consequences of cyberattacks, the EU has taken some steps in terms of increasing the cost of cybercrime operations as follows: Directive on Attacks Against Information Systems from 2013 that introduced minimum standards on the definition of criminal cyber offences and related sanctions; in 2018 the EU proposed legislation to facilitate and accelerate the adoption of regulations on accessing electronic evidence by introducing European Production Order and European Preservation Order [18]; all in 2018 the EU introduced the General Data Protection Regulation (GDPR) that is in force since May 2018. Companies must comply with this law or be subject to fines of up to 20 million euros, and in 2019 it is estimated that as much as 80% [3] of multinational companies could fail to comply with GDPR. Fortunately, this law creates a learning opportunity for IT security organizations everywhere, as it forces them to reexamine how customer data is collected, processed, stored and deleted. And GDPR will impact more than just cyber security teams; it will also present an opportunity for marketing groups to rethink how they conduct email campaigns to ensure total privacy of their customers' personal data, and an opportunity to craft a corporate brand that reflects their commitment to customer and data protection.

Several sensitive aspects have been highlighted in [9]: *"as a consequence of growing digitalisation, the risks to European societies have increased. The last five years have clearly demonstrated the extent to which cybercrime (e.g. ransomware, online fraud), attacks on critical infrastructure (e.g. energy plants in Germany,*

transportation networks in Sweden), or online disinformation - also known as information manipulation - can all have a dramatic impact on the proper functioning of societies." Consequently, the EU's approach has evolved to include a mix of instruments focused on security of critical infrastructure, integrity and freedom of democratic institutions and processes, as well as protection of personal assets and information [19]. A document complementing the 2013 EU Cybersecurity Strategy - embraced these strategic challenges under three broad objectives: building EU resilience to cyberattacks based on a 'collective, wide-ranging approach', creating effective cyber deterrence by putting in place credible measures to dissuade criminals and hostile states, and strengthening international cooperation to promote global cyber stability [20].

In his effort to ensure a minimum level of preparedness across the EU, the Network Information Security (NIS) Directive requires each member state to adopt a national strategy on the security of network and information systems, including measures to ensure high levels of security in critical sectors such as banking, energy, transportation, healthcare or digital infrastructure, as well as a governance framework, a list of actors tasked with the implementation of the strategy and a risk assessment plan.

Furthermore, member states designated a Computer Security Incident Response Team (CSIRT) and provide adequate resources for cross-border cooperation. In an effort to stimulate strategic and operational cooperation among EU stakeholders, the NIS Directive also established a NIS Cooperation Group and CSIRT network. In addition, given the potential wide-ranging impact of cyber incidents and crises, in 2017 the European Commission (EC) proposed a set of measures that form a cooperation framework for the Union in the event of large-scale incidents and crises. The so-called Blueprint for providing 'an effective process for an operational response at Union and member state level to a large-scale cyber incident', endorsed by the Council in June 2018, describes the objectives and modes of cooperation between the member states and the EU institutions, bodies and agencies in specific cases and scenarios that will be tested during the crisis-management exercises [20].

The EU has tailored a cyber capacity building model [1] that integrates its internal experience with lessons learnt from traditional development cooperation. The EU approach is based on the EU Member States' internal experience to enhance their cyber capabilities and best practice identified with the support of the European Cybercrime Centre (EC3) at Europol and the European Union Agency for Network and Information Security (ENISA).

The specific actions taken by the EU aimed at [1]: building cyber resistance bases; supporting the development of national cyber security strategies and policies; creating or strengthening the National Emergency Response Teams (CERTs) [7]; the implementation of national systems for an efficient cybernetics crisis. For example, Global Action on Cybercrime Extended (GLACY+) - one of the EU projects implemented jointly with the Council of Europe - provides assistance in policy development, strategies and enforcement of law enforcement and criminal justice frameworks in third countries.

In addition, the EU has launched and supports a number of projects specifically focused on enhancing the resilience of critical information infrastructures and networks that support the vital services of selected priority countries in the world. These include the ENCYSEC (Enhance Computer Security and Communications Network) project⁶ and the CB4CyberResilience (Capacity Building and Cooperation to Increase Internet Resilience) project.

3. NATO Policy on Cyber Defence. Activities and initiatives

“We [NATO] must be able to operate as effectively in cyberspace as we do in the air, on land, and at sea to strengthen and support the Alliance’s overall deterrence and defence posture.”⁷

NATO's assistant secretary general for emerging security challenges, Sorin Ducaru, said at the Cybersec conference in Krakow, that the military alliance should

⁶ <http://www.encysec.eu/web/>

⁷ <https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm>

innovate faster in the field of cybersecurity: "*We have a priority in having such capabilities for [the] defensive purpose of the alliance*". Since 2016, North Atlantic Treaty Organization (NATO) has recognised cyber space as one of its '*domain of operations*', like air, sea, and land [21]. In recent events, cyber attacks have been part of hybrid warfare. NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security. NATO consider necessary⁸ to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.

To keep pace with the rapidly changing threat landscape and maintain robust cyber defences, NATO adopted an enhanced policy and action plan, which were endorsed by Allies at the Wales Summit in September 2014⁹. An updated action plan has since been endorsed by Allies in February 2017. The policy establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO's cooperation with industry. The top priority is the protection of the communications systems owned and operated by the Alliance.

The policy also reflects Allied decisions on issues such as streamlined cyber defence governance, procedures for assistance to Allied countries, and the integration of cyber defence into operational planning (including civil emergency planning). In addition, the policy defines ways to take forward awareness, education, training and exercise activities, and encourages further progress in various cooperation initiatives, including those with partner countries and international organizations. It also foresees boosting NATO's cooperation with industry, including on information-sharing and the exchange of best practices. Allies have also committed to enhancing information-sharing and mutual assistance in preventing, mitigating and recovering from cyberattacks. NATO's cyber defence policy is complemented by an action plan with

⁸ https://www.nato.int/cps/en/natohq/topics_78170.htm

⁹ <https://www.gov.uk/government/topical-events/nato-summit-wales-cymru-2014/about>

concrete objectives and implementation timelines on a range of topics from capability development, education, training and exercises, and partnerships.

3.1. The NATO activities and initiatives

Allies pledged at the Warsaw Summit in 2016¹⁰ to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO's cyber defence capabilities, as part of NATO's long-term adaptation, this will reinforce the cyber defence and overall resilience of the Alliance.

At Warsaw, Allies also reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. As most crises and conflicts today have a cyber dimension, treating cyberspace as a domain will enable NATO to better protect and conduct its missions and operations.

The NATO Computer Incident Response Capability (NCIRC) based at SHAPE, Mons, Belgium, protects NATO's own networks by providing centralised and round-the-clock cyber defence support to the various NATO sites. This capability is expected to evolve on a continual basis, to maintain pace with the rapidly changing threat and technology environment.

To facilitate an Alliance-wide and common approach to cyber defence capability development, NATO also defines targets for Allied countries' implementation of national cyber defence capabilities via the NATO Defence Planning Process. In June 2017, further cyber defence capability targets were agreed by defence ministers.

Cyber defence has also been integrated into NATO's Smart Defence initiatives. Smart Defence enables countries to work together to develop and maintain capabilities they could not afford to develop or procure alone, and to free resources for developing other capabilities. The Smart Defence projects in cyber defence, so far, include the Malware Information Sharing Platform, the Smart Defence Multinational Cyber

¹⁰ https://www.nato.int/cps/en/natohq/events_132023.htm

Defence Capability Development project, and the Multinational Cyber Defence Education and Training project.

NATO is also helping member countries by sharing information and best practices, and by conducting cyber defence exercises to help develop national expertise. Similarly, individual Allied countries may, on a voluntary basis and facilitated by NATO, assist other Allies to develop their national cyber defence capabilities.

NATO conducts regular exercises, such as the annual Cyber Coalition Exercise, and aims to integrate cyber defence elements and considerations into the entire range of Alliance exercises, including the annual Crisis Management Exercise. NATO is also enhancing its capabilities for cyber education, training and exercises, including the NATO Cyber Range, which is based at a facility provided by Estonia.

To enhance situational awareness, an updated Memorandum of Understanding on Cyber Defence was developed in 2015. This updated MOU is now being concluded between NATO and the national cyber defence authorities of each of the 29 Allies. It sets out arrangements for the exchange of a variety of cyber defence-related information and assistance to improve cyber incident prevention, resilience and response capabilities.

The NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia is a NATO-accredited research and training facility dealing with cyber defence education, consultation, lessons learned, research and development. Although it is not part of the NATO this centre offers recognised expertise and experience.

The NATO Communications and Information Systems School (NCISS) in Latina, Italy provides training to personnel from Allied (as well as non-NATO) nations relating to the operation and maintenance of NATO communication and information systems. NCISS will soon relocate to Portugal, where it will provide greater emphasis on cyber defence training and education.

The NATO School in Oberammergau, Germany conducts cyber defence-related education and training to support Alliance operations, strategy, policy, doctrine and procedures. The NATO Defense College in Rome, Italy fosters strategic thinking on political-military matters, including on cyber defence issues.

4. EU - NATO Common Threats and Common Solutions

“... the concept of “one for all and all for one” as it relates to cyber space is a “fundamentally uncontroversial” idea at NATO”, Antonio Missiroli, assistant secretary general for emerging security challenges at NATO¹¹

Cybersecurity and defense have long been part of EU and NATO calculus but have only recently moved to the top of their agendas. The game first changed for Europe in 2007, when cyber-attacks in Estonia forced both institutions to think more seriously about this type of threat. As a result, NATO developed in 2008 its very first Cyber Defense Policy. Five years later, the EU followed suit by adopting its first Cybersecurity Strategy [22].

The 2014 crisis in Ukraine was Europe’s next big shock. Russia’s annexation of Crimea and semi clandestine military actions returned new urgency to European defense and deterrence, but also to cyber defense and readiness as Russia’s hybrid aggressions against Ukraine included cyber-attacks¹². Since then, NATO and the EU have intensified their initiatives in the cyber sphere. NATO endorsed an enhanced cyber defense policy and action plan in 2011, and it decided to operationalize cyberspace as a domain of defense policy and planning in 2016. That same year all Allies also made a Cyber Defense Pledge to enhance their cyber resilience as a matter of priority [23]. The EU for its part made the fight against cybercrime one of the three pillars of the European Agenda on Security, and recognized cybersecurity as one of the priorities for the Global Strategy for the European Union’s Foreign and Security Policy. In 2017 the EU adopted a “Cybersecurity Package” including the revised Cybersecurity Strategy [24]. In this climate of urgency, the EU and NATO have started to see each other as complementary partners to build up their cyber resilience. In order to foster operational level information sharing, NATO and the EU signed a Technical Arrangement on Cyber Defense in February 2016 between NATO’s Computer Incident Response Capability and the EU’s Computer Emergency Response Team. The most

¹¹<https://www.computerweekly.com/news/252458161/Nato-supports-collaboration-on-cyber-security>

¹² attackers disabled numerous news and other websites using denial-of-service attacks (DDoS)

significant step was made with the signing of the EU-NATO Joint Declaration of July 2016 that creates a concrete framework for cooperation in security and defense. With regard to cyber, the implementation plan of the EU-NATO Joint Declaration recognizes four areas of cooperation: integration of cyber defense into missions and operations; training and education; exercises; and standards. EU-NATO cooperation in times of crisis is increasingly becoming a must. And in the field of cybersecurity and defense the past years have indeed been pivotal.

The accelerating change of the digital age is placing new pressures on top of long-existing coordination difficulties of the EU and NATO. Both institutions will continue to face new cyber challenges, and they still find themselves maladapted to the new security environment. The EU and NATO must assert their credibility in cyberspace as strong powers in the eyes of their members and partners - and antagonists [10]. To achieve this result, NATO and the EU will need to continue to improve their joint force-multiplying functions, their cyber capabilities, to design common command and decision-making structures in cyber exercises, crisis and conflicts, and enhance their interoperability with partners in cyberspace. The security challenges of today require quick responses, necessitating flexible policy frameworks in which coercive reactions can be decided upon among networked actors. EU-NATO cybersecurity and defense cooperation must continue to adapt in a world that is constantly, and rapidly, evolving.

5. New trends of research and innovation (R&I) in cyber security

“As long as we treat cybersecurity as a technical problem that should have easy technical solutions, we will continue to fail. If we instead develop solutions that address the reasons why cybersecurity is a hard problem, then we will make progress” [28].

Taking into account that although the cyber security and privacy landscapes in the EU and the US are undoubtedly different - which is only natural given the different legal, political, cultural and business factors in each region - there are various areas where their priorities are the similar and to get a coherent picture of what cyber security

research and innovation means in the EU and the US and to ensure collaboration and harmonization of priorities, EC founded AEGIS project¹³ that took into account the following aspects:

Cybersecurity topics such as Security Management and Governance; Data Security and Privacy; Education and Training; Assurance, Audit and Certification; and Network and Distribution Systems get the most attention from funding program managers as well as from the research community.

The *Internet of Things* has been found to be the most demanded ICT technology from a cybersecurity and privacy point of view, followed by Cloud, Mobile, Big Data and Operating Systems. The *cybersecurity applications* considered to be priorities are Energy, Public Safety, Transportation, Financial Services and Healthcare.

When analysing the *Healthcare, Financial and Maritime applications domains*, was found that most of these domains are classified as highly important priorities and are well covered by available funding programs.

The option of the team of the project has been oriented to use a mixed terminology of JRC and NIS so Cybersecurity Research Domains which include technical cybersecurity topics related to specific cybersecurity technologies and referred to this as “*Cybersecurity Technology Topics*.” The Application and Technologies vector includes the topics on various “*ICT Technologies*,” such as the Cloud, the Internet of Things, Big Data, etc., which require cyber security protection. Sectors, e.g. Healthcare, Maritime, Energy, etc., are referred as “*Applications*,” in which the cyber security technologies are applied and contextualized.

The conclusions that have been agreed stipulate that policymaking in US is a multi-layered process made up of many agencies and initiatives and as consequence it is important to note that US priorities in cybersecurity are shaped by many publications and initiatives.

Based on the documents analysed it can conclude that DARPA and the US Department of Defense invest more in cyber security (Figure 2).

By comparison to the US, the EU’s policies and initiatives on cybersecurity have been limited to concrete actions: Horizon 2020 R&I Funding Program; Contractual Public Private Partnership (cPPP) in Cybersecurity; European Cyber Security

¹³ <http://aegis-project.org/>

Organisation Initiative; European Union Agency for Network and Information Security; and The Network and Information Security Platform Initiative.

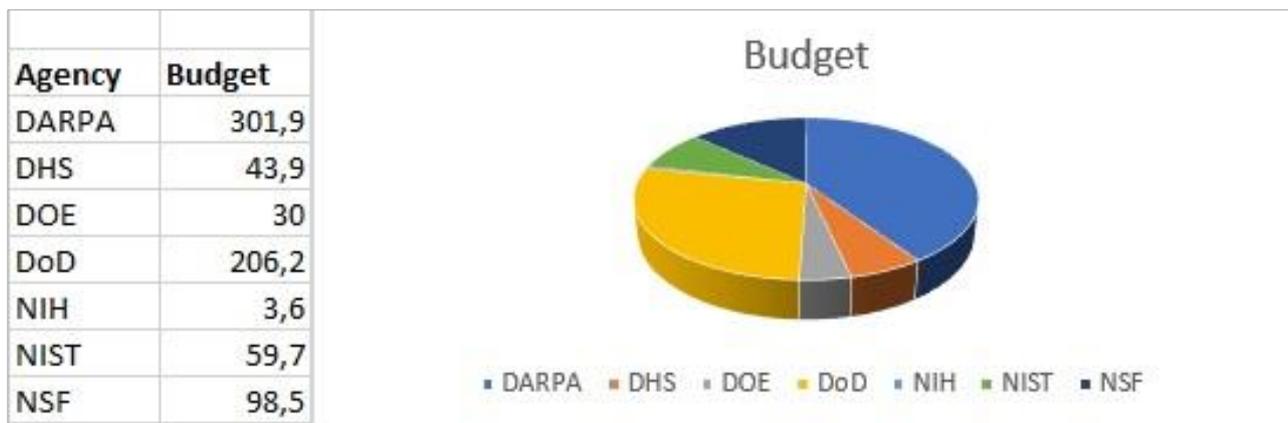


Fig. 2. 2018 Cybersecurity budget distribution for US agencies
(Source: AEGIS Project)

The most recent call on cyber security was H2020-SU-ICT-2018-2020, which closed in August 2018. The call underlined the importance of cyber security for the European digital economy and encouraged European industry players to comply with the current EU regulations and directives, such as the NIS Directive, eIDAS, GDPR and Directive 95/46/EC.

The analysis of cyber security technologies topics demonstrates that Security Management and Governance is the area that receives the highest priority. It is closely followed by Data Security and Privacy and Education and Training.

In the results, Cryptography gets a quite low score in the EU and the US. The Legal Aspects topic also gets low scores, regardless of the high scores it received in the survey (where it is referred to as the “Fight Against Cybercrime”) (Table 1).

An analysis of ICT technologies demonstrates that IoT is the leading priority topic. However, it is important to point out that there is not much difference in the first four ranked positions in the EU. This is because Cloud and Virtualization, Mobile Devices and Big Data are separated by small differences. Meanwhile, Operating Systems, the next topic in the ranking, features scores that are quite behind. It is important to note that Embedded Systems and Critical Infrastructures have very high scores in the US, but low scores in the EU (Table 2).

Table 1. Total ranking for cybersecurity technologies (Source: AEGIS Project)

Cybersecurity Technology Categories	AVERAGE			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Security Management and Governance	0.89	0.79	0.84	1	0.79	0.9	0.79	0.78	0.79
Data Security and Privacy	0.63	0.94	0.78	0.73	0.94	0.8	0.53	0.94	0.73
Education and Training	0.74	0.83	0.78	1	0.84	0.9	0.47	0.79	0.63
Assurance, Audit, and Certification	0.58	0.81	0.69	1	0.83	0.9	0.16	0.75	0.45
Network and Distributed Systems	0.68		0.68	0.73		0.7	0.63		0.63
Identity and Access Management	0.57	0.77	0.67	0.35	0.78	0.5	0.79	0.75	0.77
Trust Management, Assurance, and Accountability	0.47	0.86	0.66	0.73	0.93	0.8	0.21	0.82	0.52
Human Aspects	0.51	0.79	0.65	0.38	0.79	0.5	0.63	0.77	0.7
Software and Hardware Security Engineering	0.39	0.78	0.59	0	0.78	0.3	0.79	0.77	0.78
Operational Incident Handling and Digital Forensics	0.45	0.7	0.57	0.27	0.71	0.4	0.63	0.64	0.63
Security Measurements	0.21	0.75	0.48	0	0.75	0.3	0.42	0.73	0.58
Cryptography (Cryptography and Cryptanalysis)	0.21	0.71	0.46	0	0.71	0.3	0.42	0.67	0.54
Legal Aspects	0	0.83	0.42	0	0.85	0.4	0	0.74	0.37
Theoretical Foundations	0.08		0.08	0		0	0.16		0.16

Table 2. Total ranking for ICT technologies (Source: AEGIS Project)

ICT Technology Topics	AVERAGE			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Internet of Things	1	0.91	0.96	1	0.908	0.95	1	0.91	0.98
Cloud and Virtualization	0.71	0.88	0.79	1	0.888	0.94	0.42	0.83	0.61
Mobile Devices	0.68	0.89	0.79	1	0.885	0.94	0.37	0.91	0.58
Big Data	0.58	0.87	0.72	1	0.87	0.94	0.16	0.88	0.44
Operating Systems	0.37	0.85	0.61	0.73	0.855	0.79	0	0.79	0.3
Industrial Control Systems	0.3	0.83	0.56	0.38	0.83	0.61	0.21	0.83	0.39
Embedded Systems	0.54		0.54	0.35		0.35	0.74		0.74
Critical Infrastructures	0.49		0.49	0.35		0.35	0.63		0.63
Hardware	0	0.79	0.39	0	0.79	0.4	0	0.77	0.2
Supply Chain	0	0.75	0.37	0	0.74	0.37	0	0.77	0.19
Information Systems	0.36		0.36	0.35		0.35	0.37		0.37

Table 3. Total ranking for applications (Source: AEGIS Project)

Applications Domains	AVERAGE			EU			US		
	Desk	Surv	Total	Desk	Surv	Total	Desk	Surv	Total
Energy	1	0.85	0.92	1	0.86	0.93	1	0.8	0.9
Public Safety	0.71	0.89	0.8	1	0.91	0.45	0.43	0.81	0.41
Transportation	0.71	0.86	0.78	1	0.86	0.93	0.43	0.85	0.64
Financial Services	0.58	0.9	0.74	0.73	0.91	0.82	0.43	0.87	0.65
Health	0.37	0.92	0.64	0.73	0.92	0.83	0	0.93	0.46
Nuclear	0.54	0.54	0.54	0.65	0.65	0.65	0.43	0.43	0.43
Telecom	0.54		0.54	0.65		0.65	0.43		0.43
Water	0.54		0.54	0.65		0.65	0.43		0.43
Supply Chain	0.5		0.5	0		0	1		1
Industry 4.0	0.37	0.37	0.37	0.73	0.73	0.73	0	0	0
Defense	0		0	0		0	0		0

Energy is the application domain that is considered the highest priority (Table 3). It is followed by Public Safety and Transportation. Moreover, it is to note that in the US, it is probable that Transportation received a low score because it could be considered part of Embedded Systems (such as ICT Technology, for instance, which has very high scores in the USA). Public Safety, Financial Services and Healthcare also have low scores in the USA.

The AEGIS project's team also carried out an analysis on ICT technology in general. The findings refer to the fact that in most cases, cybersecurity technologies are well covered by existing R&I programs. There are only a few areas that require specific attention. Firstly, it has to stress the striking difference between the high demand for cryptography in many domains and the lack of attention it receives from R&I funding programs in the EU and the US. A possible explanation for this mismatch could be the fact that many ICT technologies and application domains simply require suitable methods for the application of cryptography, rather than new and stronger cryptographic schemas. Nevertheless, the topic itself should not be ignored, especially with the development of quantum cryptography (Figure 3).

Quantum computing is at once both an opportunity and a threat. One of the biggest threats concerns encryption.

Encryption provides the security and privacy for our online lives - from banking and homes to business and healthcare. It protects everything from sensitive personal data to state secrets. As the 2019 Global Risk Report¹⁴ put it, encryption forms the “scaffolding of digital life”. But what is considered safe encryption today will soon be undermined by quantum computing. It has been estimated that it would take quantum power of 4,000 qubits to break today's “strong” encryption keys. As mentioned in [26]: *“cryptography remains broken for most individuals, but the increasing availability of quantum-resistant cryptography has started to generate more demand from businesses. The US has moved to radically privatize and deregulate some of the largest quantum providers in an attempt to recapture competitive advantage over the growing - and*

¹⁴ <https://www.weforum.org/reports/the-global-risks-report-2019>

now global - quantum economy... It is possible that the broader promise of quantum computing will materialize by 2030 and beyond, but that part of the story has been significantly delayed by the ill-fated non-proliferation program. And quantum has yet to wash off the public stain of its early monopolization by the defense community.”

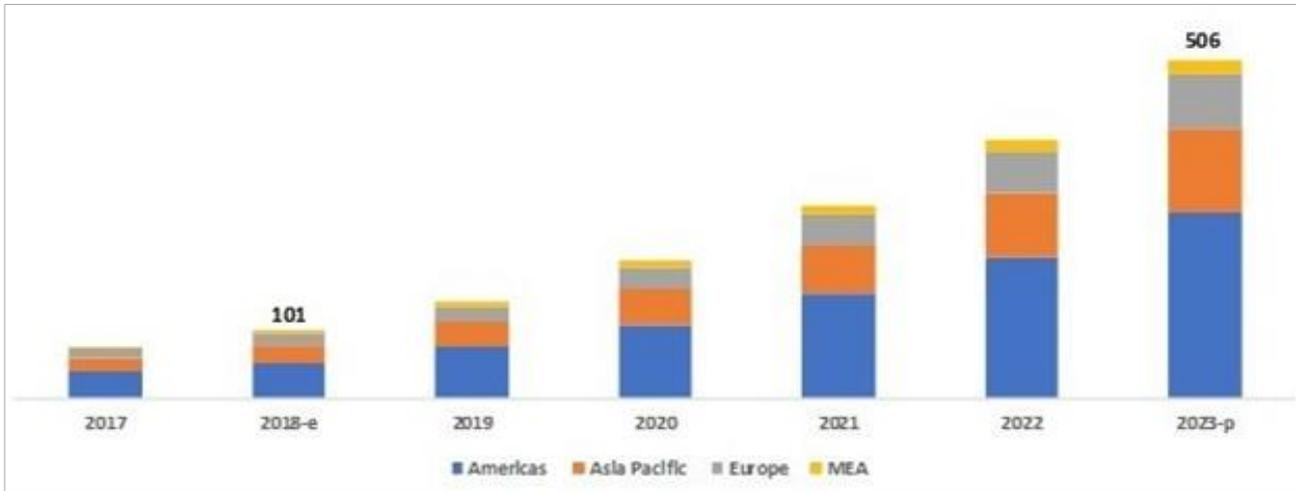


Fig. 3. Quantum Cryptography Market, by region (US D Million)

(Source: [27])

It will be necessary to pay more attention not only to the cyber security as technical problem but to the connection with social engineering because the significance of social engineering within both cyber-dependent and cyber-enabled crime continues to grow. Social engineering can take many forms. Phishing via email is still the most frequent form.

5.1. Trends in Artificial Intelligence and Cyber Security

“AI’s success against cybercrime paved the way for many other implementations of the technology to not only be accepted, but highly desired. Economic productivity jumped as the conventional distractions of the internet were curated away by AI-powered digital assistants inside firms, and the technology helped employees focus on “what matters most”. Rather than viewing the AI as dominating their perspectives or filtering information through the lens of their corporate creators, most people found the technology to be truly useful, enriching assistants in their daily lives” [26]

It is noteworthy that although the terms cyber security and information security can be used interchangeably, it does not mean the same thing.

In terms of information security, the biggest concern is protecting data from illegal access of any kind. In the field of cyber security, the biggest concern is the protection of data from illegal digital access. In other words, cyber security works to protect digital information, while information security works to protect all information, whether or not it is stored digitally. Cybersecurity analytics is defined as the study of the digital traces left behind by cybercriminals to help to better understand the weaknesses and how to prevent similar violations in the future.

AI combines with cyber security to create a new kind of tools called threat analytics. Machine learning allows threat analytics to provide greater accuracy in the context of the risk context, especially involving the behavior of privileged users, details a recent account in [29]. The usual belief that millions of hackers have gone to the dark side and orchestrated massive attacks on vulnerable businesses is a misconception. The most brutal truth is that companies do not protect their privileged access credentials from easy access.

Machine Learning (ML) algorithms allow threat analytics to immediately detect anomalies and non-normal behavior by tracking authentication, geolocation, and connection time patterns and many other variables to calculate a risk score.

The benefits of cyber security analytics can include: a more visual analysis process, usable by business users; a more holistic view of security considerations, such as how an attack fits in the context of existing systems; increased ability to enrich data, making data elements more useful; support for IT departments; and a look at the ignored data sources that may be important for understanding security threats. Adding Artificial Intelligence (AI) tools to the cyber security mix adds more power to existing technologies and leads to more efficient practice. AI knowledge charts can act as repositories for the huge amount of constantly produced data, helping to identify patterns and relationships that matter. This may allow a more efficient predictive analysis. ML has proven valuable in behavior analysis and countermeasures implementation.

6. Conclusions

Over the last decade, cyber security has drawn the attention of media and experts. Although it is a global phenomenon, this paper focuses on comparing two significant situations: those in the EU and those in the USA on the one side, on the other side, EU initiatives and NATO initiatives. If in the USA the issue of cyber-security has been dealt with and discussed since the 1990s, the discussion in the European Union began only in the early 2000s. Without prejudice to the growing interest in governmental agencies and the proliferation of initiatives in this regard, it is interesting to note that cyber-related terms are used in a rather heterogeneous and ambiguous manner at international level without a common definition of cyber threats. A reading of the relevant strategic documents adopted by the EU and the USA in recent years offers interesting indications in this respect. The analysis of the main US strategic documents shows that these documents deal with the issue of cyber security in a much wider way compared to European documents.

So the first Section dedicated to the general situation in Europe and Worldwide is followed by the second section enumerating several facts and initiatives in EU connected to the problems created by the definitions and, above all, their harmonization and the different initiatives projects launched and supports specifically focused on enhancing the resilience of critical information infrastructures and networks that supported the vital services of selected priority of countries in the world.

Special attention was paid to a short presentation of NATO policy and enumeration of NATO activities and initiatives in connection of defence and to the short presentation of EU-NATO common threats and common solutions. This framework was complemented by an analysis of the priorities for R&I identified in a financed EU project and, finally, has been underlined that most major industries already use Machine Learning (ML) and artificial intelligence (AI) to automate their processes and improve overall performance. Cyber security and cyber crime are not an exception.

Other highly sensitive issues refer to the following aspects: (1) AI is often considered to be a dual-use technology - while many cyber security companies

implement AI-based algorithms to prevent threats, hackers take advantage of the opportunity to become more efficient and (2) most AI qualities serve also harmful purposes: AI systems are cheap, scalable, automated, anonymous and offer physical and psychological distance to the attacker, diminishing the immediate morality around cyber crime. With new advances in AI-based technology, the use of AI in cyber attacks will become an even more popular but, in the same time, dangerous trend.

References

- [1] Panagiota-Nayia Barmaliou, The EU Experience in Global Cyber Capacity and Institution Building, Available: <https://www.thegfce.com/news/news/2016/06/20/eu-experience-in-global-cyber-capacity>. [Accessed: May 8, 2019].
- [2] Paul Cornish, Rex Hughes and David Livingstone, 2009, Cyberspace and the National Security of the United Kingdom. Threats and Responses, London, Chatham House, March 2009 (A Chatham House Report), Available: <http://www.chathamhouse.org/publications/papers/view/109020>. [Accessed: May 8, 2019].
- [3] Marushka Monette Dias, 2019, 2019 cyber security trends that are here to stay!, Available: <https://www.linkedin.com/pulse/2019-cyber-security-trends-here-stay-marushka-monette-dias/>. [Accessed: May 2, 2019].
- [4] Di Camillo, Federica, Valérie Miranda, 2011, Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward, IAI Working Papers, Issue 26, ISBN/ISSN/ DOI: 978-88-98042-32-6.
- [5] William H. Dutton, Fostering a cyber security mindset, in Internet Policy Review, Vol 6, Issue 1, 2017, Available: <https://policyreview.info/articles/analysis/fostering-cyber-security-mindset>. [Accessed on May 7, 2019].
- [6] Simon Kemp, THE STATE OF DIGITAL IN APRIL 2019: ALL THE NUMBERS YOU NEED TO KNOW, 2019, Available: <https://wearesocial.com/blog/2019/04/the-state-of-digital-in-april-2019-all-the-numbers-you-need-to-know>. [Accessed on May 2, 2019].

- [7] Patryk Pawlak and Panagiota Nayia Barmaliou, “Politics of Cybersecurity Capacity Building: Conundrum and Opportunity”, *Journal of Cyber Policy* 2, no. 1 (March 2017), pp. 123-144.
- [8] Patryk Pawlak, „Cyber Resilience,” in *After the EU Global Strategy - Building Resilience*, ed. Florence Gaub and Nicu Popescu (Paris: EU Institute for Security Studies, 2017), pp. 17-20.
- [9] Patryk Pawlak, Protecting and defending Europe’s cyberspace, in *HACKS, LEAKS AND DISRUPTIONS RUSSIAN CYBER STRATEGIES*, Chaillot Paper, Nicu Popescu and Stanislav Secrieru Eds., 2018, pp. 103 - 114, European Union Institute for Security Studies Paris.
- [10] Bruno Lété and Piret Pernik, *EU-NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*, in GMF, Dec. 2017, Policy Bref, pp. 1 - 9.
- [11] Gil Press, 60 Cybersecurity Predictions for 2019, 2018, Available: <https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/#1e5eeb6e4352>. [Accessed: May 8, 2019].
- [12] Alison DeNisco Rayome, As IoT attacks increase 600% in one year, businesses need to up their security, March 21, 2018, Available: <https://www.techrepublic.com/article/as-iot-attacks-increase-600-in-one-year-businesses-need-to-up-their-security/>. [Accessed: May 2, 2019].
- [13] “The Changing Face of Data Security. 2019 Thales Data Threat Report”, Global Editor, #2019 Data Threat, Available: <https://www.thalesecurity.com/2019/data-threat-report>. [Accessed: May 7, 2019].
- [14] „Anticipating the Unknowns. Chief Information Security Offices (CISO) Benchmark Study”, *CISO CIBERSECURITY SERIES*, 2019, March, Available: <https://ebooks.cisco.com/story/anticipating-unknowns#!/page/6/6>. [Accessed: May 2, 2019].
- [15] New Report Finds Global Ransomware Damage Costs Predicted to Exceed \$8 Billion in 2018, Available: <https://www.knowbe4.com/press/>

new-report-finds-global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018. [Accessed: May 2, 2019].

- [16] CyberArk Global Advanced Threat Landscape Report 2018: The Cyber Security Inertia Putting Organizations at Risk, Available: <https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018/>. [Accessed: May 2, 2019].
- [17] „Charting a new course - When investigating in cybersecurity isn't the answer”, Cybersecurity Insights, Vol 8, AT7T Business.
- [18] European Commission, “Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters,” COM (2018) 225 final, 17 April 2018.
- [19] The Commission Communication on the EU Strategic Approach to Resilience defines resilience as ‘the ability of an individual, a household, a community, a country or a region to withstand, adapt and quickly recover from stress and shocks’.
- [20] European Commission, ”Joint Communication on Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU” Join (2017) 450 final, September 13, 2017, Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN>.
- [21] NATO official: need to innovate faster in cybersecurity By EUOBSERVER 10. Oct 2017, 11:11, Available: <https://euobserver.com/tickers/139361>. [Accessed: May 3, 2019].
- [22] European Commission, Digital Single Market News, “EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity - Cybersecurity Strategy and Proposal for a Directive,” February 7, 2013.
- [23] North Atlantic Treaty Organization, “Cyber Defense,” Updated November 10, 2017, Available: https://www.nato.int/cps/en/natohq/topics_78170.htm. [Accessed: May 3, 2019].
- [24] Joint Communication to the European Parliament and the Council,” JOIN, 2017: 0450 final.

- [25] Tufiş, D., Ioniță, A. & col.: “Siguranța Informatică - Protecția Cibernetică, Protecția Proprietății Intelectuale în Proiecte și în Publicarea Electronică”, STRATEGIA DE DEZVOLTARE A ROMÂNIEI ÎN URMĂTORII 20 ANI, vol. 2, Editura Academiei, ISBN 978-973-27-2615-0, pp. 121-149, 2016.
- [26] Cybersecurity Futures 2015 Insights and Findings, February 2019, Available: <https://cltc.berkeley.edu/wp-content/uploads/2019/02/Cybersecurity-Futures-2025-Insights-and-Findings.pdf>. [Accessed: May 2, 2019].
- [27] Quantum Cryptography Market by Component (Solutions and Services), Services (Consulting and Advisory, Deployment and Integration, and Support and Maintenance), Security Type (Network and Application Security), Vertical & Region - Global Forecast to 2023, Available: <https://www.marketsandmarkets.com/Market-Reports/quantum-cryptography-market-45857130.html>. [Accessed: August 19, 2019].
- [28] Michael Daniel, Why Is Cybersecurity So Hard?, May 22, 2017, Available: https://hbr.org/2017/05/why-is-cybersecurity-so-hard?referral=03759&cm_vc=rr_item_. [Accessed: August 19, 2019].
- [29] Louis Columbus, 2019, Machine Learning Is Helping To Stop Security Breaches With Threat Analytics, Forbes, Jun 16, 2019, Available: <https://www.forbes.com/sites/louiscolumbus/2019/06/16/machine-learning-is-helping-to-stop-security-breaches-with-threat-analytics/#4392cc7977ea>. [Accessed: July 4, 2019].
- [30] EU Cybersecurity, 26 June 2019, Available: <https://www.eubusiness.com/topics/internet/eu-cybersecurity/>. [Accessed: June 30, 2019].

The Importance of Cooperation in Cybersecurity

Iulian ALECU

Romanian National Computer Security Incident Response Team (CERT-RO)
iulian.alecu@cert.ro

So much is talked about cooperation that there isn't a conference, meet-up or exhibition that fails to mention the importance of cooperation.

Yet, while it is so often discussed, it either doesn't take place on the level it should or does not occur everywhere it should. Of course, there is always the scenario in which it is only talked about in order to have a different topic of conversation or subject for presentation, but this will not be discussed here.

So much has been spoken and written about cooperation that I do not believe I could add something entirely new. I will, however, discuss cooperation from the perspective of my position within the National Cyber Security and Incident Response Team (CERT-RO).

First, it is essential to understand what is meant by "to cooperate". The word originates from the Latin verb "cooperari" (*cooperationem, cooperatus, cooperātiō*), formed from the prefix "co-", meaning **together**, and the verb "operari" (*operari, operatus*), meaning **to work**. Therefore, if I decide to cooperate with someone and they agree, this means we will be **working together** on a project or in a given field.



Photo source: *Effective Software Design*

aware of a different facet of this issue, with which to pool together knowledge in order to gain a deeper - but not comprehensive - understanding of the matter. And so forth...

The more we delve into this phenomenon, the more we understand how little expertise we have. One can draw a parallel to everyday life: the more you know, the more you realize how little you truly grasp.

In most conferences and events that I attended, cooperation was touted as a response to the question: “So what else should we be doing?”; the answer arrives quickly and with a smile: “We should cooperate.”



Photo source: *Phys*

Reality, however, tells a different story: cooperation lies at the very foundation of the institution, colleagues cooperate with each other as a matter of course; it is an intrinsic part of the job, without which the entity cannot achieve its goals.

Thus, in practice, cybersecurity begins with cooperation from the most basic level, up to the most complex. Moreover, cooperation is one of the prime mechanisms available to us when handling matters in this field.

Therefore, it is my opinion that one of our greatest issues is being so preoccupied with the technical aspect and its complexity that we often disregard one of the main tools in our arsenal, cooperation, which is always available and can help us save time and resources.

A significant advantage of cooperation is its adaptability, both horizontally and vertically - to use a well-known phrase, “the sky’s the limit” - which is quite significant. In other words, all the problems we cannot solve on our own could be dealt with through cooperation.

There are, however, some obstacles. One of them is the legal framework. Yes, we desire cooperation, but the law does not simply allow us to do so in whichever form we wish. While this may be true, one can look to nations more advanced than ours with respect to cooperation in the field of cybersecurity. They did not use to have the appropriate legal frameworks either, but they created them because cyber threats were a matter of national priority.

Of course, this may only serve to discover further hindrances. The pursuit of change requires vision, creativity, commitment, perseverance and determination. These, however, do not pertain to the spectrum of cybersecurity. They belong in an entirely different field, one that is not broached in this article.

A Cooperative Approach: the UK's Active Cyber Defence Programme

Jon BROWNING

National Cyber Security Centre, United Kingdom
enquiries@ncsc.gov.uk

1. Introduction

The UK continues to be one of the most digital economies in the world, with ever more of our lives being online. As this digitalisation continues, the potential real world impact on real people of cyber crime and cyber attack increases. This essay will examine how the UK Government's National Cyber Security Centre (NCSC) is improving the security of the country's public sector and the wider cyber ecosystem through its world-leading Active Cyber Defence (ACD). ACD represents a significant step-change in the UK's approach to cyber security, because of its voluntary, non-regulatory, non-statutory, approach delivered in partnership between central government, local government and business. As difficult as this sounds, two years in we can provide evidence that it works. In sharing this knowledge, we hope to inspire other countries to adopt bold measures, in partnership with industry, to protect their digital homelands.

The NCSC is the UK's technical authority on cyber security. It is part of GCHQ, the UK's signals intelligence agency, and was formed in 2016 to provide a unified national response to cyber threats.

Introduced by the NCSC in 2016, ACD is a bold, interventionist approach that stops millions of cyber attacks from ever happening. The programme seeks to reduce the harm from commodity cyber attacks against the UK by protecting the majority of people from the majority of the harm caused by the majority of the cyber attacks the majority of the time. The NCSC has developed a set of pioneering services including Web Check, Mail Check, Public Sector DNS and a takedown service:

- Web Check helps make websites a less attractive target, by finding obvious security issues and pointing them out to the website's owner so they can fix them.
- Mail Check helps public sector organisations take control of their email, making phishing attacks which spoof those organisations more difficult.
- Protective DNS blocks public sector organisations from accessing known malicious domains.
- The Takedown Service finds malicious sites (either attacks or attack-supporting infrastructure) and sends notifications to the host or owner to get them removed from the internet.

The ultimate goal is for there to be fewer cyber attacks in the world, and more specifically, less harm from cyber attacks globally.

2. Successes

The NCSC is committed to providing an evidence base to help judge the effectiveness of the ACD measures and to do so in a transparent way, as per our stated aims. We publish an annual report, setting out detailed analysis of the outcomes achieved and honest appraisal of the services, alongside future ambitions.

Now in its second year, we can report on the effects of our tools on the cyber ecosystem. At a top level, our analysis evidences unequivocal success, with figures for 2018 showing:

- The NCSC took down 22,133 phishing campaigns hosted in UK delegated IP space, totaling 142,203 individual attacks;
- 14,124 UK government-related phishing sites were removed;
- The total number of takedowns of fraudulent websites was 192,256, with 64% of them down in 24 hours;
- The number of individual web checks run increased almost 100-fold, and we issued a total of 111,853 advisories direct to users.

Moreover, a combination of ACD services has helped the UK tax authority's own efforts in massively reducing the criminal use of their brand. Her Majesty's

Revenue and Customs (HMRC) was the 16th most phished brand globally in 2016, but by the end of 2018 it was 146th.

In 2018 we used ACD tools to tackle advanced fee fraud impersonating the UK legal sector. Both bogus law firms, and impersonation of legitimate law firms, are techniques used by fraudsters in an attempt to increase the credibility of their attacks. Increasingly, we're seeing scammers use real law firms and other entities to try to make their attacks look more legitimate. There's no common brand being abused here, so no-one is incentivised to go after these attacks. However, the reputational and financial impact is significant.

Elsewhere, we've been tackling the abuse of public sector email domains. One such incident occurred at the height of the summer 2018, when criminals tried to send in excess of 200,000 emails purporting to be from a UK airport, using a non-existent gov.uk address in a bid to defraud people. However, the emails never reached the intended recipients' inboxes because the ACD system automatically detected the suspicious domain name and the recipients' mail providers never delivered the spoof messages. The real email account used by the criminals to communicate with victims was also taken down.

And finally, ACD tools highlighted a primary school network behaving as though infected with Ramnit, a worm which affects Windows systems. The local authority was notified and they investigated with the network owner. The antivirus software that was installed on the school's endpoints was not working, unbeknown to the local authority or the school. As a result, the school had a wide level of infection. Not only did the ACD tool block the malicious connections, containing any harm, it also identified the malware and notified the local authority. The fix was uncomplicated, the local authority installed a working antivirus and it cleaned up the infection within a day.

3. The future of ACD

These are just some examples of the value of ACD, and where they protected thousands of UK citizens and further reduced the threat of UK brands being exploited

by criminals. While this and other successes are encouraging, we know there is more to do. We have a number of projects in the pipeline, including:

- A new automated system which allows the public to report suspicious emails easily. The NCSC aims to launch this system to the public later in 2019;
- The Infrastructure Check service: a web-based tool to help public sector and critical national infrastructure providers scan their internet-connected infrastructure for vulnerabilities;
- Exploring additional ways to use the data created as part of the normal operation of the public sector protective DNS service to help our users better understand and protect the technologies in use on their networks.

4. Conclusion

One of the founding principles of the NCSC was making decisions based on evidence and being as transparent as possible in that. While the ACD programme is still young, we believe it demonstrates the value of the new approach adopted by the Government in the National Cyber Security Strategy. We are not expecting ACD interventions to be perfect, or to defend against every single type of cyber attack. However, we continue to believe that the ACD programme - by providing real services and generating real data and analysis - has to be a first step in demystifying cyber security, and in beginning to tackle the impacts of cyber attacks at scale. However, cyber crime really does run on a return on investment model, and if we can affect that, we can demotivate attackers.

The NCSC is not the only organisation with good ideas, and the UK is not the only country connected to the internet. We would welcome partnerships with people and organisations who wish to contribute to the ACD service ecosystem, analysis of the data or contributing data or infrastructure to help us make better inferences. We believe that evidence-based cyber security policy - driven by evidence and data rather than hyperbole and fear - is a possibility.

Collaboration: The Key to Disrupting Cyber Attacks

Matt LAVIGNA, Tara TRICKETT

National Cyber Forensics and Training Alliance (NCFTA), United States of America
ttrickett@ncfta.net

1. The Current State in the Field

No matter what media you turn to today, headlines the world over are certain to include some level of cyber security breach or threat. Twenty-nineteen statistics show that security breaches have increased over the last year by 11% and by 67% over the past 5 years [1]. The two fastest growing attacks are people based. Malicious Insider attacks are up 15% while Ransomware attacks are up by 21% [1].

While cyber threats are on the rise, private industries are on their own to navigate cyber threat preparedness. Industries struggle to be successful in this area due to the beliefs that it won't happen to them and it's not their issue.

The belief that you are too big or too small to be impacted by a cyber security attack is absolutely false. A novice hacker may initiate his malicious acts by "cutting his teeth" on small businesses who are less likely to have robust security measures in place due to financial constraints. However, as the hacker matures and his skill set becomes more sophisticated, he will move up the food chain to larger more secured infrastructures. That is assuming that all cyber-attacks are targeted. Leveraging a leased distribution network, or botnet, virtually anyone can widely deploy malicious code or phishing schemes to potential victims anywhere in the world. Therefore, no one is immune to the possibility of a cyber-attack. While many organizations believe that they must implement some level of cyber security, there is often lack of knowledge as to where responsibility for such an implementation should lie. Often businesses believe that the Information Technology departments should be the sole overseer of all things cyber related. However, developing, implementing and managing a robust cyber security program takes a village, or perhaps at a minimum, a cyber-neighborhood. It is

equally important for all levels of management and all departments to be active participants in the cyber security processes of the organization. While the information technology team is responsible for the computers and the network that supports the data, the departments are ultimately responsible for the data's availability and integrity.

Collaboration begins at the business level. Department heads need to understand the importance of their data and how to best preserve and protect it. The IT team can then help the departments by implementing any hardware or software that is needed to maintain the availability of the data and the continuation of business.

2. Emerging Trends

While data theft has been the focus of threats in recent years, cyber criminals are now showing an interest in disrupting business and destroying the data that the businesses rely on. Even more disturbing is that particular data could be manipulated to have an impact on the integrity and value of that data. The criminals are now focusing on two objectives. The first objective is to gain access to an organization's data and then modify or destroy critical information to destroy the integrity of the business data. Prior to this, the focus was on gathering the data and selling it. Selling off the data is now a side benefit. Secondly, the criminals are exploiting the human factor by issuing phishing attacks where unsuspecting victims are tricked into downloading and applying malware that then impacts other contacts that the victim may be connected to.

The most disruptive and disturbing emerging trend is the fact that moving forward battles will be started, fought, and won from behind a computer screen. The battles may be initiated by foreign entities or domestically. Due to the accessibility to credentials on the dark web, it has never been easier to wage an attack on another person, business or government. A single individual armed with the right information procured on the dark web could destroy the livelihood of their neighbor, taint the reputation of a business or wage a personal war with a department of the government. From a global standpoint, countries have organizations of individuals who sit behind computers spying on other people and countries. These individuals have the ability to

reach out and attack using cyber technology. These “attacks” are executed quickly and quietly by an anonymous face sitting behind a computer screen.

3. Future Directions and Recommendations for Improving the Current State

Industries need to place a focus on cyber security programs. The first step is a business must focus on securing the data that they house. With GDPR and many other privacy regulations, leakage of personal data can cost a business more than \$178 per record [2]. It is in the best interest of any organization to implement tools that can help notify of active attacks. The second step is to develop training for all employees. With phishing and malware being a growing area of threat, industries need to make sure that the individuals that work for them, and by extension third parties they do business with, can identify these threats and that they know how to respond to them.

Collaboration is going to be the key component to standing up to the cyber bullies of tomorrow. Criminals rely on the fact that their victims aren’t talking to one another and can therefore use the same TTP’s over and over. No one organization is going to have the answer to solving every attack that is distributed. Members of all business sectors as well as governments, and law enforcement need to come together to learn of and brainstorm solutions for emerging threats. Being a member of a collaborative cybersecurity group has many advantages. Organizations can learn of threats affecting others in their field and be aware that they may soon see the same attack. They can take the information regarding emerging threats and harden their environments to build a proactive defense against it. Organizations can draw on the diverse knowledge of the group to make decisions on the best defensive measures to put in place in their own environment.

Law enforcement should be an integral member of a truly successful cyber information sharing group. Without the disruptive powers of a committed law enforcement component, the threats actors will get richer, smarter, and not be deterred.

There are many groups coming together to collaborate on cybersecurity issues. The biggest hurdles to overcome in such a group are developing an environment of

trust and a mentality built around equal sharing of information. All groups involved in the collaboration must be able to trust the others. They need to be certain that the others in the group are not going to use the information they are sharing to do harm, use to gain a competitive advantage, or make public statements that could harm the reputation of another. This trust can be very hard to build but is critical to the collaboration's success. The other hurdle is equal sharing. All members of a collaborative group must be willing to share information. If an organization is dealing with an attack, they must be willing to talk about it. By doing so, others in the group can discuss similar situations or provide advice for remediation. Even governmental and law enforcement members must contribute to the conversations. Organizations not being willing to share equally will only hinder any trust building within the collaborative group.

4. Conclusions

Cyber criminals have developed a well-oiled network to communicate vulnerabilities within systems as well as share private information. They are sharing this information every day in order to improve existing attack methods and develop new attacks. With the criminals working so closely together, the public sector is always ten steps behind. The only way to get ahead of the cyber criminals is through collaboration. The collaboration must start internally and must include all business levels from the executive level down to the departments that rely on the data they hold.

Moving forward it will be critical for all industry, government and law enforcement sectors to work together. By working together, they can develop plans for thwarting cyber-attacks.

References

- [1] Cyber Resilient Business: Ninth Annual Cost of Cyber Crime Study <http://www.accenture.com>. [Accessed: May 30, 2019].
- [2] The Average Cost of a Data Breach <https://securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx>. [Accessed: June 3, 2019].

SELEC's Role in the Fight Against Cyber Crime

Robert PĂTRĂNCUȘ

Operational Directorate, Southeast European Law Enforcement Center (SELEC)
rpatrancus@selec.org

1. Introduction

The globalization of crime is a process that started many years ago and its outcome can be easily seen today. Enabled by the technology development, cybercrime is a continuously growing and evolving white-collar global phenomenon that affects all the countries as the criminals are no longer confined to physical boundaries.

It is clear that cybercrime cannot be addressed by each country individually, but through a synergy of actions from all the actors involved, therefore, a growing police and judicial cooperation need can easily be observed. Except for the well-known cooperation channels (*e.g. liaison officers, bi/multilateral agreements*), international organizations that brings together, in the same place, liaison officers from different states and offer platforms for information exchange, play the most important role by offering the most comprehensive and fastest channel for law enforcement cooperation.

There are a few international bodies dealing with Police and Customs cooperation in Europe, in this section I would like to focus on a successful story, namely the regional body Southeast European Law Enforcement Center (SELEC).

2. About SELEC

2.1. SELEC's role and its Member States

SELEC is a treaty-based¹ international law enforcement organization bringing together the resources and expertise of Police and Customs authorities that join efforts

¹ The Convention of the Southeast European Law Enforcement Center, entered into force on 7th of October 2011

in combating more effectively trans-border organized crime in Southeast Europe. SELEC, as successor of SECI Center founded in 1999, is established to provide support to its 11 Member States, to enhance the coordination in preventing and combating crime, including transnational serious and organized crime.

The 11 Member States of SELEC are:



Fig. 1. SELEC Member States

Since 2003, under SELEC's auspices, it functions the Southeast European Prosecutors Advisory Group (SEEPAG) that facilitates and speed up the cooperation in trans-border crime investigations and cases in Southeast Europe.

2.2. Organizational structure and partners

To implement the SELEC convention, in each Member State it was established a National Unit which consists in: (i) The National Focal Point (NFP) which acts as single point of contact in the Member States and (ii) Liaison Officers from Customs and Police who are located at SELEC HQ and represent the State.

SELEC also has 24 partner countries and organizations. The Operational partner status grants the right to exchange personal data, while the Observer Status entails the right to receive only strategic information.

3. SELEC's Operational approach in fighting cybercrime

SELEC has not a public annual strategy on cybercrime; however, it has a permanent strategy set up in line with its mandate and focused on operational priorities.

In this respect, SELEC provides a multinational expertise to law enforcement authorities (LEA) across the Southeast European region offering the necessary platform for exchanging information and requests of assistance, supporting operational meetings, joint investigations and regional operations, as well as delivering quality analytical products.

SELEC is organized as an operational entity, all its activities being conducted within the framework of eight specialized Task Forces:



Fig. 2. SELEC Task Forces

3.1. Financial and Computer Crime Task Force

When we discuss on cyber-related activities, these are concentrated within the Financial and Computer Crime Task Force.

This Task Force was established in 2001 and it is coordinated by Republic of North Macedonia and has regular meetings, providing forums for experts to share good practices and challenges, to initiate joint investigations, to evaluate the activities conducted and to decide upon further steps to be taken at regional level, as part of a common and more efficient endeavor for tackling cross-border cybercrime.

3.2. Exchange of information

The exchange of cybercrime information is one of the key operational activities, this being conducted via the Liaison Officers posted permanently by the Member States at SELEC HQ.

The exchange of information and requests of assistance (including those referring cybercrime) is carried out through the National Units composed of Liaison Officers (LOs) and National Focal Points (NFP), as depicted in Fig. 3.

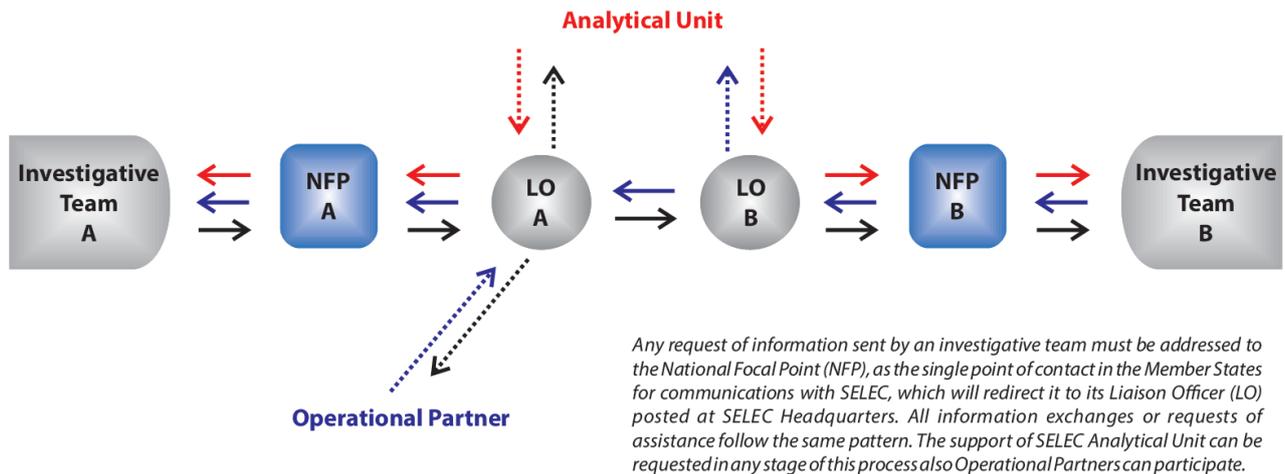


Fig. 3. Information flow

With a view of further enhancing the capacities of LEA a new Operational Centre Unit, with cutting-edge technology, will be opened in 2019.

The aim of the OCU is to increase the operational capacity of the law enforcement authorities. The OCU will bring together information from the entire SELEC region, EU and non-EU countries, thus addressing a proper operational response to different threats.

A real-time exchange of information and criminal intelligence among SELEC Member States and Operational Partners, subsequently collected, collated, processed, analyzed and disseminated will support better operational, tactical and strategic decisions and efficient actions against the organized crime groups.

The OCU is permanently interconnected with SELEC Member States through the National Focal Points (NFP).

3.3. Joint investigations

SELEC’s joint investigations aim to tackle trans-border cybercrime in SELEC region. They are conducted under the coordination of SELEC based on the proposals coming from the Member States or Operational Partners.

SELEC operational meetings, as part of joint investigations, are attended by law enforcement officers and prosecutors in order to exchange additional intelligence, and to plan future operational and judicial activities.

Many successful cyber-related joint investigations were carried out under SELEC umbrella, and I would like to shortly describe some of them because they are examples of good practices in operational international cooperation.

Joint investigation CORVUS was conducted by Greek, Romanian and Turkish authorities, with the support of Israeli authorities with the purpose of investigating a special case which initially started as a test for deep inserted skimming case.

During the investigation surveillance activities and wiretapping of almost 85 suspects, intelligence about other crimes too, such as drugs trafficking or extortion, was also collected.

As a result of the investigation, 20 suspects were prosecuted for crimes such as setting up an organized criminal group, making fraudulent financial operations, illegal access to an IT system, counterfeiting of bonds or payment instruments, circulation of counterfeited securities and money laundering.

Joint investigation PRATKA/VIRUS targeted dismantling the organized crime group that consisted of Bulgarian nationals having connections in Republic of North Macedonia, Hellenic Republic, Romania and Republic of Serbia.

The modus operandi used was corrupting Customs officers in all involved countries with the purpose to infiltrate a virus in the Customs' computerized systems in order to avoid the payment of taxes. The Bulgarian authorities have searched more than 100 addresses, suspects and vehicles.

A large quantity of money was seized, as well as equipment, devices for communication, computers, tablets, bank documents, etc. 23 suspects were arrested, 5 of them acting or being former Bulgarian Customs officers.

As result of this criminal activity the damages recorded by the Customs Agency, only for year 2015, was around 5 million Euro. It was determined that the members of the organized crime group invested the money obtained from these illegal activities in Bitcoins.

Joint investigation MONEY MULES between Republic of Moldova and Romania targeted an organized criminal group consisting in Moldovan, Romanian and Ukrainian nationals, dealing with cybercrime.

The modus operandi of the group consisted in organizing a network of “mules” (persons with double citizenship) that received the money from illegal transactions, as result of cyber-frauds committed by suspects from Russian Federation and Ukraine, in accounts opened in EU countries, withdraw the money and transport it, in cash, to Republic of Moldova in order to be distributed to the higher level members of the organized criminal group.

The estimated damages were in value of 6 million Euro. Following simultaneous actions, 19 persons were taken in custody.

Joint investigation SIMBOX involved authorities from Republic of North Macedonia and Republic of Serbia, and targeted an organized criminal group dealing with illegal transfer of international phone traffic to national phone traffic.

The operation led to the arrest of 1 person, placing 10 persons under financial investigation, and seizure of several SIMBOX devices, over 40,000 SIM cards, and computer equipment. The organized criminal group illegally started using telecommunication devices for the use of telephone calls termination.

The devices were connected through internet and using the network of foreign mobile communication operators, with their SIM cards, were establishing international communication at the price of a local voice call. In this way they bypassed international telephone traffic using “VOIP” technologies on unregistered pre-paid mobile telephone terminals.

As a result of this criminal activity, the mobile communication operators suffered a financial loss of more than half a million Euro.

4. Strategic approach in fighting cybercrime

From strategic point of view, SELEC supports its Member States from many viewpoints, but I would like to mention herein the most relevant: (i) providing reports, (ii) organizing regional events, (iii) initiating regional projects, (iv) offering trainings for LEA.

SELEC support its Member States by providing strategic reports, the latest report being the Organized Crime Threat Assessment for Southeast Europe (OCTA SEE

2018), covering years 2013-2017 (the main aspects of this report are detailed in the next chapters).

SELEC also provides a platform for trainings, having a fully-equipped Training Center, as part of its HQ.

In the framework of the EU project S.I.R.A.S, the training room was upgraded with cutting edge technology (laptops, server, network attached storage, projector, software tools, a/o). Focusing on the fight against the most sophisticated and fast-evolving types of cybercrime, this initiative is another example of SELEC's constant effort to lead the law enforcement endeavors in Southeast Europe.

As a part of SELEC cyber-related strategy, the center has already hosted and organized in the last years specific training on Darknet and cryptocurrency investigation, as per example: investigations on the Surface Web and Darknet (three sessions - 2 first-level and 1 second-level) and, jointly with DEA, online investigations, virtual currency and dark web.

4.1. OCTA SEE 2018

OCTA SEE is a qualitative assessment, a strategic report, illustrating the current situation and trends, identifying threats in SELEC Member States, highlighting vulnerabilities and opportunities revealed by various types of crime.

The organized criminal groups (OCGs) are increasingly incorporating technology and the Internet into their criminal activities, either by committing cybercrimes or by using them to commit other crimes. For all these reasons the report carries the motto "Crime Steers Online" and it applies to all the major crime areas today.

4.2. OCTA SEE 2018 - Key findings on cybercrime

In the area of cybercrime, the public version of the report compiles the regional current state, emerging trends and cyber-related challenges, as follows:

- Cybercrime embraces many forms in the region, classified into three categories: cyber-dependent crime, cyber-enabled crimes, and payment card frauds.

- Cybercrime has increasingly been commercialized and converted into a business-like concept. Cyber-as-a-service has opened the door to any person looking to commit cybercrimes, regardless of the level of their technical IT skills.
- As a result of the expansion of the mobile devices, there is an undeniable recent and emerging cyber-threat to all the Internet-connected mobile devices. The attacks and malware against them are expected to increase in number and complexity.
- Nowadays, cybercriminals are as diverse as the real world criminals. An important role is given to “money mules”. Related to OCGs, there is a wide-range of structures, ranging from hierarchical to horizontal, with cell-like structures located in other countries on the globe.
- New technologies may be used increasingly by the cybercriminals. For instance, they may task artificial intelligence to study the behavior of the social media users and subsequently initiate social engineering attacks, or we could see in the future “artificial” hackers with a human-like ability to learn to commit cyber-attacks.
- In the next future we may have an overflow of AI-powered malware.
- New tools available to criminals such as open source intelligence (OSINT), Social Network Analysis, chat bot, misuse of Linked Data, and profiling may be used to initiate complex attacks against many victims simultaneously.
- Blockchain technology has experienced in the last years a notable breakthrough, and, as an outcome of this technology, many cryptocurrencies have emerged recently. The cyber-criminals will definitely continue to use this opportunity, especially the one offered by the privacy coins created to avoid tracking.
- The permanent evolving Darknet continues to represent a major challenge. There are dozens of Darknet markets (open or requiring registration, or accessed strictly based on an invitation) linked to cybercrime-as-a-service, offering illegal items, including cybercrime tools, credit card data, services.

- SIM BOX frauds are used in the region to bypass the international calls.
- In line with traditional crime becoming more connected to cyberspace and criminals becoming more aware of its added value, we can expect to see more and more specialists hired to carry out cyber-attacks to complement other criminal activities.
- Using mainly DDoS, more and more the targets of the cybercriminals are servers and infrastructure of the public and private sectors.
- Ransomware continues to have enormous potential to develop. The ransomware on mobile devices will be most likely one of the major threat.
- Cybercriminals will probably focus on techniques to obtain cryptocurrencies through various means, such as cryptojacking or wallet address stealer.
- Bearing in mind its nature and the fact that it may be used to commit many other crimes, identity theft can be put in the midpoint of all types of frauds.
- Social engineering is a key skill of the criminals involved mainly in frauds, as for example in the increasing number of registered cases of CEO frauds.
- Document forgery is a frequent and necessary technique for Internet fraudsters to deceive victims.
- Even if it remains a practice of the OCGs in the region, the traditional skimming is replaced more and more with massive and complex cyber-attacks. OCGs turn to cashing out in these areas with delayed EMV implementation.
- The skimmers are becoming smaller and more sophisticated.
- Cyber-criminals in the region may exploit hardware and software vulnerabilities to initiate a contact with the ATM, as Blackbox or ATM malware.
- Alternative payment systems based on contactless technology, wearables, augmented reality are expected to sustain the growth of non-cash payments, bringing along new form of crimes.
- The most prioritized cyber-enabled crimes are those related to child online sexual exploitation. The online environment *e.g. files hosting sites,*

cyberlockers, social media, chat rooms and forums, offers opportunities for sexual offenders to find new victims.

- The Internet is used by criminals also to blackmail or disparage people by taking over their social media accounts and/or by publishing photos/videos with compromising content.
- The challenges for LEA in the field of cybercrime investigations are enormous since the cybercriminals and evidence may be located anywhere.
- A dangerous type of cybercrime has emerged, the cybercrime initiated to support traditional crime (e.g. drug trafficking), which can only pose new threats.

4.3. OCTA SEE strategic recommendations

The today cyber-related challenges can be faced with clear strategies and directions empowered by recommendations. The experts of OCTA SEE 2018 are proposing a set recommendations developed within 7 strategic pillars, as depicted in Fig. 4.

All the strategic direction may easily be transposed into national strategies.

OCTA SEE 2018 calls for 5 (five) key priorities, as follows: Terrorism, Cybercrime, Drug trafficking, Trade and industry crime, Trafficking in human beings and smuggling of migrants. A special focus is on money laundering and the adaptability of the criminals to technology and the Internet.

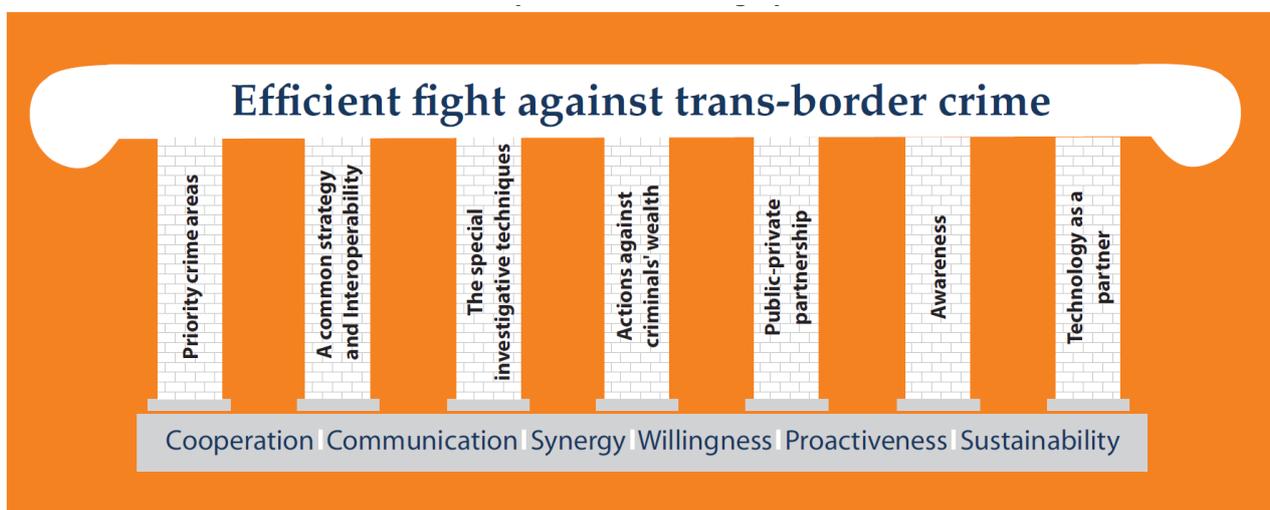


Fig. 4. Strategic pillars OCTA SEE 2018

LEAs must prioritize the resources on countering the emerging crimes with the highest impact on society's safety. A common strategy is the core for an effective fight against cybercrime. Working in partnership, exchanging information on perpetrators, patterns and criminal profiles, setting joint investigations, organizing regional operations in a coordinated manner will adapt the actions and increase the efficiency of the efforts deposited by the Member States, through a tailored approach to the particularities of the region in a resource-oriented approach.

To respond to cybercrime in a proactive manner, LEA has to adapt their investigative means and apply the latest special investigative techniques such as online operations to elucidate the latest multifaceted cyber investigations.

Clear actions against cybercriminals' wealth by cutting off the money flows and the profit will lessen their power and increase LEA's overall capacity.

A more innovative approach is required and LEA must be equipped with the latest technologies. Hands-on trainings on the latest technologies (*e.g. Darknet, cryptocurrency*) developed for the field officers from all the crime areas will provide greater awareness of less visible actions of criminals, as well as teaching law enforcement how to go deeper into crime and discover hidden parts of crime.

In addition to current efforts of the Member States, we must search for coordinated actions requesting governments, experts, the private sector, and civil society to work together by promoting joint international efforts in the same direction.

Public is exposed to cybercrime, therefore a clear strategy on prevention, including awareness companies about the risks and the impact should be settled.

5. Conclusions

Along with the benefits, the Internet offers plenty of opportunities for cybercriminals, causing serious harm to victims that can be located anywhere around the world, as long as they are connected and have valuable information.

Cybercrime is now a very diverse crime with the potential to become the crime with the highest impact at global level, while the Internet may become the most dangerous weapon used in the hand of the criminals.

Therefore, international law enforcement cooperation is a sine qua non condition for an effective and coordinated fight against cybercrime.

A successful story is SELEC, a law enforcement international organization that goes beyond the traditional cooperation and brings in the same place different LEAs from Southeast Europe.

SELEC's core business is to support the operational activities of its Member States by providing a secured platform for real-time exchange of information and by developing joint investigations.

The good examples in cybercrime cases show the organization's resources and capacity to be a useful operational cyber-related instrument for its Member States and partners in the region.

More, SELEC has a deep strategic input at regional level, as its assessment can easily set up regional strategic priorities and approaches.

References

- [1] SELEC, "Organized Crime Threat Assessment for Southeast Europe 2018" [Online]. Available: www.selec.org [Accessed: May 20, 2019].
- [2] SELEC, "Annual Report 2018" [Online]. Available: www.selec.org [Accessed: May 20, 2019].
- [3] SELEC, "Annual Report 2017" [Online]. Available: www.selec.org [Accessed: May 20, 2019].
- [4] www.selec.org [Online]. [Accessed: May 20, 2019].



HUMAN LAYER



HUMAN LAYER

People and Machines: Dealing with Human Factor in Cyber Security

Ana BADEA-MIHALCEA
National Cyberint Center, Romania
cnc@cyberint.ro

“Only amateurs attack machines; professionals target people”
Bruce Schneier, 2000

1. Introduction

In the last years, ensuring cyber security has been a difficult challenge for public and private entities, as well as managing the confluence between technology and the human layer. The reason is the paradox to where organizations are frequently driven, as these entities invest in high technology acquisition without focusing to solve the main issue represented by people, the weakest link. And this issue should be analysed from two different perspectives: the human factor vulnerabilities and the lack of cyber security specialists. Indeed, people are considered to be an easy target for hackers who have adapted their attack techniques and are using social engineering. In the same time, as statistics show, the cyber security workforce is currently affected by a significant shortage of specialists worldwide. Not solving the two human-related issues can generate higher risks for national or even international security. Furthermore, there is a question to which not only specialists but also the research community in cyber security is trying to answer: is the world capable to generate enough skilled experts in order to protect its systems and defeat increasing cyber-attackers? Before trying to find a solution for solving the workforce gap, people should understand the source of the problem and determine the challenges that each institution should overcome. This article aims to discuss the role and function of cooperation in cyber security, having education as the main focus, and analyse the best approaches that can be applied nationally.

2. Understanding the current situation of Cyber Security

In order to understand the current context of cyber security at a world-wide level, some important topics should be analysed first: lack of awareness, rethinking education and the skills set to have by cyber specialists. A study conducted by ENISA [2] shows that cyber threats have undergone significant evolution in terms of impact, like ransom activities and user information stealing. Data breaches have shown enormous growth with hundreds of millions of items of user data flooding the internet and security incidents involving IoT and large volume DDoS attacks complement the threat landscape.

Workforce gap and lack of awareness in cyber security are the main reasons for which the educational system must be adapted to the actual context and a more “rethinking education” approach should be adopted by all public and private institutions involved. Traditional teaching methods should be updated accordingly to the IT industry requirements because students need to be trained in an environment where they can acquire practical skills [6]. This goal can be achieved by providing hands-on laboratory training to students so they can simulate real-life scenarios and see how they react to different threatening situations, like a cyber-attack. Therefore, a hands-on curriculum is likely to produce the most effective results in training cyber security professionals.

Furthermore, public-private partnerships can be used when talking about constructive techniques in education. Private companies and governmental authorities - the future employers of university students - can cooperate with universities on creating together practical educational programs with the use of advanced technology developments, such as cloud computing, artificial intelligence, 5G, etc. According to cyber security studies [4], as professionals gain on-the-job cyber security work experience, organizations can help close the gap by providing more training opportunities - and focusing on the types of training that those already in the cyber security field find the most helpful.

3. Human Layer

As recent studies show, the progression of automation and major technology development have led to the idea of possible job losses and that not only the quality but also the quantity of the workforce is going to be affected. Smart automation, as it is called by specialists, will essentially transform our way of living and working as artificial intelligence (AI), machine learning (ML), robotics and other advanced technologies are gaining remarkable levels of development. In other words, it can be perceived as a digital transformation which is no longer a matter of future, it is actually happening now. Therefore, organizations, industries and each individual should line up with the digital evolution and integrate it into their business strategy or daily lives.

Despite the positive side and all the benefits, the evolution of technology is coming with, there is still one question left to be answered - what about human workers and how will they be affected? It is a fact that there is more concern than excitement surrounding the emergence of digital technologies, as studies show [1], considering that people are roughly twice as likely to express worry (72%) than enthusiasm (33%) about a future in which robots and computers can perform many of the jobs that are currently done by humans. According to a PwC report [8] regarding the type of industries affected by the evolution of digital technology, over half of these potential job losses are in four key industry sectors: wholesale and retail trade, manufacturing, administrative and support services, and transport and storage.

The potential impact of job automation also varies according to the characteristics of the workers, for e.g. those with lower levels of education are at greater risk of job automation. However, besides the potential job losses generated by automation, people should see the advantages that come with the new technologies, like AI and robotics, and integrate them in their daily lives. The good side is that brand new jobs and working sectors will be created so that education can be used as a tool for learning and gaining a new set of skills. It is all about ascending to another level of knowledge and functioning.

3.1. Human factor vulnerabilities

Besides focusing only on technology development, researchers in cyber security warn that the human factor should be considered when combating cyber threats. Sometimes, the human factor represents the weakest link when ensuring the network security and this is due to lack of basic cyber hygiene knowledge. Cyber threats have a psychological side, besides the technical one, which is highly exploited by hackers who constantly seek to identify human errors in order to gather sensitive and private data. Therefore, we can also talk about an insider threat - the authorised personnel who, by mistake, leave a back door open for security threats.

A case study on how social engineering can be used to extract confidential data is the breach against eBay, the e-commerce website, in 2014. An investigation later determined that a group of attackers leveraged phishing attacks to steal the credentials of as many as 100 eBay employees. They used that information to gain access to eBay's internal network, where they then exfiltrated the names, passwords, email addresses, physical addresses, and other personal information of 145 million customers. Social engineering relies on human error, rather than vulnerabilities in software and operating systems. The solution for fighting against this type of cyber threats is exactly the root cause of the problem - human behaviour. Firstly, the entire workforce within an organisation should be trained and educated accordingly in cyber hygiene. Secondly, researchers and experts in cyber security should study hackers' behaviour in order to understand them better so that their next moves to be anticipated and prevented. The board of the company might be in charge, but the whole staff should be aware that they are individually responsible for the infrastructures security.

According to an ENISA study [3], most successful attacks leverage well-known security problems. Reporting from the UK Government's CESG (the part of GCHQ tasked with protecting the nation) indicates that around 80% of cyber-attacks are the result of poor cyber habits within the victim organisations. To address this, a cyber-hygiene strategy should be implemented which emphasises the importance of carrying out regular, low impact security measures. This will minimise the risks of becoming a victim of a cyber-attack or spreading the impact of a cyber-attack to other organisations.

Cyber hygiene is a fundamental principle relating to information security and, as the analogy with personal hygiene shows, is the equivalent of establishing simple routine measures to minimise the risks from cyber threats.

3.2. Lack of specialists - Exactly, how big is the problem?

It is a certain fact that there is a real need to create and expand the mass of cyber specialists to satisfy the increasing demand for workforce required by public and private institutions. Cyber security workforce studies [4] have shown that despite increases in tech spending, this imbalance between supply and demand of skilled professionals continues to leave companies vulnerable. It's no surprise that research shows the shortage of cyber security professionals is now the first job concern among those who already work in the field. According to (ISC)² research, the shortage of cyber security professionals is close to three million globally, including the openings that are currently available, along with an estimation of future staffing needs. This number may seem abstract, but it's having a real-world impact on companies and on the people who are responsible for their cyber security.

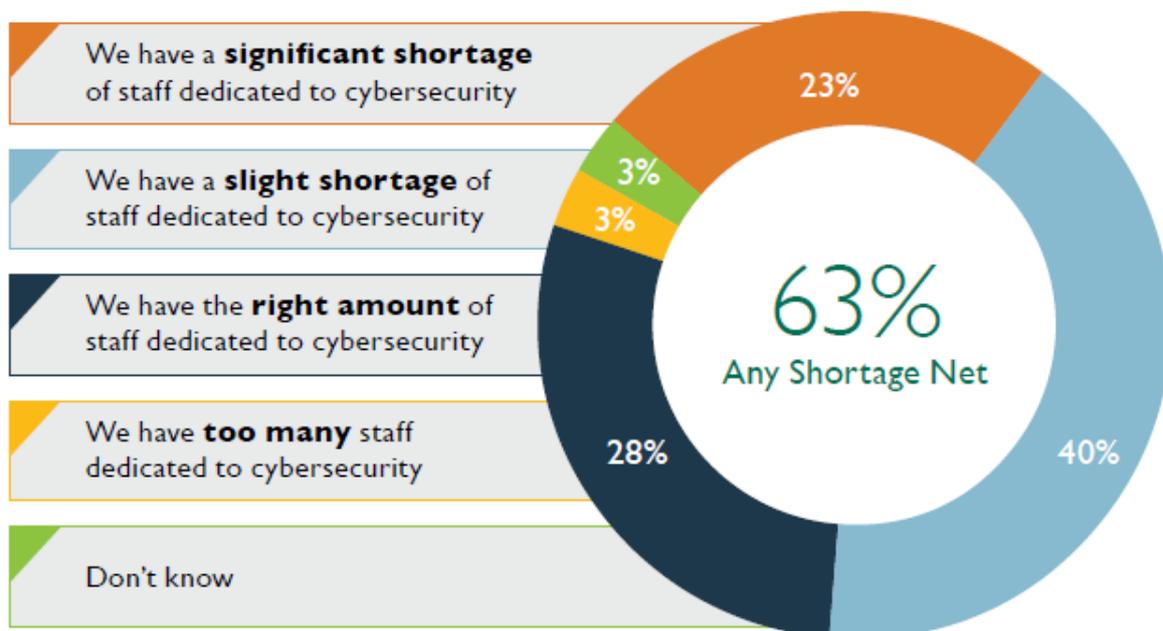


Fig. 1. Current cyber security Staffing & Level of Risk Caused by Staff Shortage [4]

Moreover, 63% of respondents report that their organizations have a shortage of IT staff dedicated to cyber security. And nearly 60% say their companies are at

moderate or extreme risk of cyber security attacks due to this shortage. Workers cite a variety of reasons why there are too few information security workers, and these reasons vary regionally, however, globally the most common reason for the worker shortage is a lack of qualified personnel [4].

The impact can be noticed at a wider level [9] and this is because the continued cyber security skills shortage creates tangible risks to organizations, the individuals and the nation. Consequently, the responsibility for safer cyberspace and society lies with both the government, the organizations and ultimately with the individuals themselves.

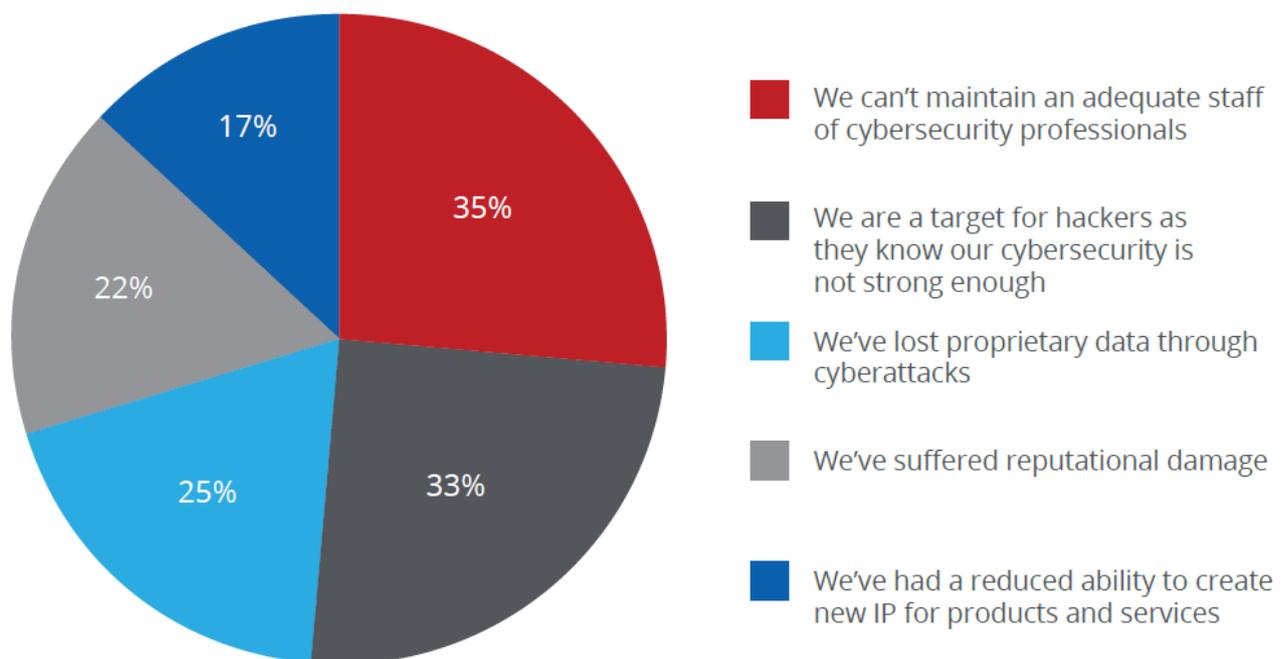


Fig. 2. Impact of cyber security workforce shortage [5]

A country with a weak cyber security workforce is exposed to cyber espionage, remote interference with government elections and ultimately to the safe and reliable running of critical infrastructure services such as healthcare, transportation, power generation, distribution and much more. For a private organization, not having skilled employees certainly impacts on its ability to identify, contain and mitigate complex security incidents, which results in increased cost to the enterprise. And finally for the individuals, lack of security awareness brings about issues of personal privacy, financial fraud and abuses of personal data.

3.3. The role of education in cyber security

When talking about education in cyber security, several different perspectives should be considered. Firstly, education has always been the main tool in creating a mass of professionals, whether we refer to education in an academic environment (schools and universities) or to training and courses which can be attended for specialization in a certain domain. Secondly, public and private institutions should see education as a tool for training their personnel in order to achieve a higher degree of knowledge or a new set of skills in a given field. Last but not least, education plays a critical part in cultivating a culture of secure behaviour amongst internet users.

In order to solve the main problem in cyber security - lack of specialists and skills gap - academia can be used as a starting point for creating a mass of cyber specialists and support universities accordingly. Unfortunately, cyber security as an academic discipline is not as accessible to students as it should. Only 7% of top universities in the countries researched offer an undergraduate major or minors in cyber security [5]. As for graduate work, about a third of top universities offer a master's degree in some cyber security field.

The reasons for not introducing cyber security programs and professional certifications into academic curriculum vary: from sourcing for staff capable of delivering practical learning experience required by the industry, to the laborious accreditation process in order to prepare a course study to be ready delivered to students. A secure cyber security environment requires a skilled workforce and an ongoing learning process, yet currently there are not enough cyber security professionals to properly defend computer networks. Therefore, universities should explore a more untraditional approach, like a public-private partnership, and work with the IT industry and governmental authorities to tailor the right curriculum, deliver hands-on experience and know-how in order to provide students with strong and practical skills. In turn, the government should have a more extensive approach towards education by encouraging cyber exercises and accelerating cyber security studies in universities.

4. Dealing with human layer in cyber security: Romania as a case study

When finding solutions for solving the human layer issues in cyber security, each public and private organization, and even governments, should adopt a multi-layered approach focused on two directions: creating a mass of cyber specialists and educating the already existing personnel. In order to achieve these two goals and generate both near-term as well as long-term solutions to growing the cyber security workforce, cooperation and private-public partnerships are the main keys.

In Romania, the situation has been different until recently: cyber security could not have been studied in schools since computer science was the only subject. This situation was quite alarming since some minimal cyber hygiene elements are absolutely mandatory for every internet user, especially for young ones. According to a national study [7], over 90% of children, between 9 and 18 years old, were using social networks and 33% of them were not protecting their real-life identity, while 47% of children had online conversations with strangers and 27% met each other in real life.

The lack of highly qualified workforce in cyber security is an issue worldwide from which, unfortunately, Romania makes no exception. In order to better respond to the national demand of workforce in cyber security, it is absolutely necessary to expand educational programs and line them up with technology evolution and industry requirements. Therefore, the Romanian Intelligence Service, through the National Cyberint Center, together with the Ministry of Education and the IT industry, has already initiated important steps for developing educational programs in cyber security: postgraduate studies and master studies were implemented in universities with technical background, as long as cyber-security modules for middle-level high-school (10th and 11th grades). The achievements attained in 2018 represented a step forward towards better education in cyber security. By the end of the year, the postgraduate courses in cyber were already being started in 20 universities across the country, to result the first postgraduate students with diplomas in cyber security.

Another essential step was made by creating postgraduate curricula in cyber security, containing a wide range of subjects for master and postgraduate studies, in order for students to obtain professional performance as well as decreasing timing in

career integration. Additionally, several important steps were made for delivering high-quality educational courses with a practical side: on one hand there were created laboratories and centers of excellence in cyber security with European and Norwegian funding programmes, on the other hand professional expertise was delivered by cyber security experts during these courses with the support provided both by the National Cyberint Center and private companies.

Based on the success of the postgraduate programs and welcoming the legislative changes in cyber security on a national and international level - the implementation of Directive on Security of Network and Information Systems (NIS) and the EU General Data Protection Regulation (GDPR) - the initiatives in education have been extended to including data analysis as an academic subject in the postgraduate and master studies. This measure is expected to result in a wider range of IT specialists: cyber data analysts and cyber data engineers. Similar action has been started at pre-university level with a pilot cyber program initiated in several national high-schools with IT background. Thus, four high-schools specializing in computer science from Bucharest, Iași, Cluj-Napoca and Timișoara were chosen to integrate elements of cyber security and cyber hygiene based on curricula specially tailored for high-school level. This pioneering program was initiated by the National Cyberint Center with the support of the Ministry of Education. Another aspect of this educational strategy is that early exposure to cyber security is essential for teenagers to develop interest and acknowledgment in this domain. In this way, they will know not only by what means to protect themselves on the internet, but why and how to choose a career in cyber security.

The National Cyberint Center, together with its partners (National CERT, ANSSI), have encouraged young talented people and supported them with professional training, to participate in the European Cyber Security Challenge. The contest is an initiative of the European Union Agency for Network and Information Security where junior (ages between 16-20) and senior (ages between 21-25) participants have to solve a scenario with the aim of developing and protecting their team infrastructure, as well as attacking the others. With professional training provided to the national team by Cyberint specialists, Romania has been the vice-champion two consecutive years.

However, not only teenagers should be engaged in such activities, but also professionals who actually work in cyber security industry. For example, by participating in cyber security exercises that simulate a real cyber-attack an organization can understand its level of defence when it comes to protecting internal infrastructures. In Romania, CyDex is the only hands-on exercise developed at a national level which contains real-life scenarios by being played in a cyber range. The main objective of the exercise is to check the cyber defence capacities against cyber-attacks targeting IT&C infrastructures with critical valances for national security. The approach endeavours Romanian Intelligence Service to create an efficient alerting and reacting mechanism in order to respond to cyber incidents and also for developing cooperation between the private and public sector in the cyber security field.

5. Conclusion

The topic of cyber security and its implications on human layer is a vast one, with numerous questions and issues to be discussed not only by specialists but also by the research community. On one side we have the pros and cons of the automation era and the fear of human being replaced by machine, on the other side we have a big lack of workforce in cyber security. So, the question is how to work out through this paradox?

As discussed in this article, most educational systems do not offer programs to prepare their students for a career in cyber security. Moreover, cyber education should start at an early age and focus on hands-on experience. Therefore, cyber security and automation need the support and intervention of government so that the entire society to benefit from the advantage of high technology through education and awareness. In order to achieve this goal, there can be established partnerships with educational institutions for developing specialised courses and trainings for people to attain in this increasingly automated world.

In Romania, such kind of educational strategy in cyber security has already been implemented nationally with the support of governmental institutions and the IT industry. All the cyber programs initiated by the National Cyberint Center, along with

the proactive approach towards the development of the Romanian educational system, are going to contribute to solving the human layer issue: creating a mass of highly skilled specialists capable of responding to all the cyber security challenges. The results of these joint efforts will be rising the national level of cyber security and, consequently, of international resilience in cooperation with partners.

References

- [1] Aaron Smith and Monica Anderson, "Automation in Everyday Life", Pew Research Center, October 4, 2017, [Online]. Available: <https://www.pewinternet.org/2017/10/04/automation-in-everyday-life/>. [Accessed: May 7, 2019].
- [2] ENISA, The EU Cybersecurity Agency, "ENISA Programming document 2018-2020", November 2017, page 15, [Online]. Available: <https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020>. [Accessed: May 6, 2019].
- [3] ENISA, The EU Cybersecurity Agency, "Review of Cyber Hygiene practices", December 2016, page 6, [Online]. Available: <https://www.enisa.europa.eu/publications/cyber-hygiene>. [Accessed: May 7, 2019].
- [4] International Information System Security Certification Consortium (ISC)², "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens", Cybersecurity Workforce Study, 2018, page 3-9, [Online]. Available: <https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx>. [Accessed: May 7, 2019].
- [5] McAfee Report, "Hacking the Skills Shortage", 2017, page 7-10, [Online]. Available: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf>. [Accessed: May 7, 2019].
- [6] Nancy Martin and Belle Woodward, "Building a Cybersecurity Workforce with Remote Labs", Information Systems Education Journal (ISEDJ), no. 11 (2) April 2013, page 58, [Online]. Available: <https://files.eric.ed.gov/fulltext/EJ1144996.pdf>. [Accessed: May 7, 2019].

- [7] Organizația Salvați Copiii, "Studiu privind utilizarea internetului în familie", Cercetare socială de tip cantitativ, București 2015, (NGO Save the children, "Study regarding the use of internet within family", a quantity social research, Bucharest 2015), [Online]. Available: https://oradenet.salvaticopiii.ro/docs/raport_cercetare_safer_internet_2015_web.pdf. [Accessed: May 7, 2019].
- [8] Richard Berriman and John Hawksworth, "Will robots steal our jobs?", UK Economic Outlook, PricewaterhouseCoopers LLP, March 2017, page 34, [Online]. Available: <https://www.pwc.co.uk/economic-services/ukey/pwcukey-section-4-automation-march-2017-v2.pdf>. [Accessed May 7, 2019].
- [9] Silensec, "Addressing the Cyber Security Skills Gap", A Reading for Policy Makers, Employers and Young Professionals, page 5, [Online]. Available: https://www.silensec.com/downloads-menu/whitepapers/item/download/10_d3d9446802a44259755d38e6d163e820. [Accessed: May 7, 2019].

The Importance of Human Resources

Iulian ALECU

Romanian National Computer Security Incident Response Team (CERT-RO)

iulian.alecu@cert.ro

Every day is a new beginning, both personally and professionally. It represents starting or continuing a journey with priorities and objectives, with expectations and hopes, with joy and disappointment, with achievement and effort, a journey made to accomplish what we set out to do in the short, medium or long term.

Each person's journey intertwines across different periods, in different ways and with varying intensities, with other people's, with their goals, hopes and expectations. Effectively, there is a sense of mankind's pursuit of something better, where that "something" has different meanings for each of us.



Photo source: *Aledo ISD*

We could continue to expand upon this and would surely find interesting hypotheses on how each individual journey could be improved, become more efficient, more worthwhile. In our case, however, we will focus on the impact that this dynamic has on a state institution that handles cybersecurity on a national level.

Being made up of people, such an institution has its own trajectory, its own dynamic. The people who work there contribute to its journey.

We are dealing with the following components of the institutional dynamic: its (human-established) goals, the way in which they are attained (the process of institutional growth), and the engine driving said growth, the human resource.

Moreover, this human resource is, or should be, in constant flux: you cannot keep any single person in the same place forever, life accelerates, expectations shift, and so do goals. Yet the institution must continue onward to the desired objectives.

We find ourselves in the situation where the personal dynamic meshes with the institutional one, in the short or the long term, which should, ideally, develop into “something better” for both parties.

This is where the problems start:

1. An institution is not always properly adapted to the reality of human existence in which it finds itself.
2. The people who (wish to join or) work for that institution cannot always adjust to the needs, goals, expectations and challenges of both it and their world.
3. Certainly, the institution does not “exist” beyond the living, breathing people that make up its various levels of activity and decision-making; and yet, what one group of people creates within it - objectives, atmosphere, work ethic, mentality - goes on to represent the institution for those who come after them.

Thus, we find ourselves discussing two standalone realities, even though they have a single common denominator, the **human being**.

On one hand, it all comes down to the manner in which organizational development, policies, and objectives are determined, while on the other, the deciding factor is the way in which humans cope with the aforementioned objectives, policies and work ethic, all while striving to improve them.

There is a crucial need for people to have the vision and the capability to decide strategic objectives, while at the same time to be able to work efficiently in order to reach them.

The fact that this institution is not an isolated entity, but an organic component of national and international systems, whose “lives” constantly influence its journey, must also be taken into account.

Likewise, its objectives within the realm of cybersecurity must provide an efficient answer to threats and risks caused by other people and institutions who, in turn, lead their own journeys of personal and professional fulfillment.



Photo source: *OEC Strategic Solutions*

People have vision, set objectives, determine the course of personal and professional progress (preferably at the same time).

People, who are increasingly harder to find, to motivate, to please.

People, deploring the fact that they are unable to find others who match their (and the institution's) expectations.

What can be done about this?

Ironically, these very **people** must determine a course of action that allows their (personal and professional) journeys to converge with others in their effort to build something better.

People must properly know themselves in order to understand what they truly want, to find their way towards their new values, their new expectations and goals, their new selves.

People must know themselves and be prepared to achieve their desires.

Upon further scrutiny, we require a bit of managerial vision: we should invest resources now - and this is a continuous now - in order to understand and adapt to what modern people need, rather than fruitlessly waste time and resources in the conviction that we cannot change this status quo.

This must be a joint effort - state, private and academic - because each of these holds pieces the other two do not possess, but when combined can provide a realistic image of how **people** can be understood, approached, trained and motivated so that they can support the achievement of goals these same **people** have set for cybersecurity.

About the Real Value of Knowledge, Intellectual Capital and Resilience in the New Cognition Economy

Călin M. RANGU

Financial Supervision Authority, Romania
calin.rangu@asfromania.ro

1. Summary

The society in which we live is defined as a knowledge society, and the economy is a **post-knowledge economy** which is a mixture of knowledge and networks. In **Intellectual Capital (IC)** terms this means that **Structural Capital (SC)** derived from **Human Capital (HC)** and **Relational or Strategic Alliance Capital (SAC)** are becoming the key aspects.

People **possess IC based on knowledge** like intangible, explicit or tacit assets. **They hold some values**, informally recognized, but often formally ignored. **Cyber-attacks target exactly these values.**

The word “**knowledge**” **has many valences**. One being targeted by cybercrime (money, identities, intellectual property, etc.).

One of the main problems is that knowledge does not provide you with skills, and knowledge-skills fracture leaves free attacks, fraudulent practices, astronomical losses brought by cybercrime.

Accounting standards remain a tribute to classical principles not adapted to the reality of the knowledge society. For this reason, the value of the assets lost as a result of cyber losses is difficult to quantified. This is partially caused because companies have inventory of their tangible assets whilst most cyber-crime focusses on intangible assets which rarely have inventory. This can partially be dealt with by using enabling technologies such as machine learning, Artificial Intelligence and robotics. This is best seen in the extremely low level of cyber risk insurance. We should take policies, strategies to cover this gap.

At human level it is necessary to shift from the accumulation of knowledge to the development of skills, to cognition.

At the accounting level it is necessary to create the system of evaluation and registration of intangible assets of knowledge and networks, human, structural and relational capital.

2. About cyber risk and (un)known or (un)covered assets

If we are looking technically, cyber-attacks lead to disruption of activities/business, by freezing **public or private infrastructures, productive, financial infrastructures**, etc. affecting people and property, through **compromising the confidentiality, availability or integrity of the data or services**¹. But that's the effect. The cause is human, we are talking about people and their assets that are affected, people who are assuming responsibilities and taking actions, or those who disregard them with good science or ignorance. In the same time fellows orchestrate and attack.

According to the thematic analysis of the Romanian Financial Supervisory Authority (A.S.F.) on cyber risk insurance², **the management of institutions and companies in the same time with employees are responsible for**, the role of people being essential.

Institutions or companies need **a comprehensive cyber-risk management strategy** to return to normal operations as quickly as possible with the lowest cost. People need to develop skills in addition to the necessary technical education to provide them with basic knowledge. This knowledge, the experience gained must be monetized. Education should not be found only at the expense cap, but also to intangible assets accumulated in the wake of education, to implement structures, procedures, knowledge-based mechanisms.

When talking about **risks** we are talking about **threats (external**, from those who have interest, knowledge and skills) on the one hand, and **vulnerabilities** on the

¹ L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019

² https://asfromania.ro/files/analize/Asigurari_risc_cibernetice.pdf [Accessed May. 09, 2019]

other side (those who have intangible values of data type, information, monetary or identity value) who do not know, do not can, or do not have skills, cognition and no defense capabilities. All gains obtained by attacking intangible assets are also unlawful acquisition by affecting the image of companies or people, leaking information, disruptions of activities. **If someone is gaining, where is the loss recorded**, where are those assets that disappear, where we will see it in accounting? The fact is that they are not found in accounting as a direct losses, as assets destroyed. Maybe the goodwill will be affected. It creates problems in sizing the real loss. There are default problems in securing that loss. An insurer cannot ensure that even the owner of the active needle does not evaluate it prior to the risk of the damage to the product.

Threats may be **intentional** (criminal, terrorist, hostile, activism, blackmail or personal reasons), or represent **accidental events** (data deletions, service interruptions).

Estimating the cost of cyber incidents is a challenge, companies avoiding reporting losses, whether they can't calculate them, or they don't want their image to be affected (another intangible asset of intellectual capital). The **damage caused by cyber risks** is estimated at around 0.5% of the world's GDP and almost twice as much as the annual average of losses caused by natural disasters³.

On the basis of a risk barometer, conducted by interviews on 968 participants, the main causes of the losses generated by cyber incidents were established in the year 2019 (Fig. 1):⁴ 1. Business Interruption; 2. Loss of reputation; 3. Damage caused by data loss; 4. Data restoration costs; 5. Fines and penalties.

Vulnerabilities can be covered with internal resources or by outsourcing the risk. The **residual risk**, which costs too much to be covered internally can be taken over by the insurance system. But this also leads to lack of knowledge and cognition in order to retrieve it. The cyber-risk coverage of only 2025 will cover 1% of total insurance, according to Swiss Re, while uncoated losses are huge.

³ L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019

⁴ Allianz Global Corporate & Specialty, „Allianz Risk Barometer” 2019



Fig. 1. The main causes of economic losses caused by cyber incidents
(Source: Allianz Risk Barometer, 2019)

According to L. Badea (2019) "The amount of financial losses generated by cyber risk is difficult to estimate, with a shortage of information. **Some cyber-criminality activities do not have a direct cost or cannot be quantified.** The industry is attempting to estimate the total costs, costs per incident, and the cost of registering a data violation according to Table 1. Fig. 2 present estimates of average annual cybercrime costs by areas and main affected countries"⁵.

Table 1. Estimated cybercrime costs
(Source: Geneva Association, 2016)

GLOBAL COSTS (IN BILLION USD, PER ANNUM)		COSTS PER INCIDENT (IN MILLION USD)		COST PER RECORD (IN USD)		COSTS BY COUNTRY (IN % OF GDP; MCAFEE, 2014)	
Symantec (2013)	113	Ponemon Institute (2015)	3.8	Symantec (2013)	298	U.S.	0.64
McAfee (2014)	445 (375-575)	Geschonnek et al. (2013)	2.1	Ponemon Institute (2015)	217	China	0.63
Kshetri (2010)	100-1'000	Kaspersky Lab (2013)	2.4	NetDiligence (2014)	956	Japan	0.02
						Germany	1.60

According to Accenture, the biggest cyber-crime damage is registered in the field of loss of information stored electronically, followed by business, turnover losses and equipment damage (Fig. 2.):

⁵ Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, Nov 2016

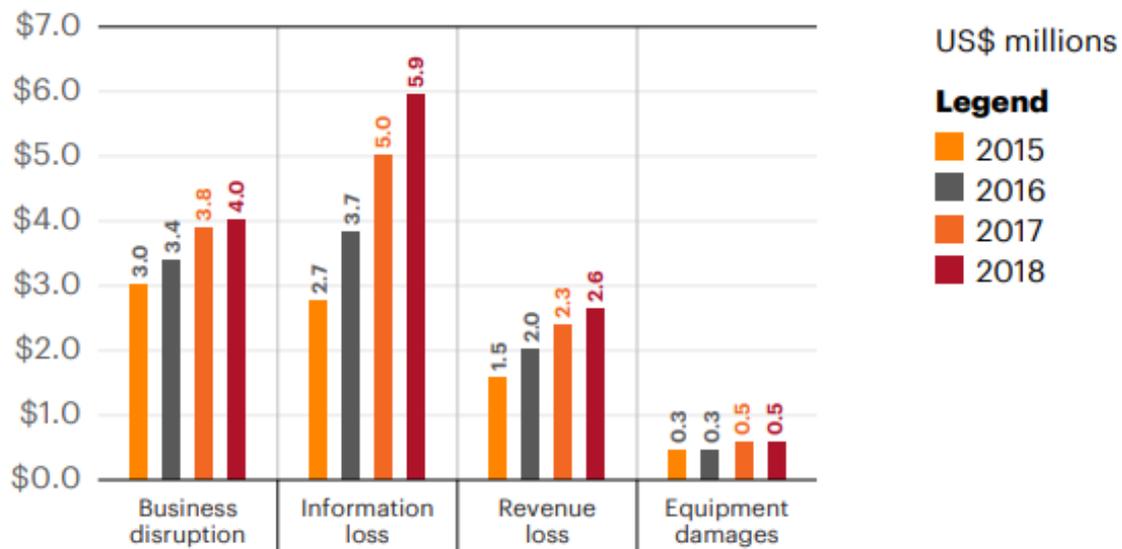


Fig. 2. Average annual cyber Crime costs on the main areas of losses
(Source: Accenture, 2019)

According to L. Badea and C. Rangu (2019), cyber risk insurance can play a key role in taking over/transferring the risks to which companies and people are exposed. "This can be a tool that complements (and does not replace) the risk management framework that each organization should have and should be an element of economic and social stability, both for critical infrastructures, both commercial and personal, including for the financial sector. Cyber risk insurance should be **used in assessing financial soundness/health** and supporting activity through rapid recovery of losses and continued activity". But how to do it is the biggest challenge, in which IC methodologies are essential.

3. About the Intellectual Capital (CI)

According to F. Stibli⁶ "intellectual capital of an organization is divided into four categories: human-centered assets, infrastructural assets, intellectual property assets and market assets". It can be seen that all these assets can be impacted cyberspace and can generate profits to the attackers. Each of them should be evaluated, including

⁶ F. Stibli, Intellectual capital - the key resource for expanding organisational intelligence, <https://intelligence.sri.ro/capitalul-intelectual-resursa-cheie-pentru-extinderea-inteligentei-organizationale/> [Accessed: May. 10, 2019]

monetary to be able to establish the risk picture, and protect them because "knowledge can be converted into value" according to Leif Edvinsson and Sullivan Pat.

Thomas Davenport (Davenport, 1999) builds a model of the employee as an investor in human (educational) capital⁶. He notes that in recent years, the number of highly specialized jobs has increased at all levels of education, to the detriment of unskilled, poorly specialized work, as well as managers on lower levels (major, team leaders etc.). Investing in lifelong learning thus appears as a priority for individuals and insurance against the risks of unemployment and poverty. On the other hand, companies can obtain a higher profit by investing, rather, in the education of their employees, than in increasing the stock of economic capital".

Since 1999⁷ it has been noticed that it would be time to define the concepts of intangible assets, human capital, and knowledge. The International Accounting Standard Committee - International Accounting STANDARD IAS 38 defines **an intangible immobilization as a non-monetary identifiable asset, no physical substance**. According to IAS 38 "intangible assets", an intangible asset is a non-monetary identifiable asset, without material support and held for use in the production process or the supply of goods or services, to be rented to others, or in Administrative purposes. Particularities are represented by the identifiable nature, control over a resource and the existence of future economic benefits.

The intellectual capital (CI) that interests us in this analysis are the **Human capital** (referring to knowledge, skills, motivation, team relationships, briefly all factors in relation to employees who promotes the performance that customers are willing to pay) and the **Structural Capital**, referring to "all that remained when people left the night" (Edvinsson & Malone, 1997, p. 17), such as databases, structure detailed procedures transposed into the software, etc.⁸ The effective management of IC lies in managing the hybrids particularly HC-SC, SC-SAC, SC-CC, HC-SAC and HC-CC.

⁷ 10 June 1999 HOLISTIC MEASUREMENT OF INTELLECTUAL CAPITAL COUNTRY covered: AUSTRIA RESEARCH TEAM: Manfred Bornemann, Karl Franzens University Adolf Knapp, Karl Franzens University

⁸ Edvinsson Malone Intellectual Capital, Realizing your Company's true Value by finding its hidden Brainpower. New York: Harper Business, 1997, p. 17

The **human value** is defined by OECD⁹ as being the knowledge, skills, competences and attributes incorporated into individuals that facilitate the creation of a personal, social and economic goodwill.

Education is not the only or main form of HC development. Experience, insights and networks may be equally important. But Education is important for human capital development. In the company's records we only have the expense of the studies, not the human asset as an additional human value. Man/woman is the only asset that should be continuously appreciated, compared to the other assets that are continuously depreciating. There are researchers such as Ludo Pyis from Areopa which also proposes the **formula for calculating the human value**. When the human asset is evaluated, it will find it placed in the balance sheet/accounting balance of company, then the man will be positioned correctly in the company, in society. But for that, the general ledger and accounting methods have to be updated, and there are specific methodologies.

An example is the **Wissensbilanz** -the declaration on intellectual capital - developed by Fraunhofer Institut¹⁰ which is 'an instrument essential for maintaining the competitive advantage and maintaining their business successfully in the knowledge-based economy.'

A generally recognized classification divides KBC¹¹ into three categories: "Computer information (software and database), innovative properties (patents, copyrights, design, trademarks) and economic skills (including capital Brand, company-specific human capital, people's networks and institutions and organizational knowledge that increase the efficiency of the Enterprise (Corrado, Hulten, and Sichel, 2005)". Thus appears the third important component of intellectual capital, the **relational/customer capital**.

As a summary, the Table 2 define the main categories of IC phenomena.

⁹ Human Capital-The Value of People <https://www.oecd.org/insights/humancapital-thevalueofpeople.htm>

¹⁰ Wissensbilanz, https://www.academy.fraunhofer.de/en/continuing-education/technology-innovation/intellectual_capital_statement.html

¹¹ OECD (2013), "Introduction and Overview", in Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing, <http://dx.doi.org/10.1787/9789264193307-4-en>

Table 2. IC calculation building blocks
(Source: Areopa slides, Guthrie, 2001)

Intellectual Capital Calculation Building Blocks – Elements/Phenomena			
	Human Capital	Customer Capital	Structural Capital (Organizational Capital)
GUTHRIE (2001)	<ul style="list-style-type: none"> • Know-how; • Education; • Vocational qualification; • Work-related knowledge; • Work-related competencies; • Entrepreneurial spirit • Innovativeness, • Proactive and reactive abilities • changeability 	<ul style="list-style-type: none"> • Brands • Customers • Customer loyalty • Company names • Distribution channels • Business Collaborations • Licensing agreements • Favourable contracts • Franchising agreements 	<ul style="list-style-type: none"> • Patents • Copyrights • Trademarks • Management Philosophy • Corporate Culture • Management processes • Information Systems • Networking Systems • Financial Relations

According to AREOPA¹², „apart from Structural Capital, the base IC classes are in fact *shared* capital. For instance, Human Capital (HC) is shared with its ‘owners’: when a staff member decides to leave the organization, he/she takes his/her skills and competences, reputation and potential along. Similar rules apply to both Customer Capital (CC) and Strategic Alliance Capital (SAC): when the customer takes his business elsewhere or an alliance breaks up, the customer’s revenue potential and partnership’s leverage are gone. The consequence of this is that Intellectual Capital may flow from one sector into the next. And this is where management of IC comes into play. It is important for companies to realize where their IC is situated, and which actions need to be taken to convert IC that is at risk of being lost into IC that has become structural, i.e. to structuralize its Human, Customer and Strategic Alliance Capital to the maximum extent possible”.

Their conclusion is that „the knowledge company travels light. ...Not only are the key assets of a knowledge company intangible, it’s not clear who owns them or is responsible for caring for them.”

¹² Ludo Pyse, NO CURE, NO PAY? Would applying this rule bring IT projects failure statistics down? ... and how do we measure sure success?, www.areopa.com

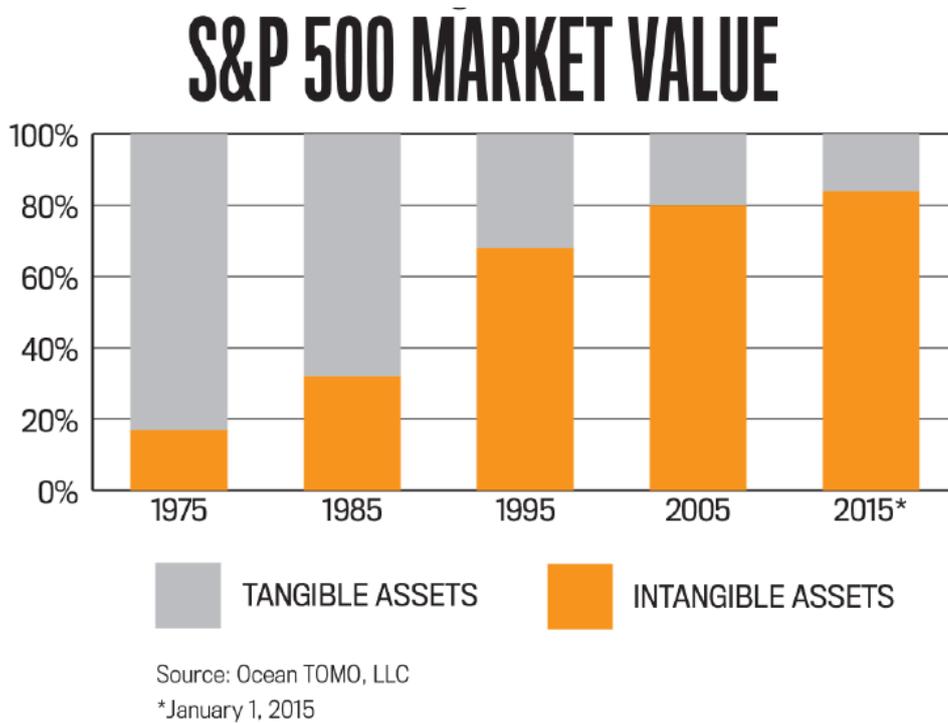


Fig. 3. The evaluation of intangible assets in S&P 500 Market Value
(Source: G. Cokins, 2017)

According to Cokins, G. and Shepherd, N. (2017), figure 3 shows how “hidden value” can be made visible. The left side of the Figure represents the publicly disclosed financial statements prepared according to Generally Accepted Accounting Principles (GAAP) or International Financial Reporting Standards (IFRS). First consider the published balance sheet at the top. Early efforts to understand and quantify the difference between the book value and the adjusted value with added intangible assets can be traced back to the early 1990s and the rise of knowledge management and intellectual capital. More recent and ongoing work in the science of valuing intellectual capital has been undertaken and published by AREOPA, a thought-leading consulting firm specializing in this area”¹³.

Gary Cokins¹⁴ (2017) show clear in fig. 4 that the new world is of the intangible assets and „the traditional balance sheet understates the economic value of a company

¹³ THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, <https://sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/>

¹⁴ THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, <https://sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/>

because it doesn't include a large portion of intangible assets.Forty years ago, more than 80% of the average valuation of companies on the S&P 500 was represented by tangible assets such as property, plant, and equipment—the majority of which were reflected on an organization's balance sheet. - the number is now reversed with more than 80% of an organization's attributed value represented by intangibles such as its intellectual capital, workforce, supply chains, and other key relationships.

HIDDEN VALUE MADE VISIBLE

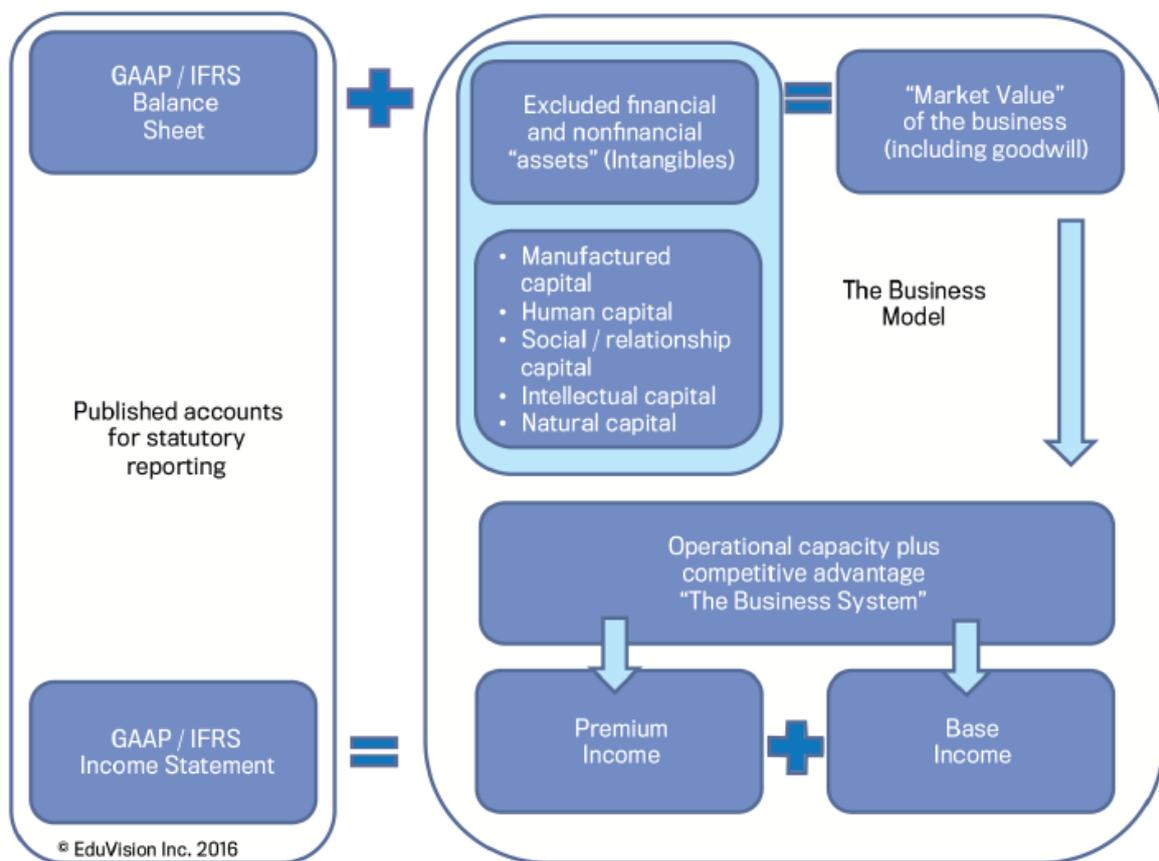


Fig. 4. Hidden Value Made Visible
(Source: G. Cokins, 2017)

From an accounting perspective, this has driven the growth in calculating a goodwill amount as organizations have been bought, sold, and amalgamated, and the excess of the purchase paid over accounting book value has been reported as goodwill. A recent article by Bloomberg quoted a Goldman Sachs Global Investment Research study that showed the continued growth in goodwill in U.S. companies reached \$2.5 trillion dollars overall by 2015. (See <https://bloom.bg/2pIcKNS>.)”

4. Assessment of Intellectual Capital

European Commission mentions in the Intellectual Property Valuation Report¹⁵, in 2013 “the opportunity of, if not need for, leveraging on intangibles, and especially those with a legal recognition, such as brands and IPRs, for favoring innovative and more knowledge-consistent forms of bank financing for company growth and investment processes. This is particularly true for European research-intensive SMEs”.

EU is stressing “the need for developing new segments of financial markets devoted to the valuation, exchange and funding of IPRs and other intangibles, by creating the necessary pre-conditions and infra-structures for such markets to operate in an efficient and effective way on a European scale”¹⁶.

The lack of measurement of intangibles at micro-level (i.e. company) is another recurrent policy priority which underlies many of the above issues. Shared methods for valuation and accounting are a relevant basic issue which may explain the difficulty to see intangibles in company annual financial statements and disclosures. This issue is particularly true for internally generated intangibles; such are - in many cases - the IPRs. As Mr. Hans Hoogervorst, Chairman of the International Accounting Standards Board (IASB), pointed out recently¹⁷ “Intangible assets go unrecorded (or under-recorded) on the balance sheet.... we know that the [accounting] standard [IAS 38] is rudimentary because it is based on historical cost, which may not reflect the true value of the intangible asset”.

A brief analysis of international practices for the development of Intellectual Capital reports¹⁸ can mention by Brooking¹⁹ which fragments in four categories: Human-centered assets; Infrastructural assets; Intellectual property assets; Market assets.

¹⁵ https://ec.europa.eu/research/innovation-union/pdf/KI-01-14-460-EN-N-IP_valuation_Expert_Group.pdf

¹⁶ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=11602&no=1>

¹⁷ <https://magazine.lucubrates.com/intellectual-capital-and-knowledge-management/>

¹⁸ <http://www.incd2020.ro/sites/default/files//Analiza%20bune%20practici%20intl%20rapoarte%20CI.pdf>

¹⁹ Brooking A., 1996. Intellectual Capital: Core Asset for the Third Millennium Enterprise. New York: International Thomson Business Press

Leif Edvinsson has made a standardized model and language for the presentation of the CI. Edvinsson concludes that the result of a decrease in the accounting value of an organization's market value actually signifies the CI existing in that organization, according to the formula: ²⁰

$$\text{Market value} = \text{Financial Capital} + \text{CI}$$

Leif Edvinsson²¹ has decomposed the CI in four distinct areas: Human capital; Customer capital; Process capital; Innovation capital.

L. Pyis²² presents eloquently in Fig. 5 the stages by which the bits pass through the date due to the implementation of a syntax, to information through semantics, to the actual knowledge due to the placement in context, know-how, experience and expertise through use, by practice and an effective approach. We note that at each level the cyber risk is there, the intellectual capital assets are more valuable and interested for both the company and the external factors.

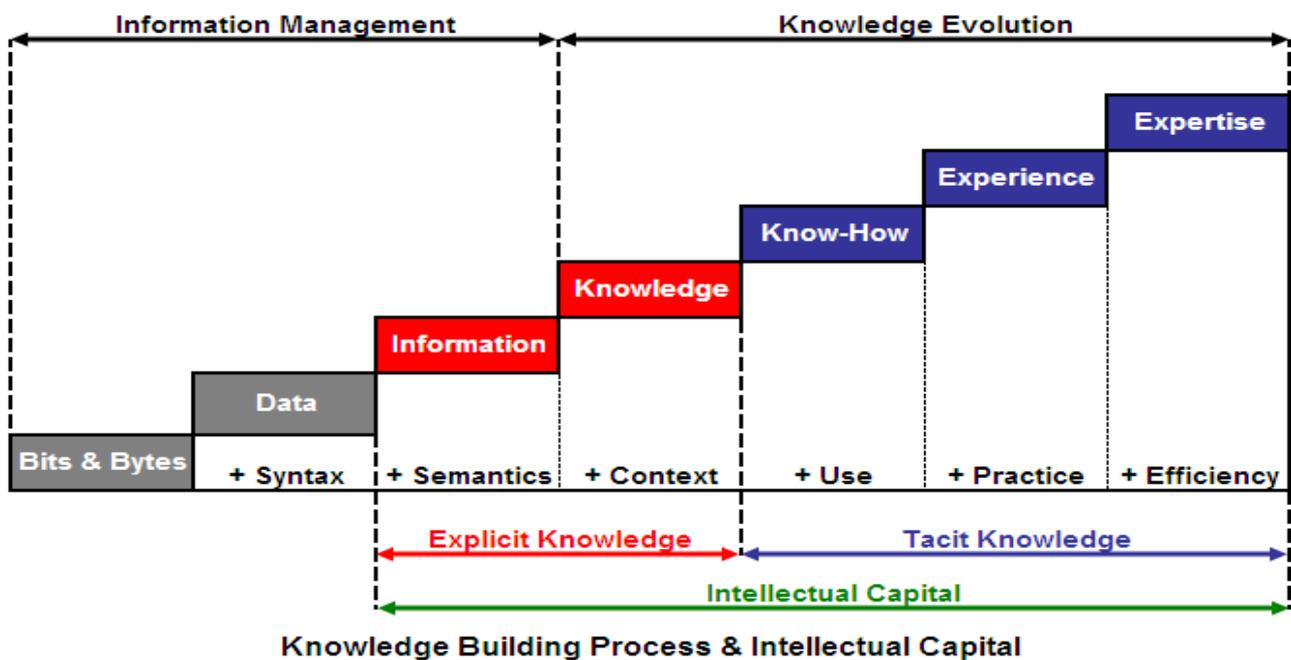


Fig. 5. The IC Building Process
(Source: Areopa, 2015)

²⁰ Leif Edvinsson Intellectual Capital: Realizing Your Company's True Value by Finding Its Hidden Brainpower Hardcover, 1997

²¹ https://www.researchgate.net/profile/Selcuk_Burak_Hasiloglu/publication/28263308/figure/fig1/AS:394353668313091@1471032649090/Edvinssons-Categorization-of-Capital-Resource-Leif-Edvinsson-and-M-S-Malone.png

²² Ludo PYIS, AREOPA GROUP, IS IT WORTH PROTECTING YOUR INTELLECTUAL CAPITAL FOR CYBER INTRUDERS (PPT presentation), 2013

If we analyzed the risks posed by the brainstem they are related to the operational risks of those generated by people, processes and systems.

Intellectual capital deals with: Human Capital Control, Structural Capital Control, Controlling the relational capital and alliances.

IT is the entry into change management and knowledge management, risk management, evaluation, coverage and insurance.

According to AREOPA:

- **Knowledge is critical in** time, virtual, now relevant, reflective, complex, evolving, interactive, untidy, created for a purpose, but based on past, social, often self-organizing experience, carried out by questions, challenges and debates, filter, creative, selective.
- **Knowledge is found in** presentations, reports, journals, licenses, patents, licenses, intellectual property, databases, software, risk instruments, audits, libraries, catalogues, archives, manuals, policy documents, memoirs, individual capacity, memory, know-how, experience, teams, communities, groups, networks.
- **Explicit knowledge** is easily identifiable, re-usable in a consistent and repeatable manner-for decision making and/or for the exercise of judgement, can be stored as a written procedure or as a process in a computer system, stored as artifacts-artificial, physical or virtual entities that can be measured, identified, distributed and audited.
- **Tacit knowledge** are as lessons learned, methodologies, cases, stories, staff, specific context, difficult to formalize and communicate, insights, mental rules, mind sets, unwritten rules, values unconsciousness, the fundamental philosophy.

Karl-Erik Sveiby proposed **a model for the methods to evaluate IC** in accordance with Fig 6, in four categories: market capitalization, return on assets, direct IC, score card methods.

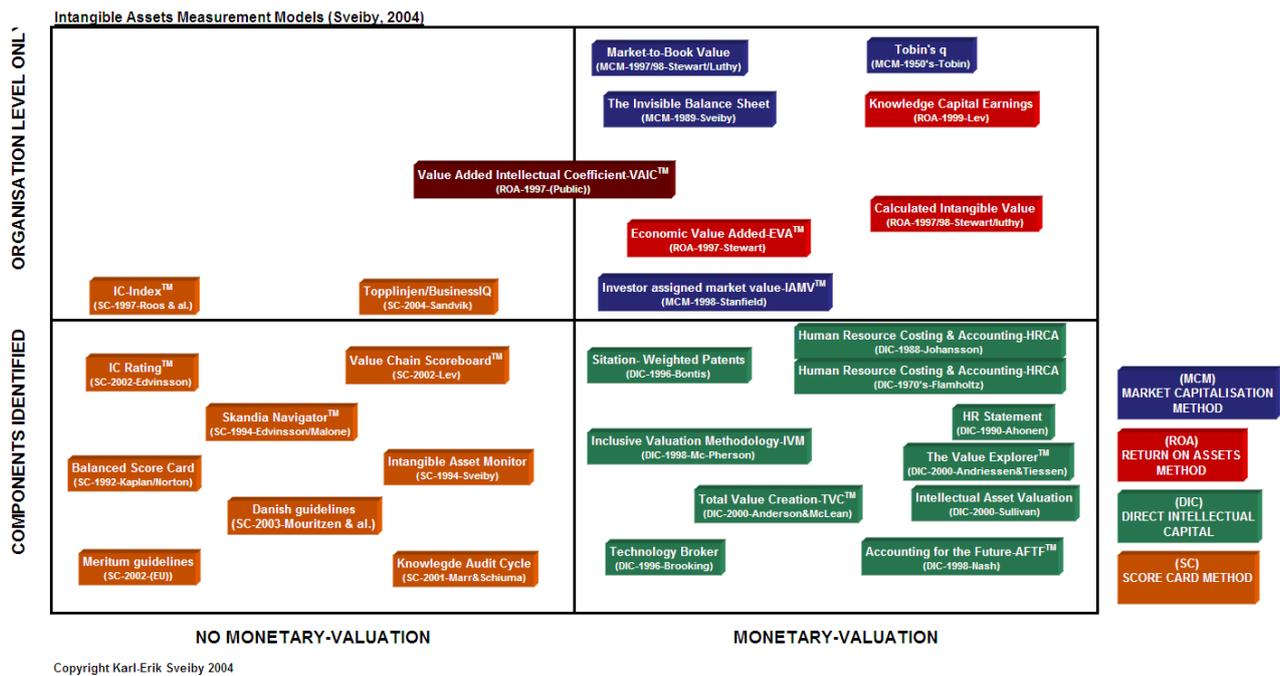


Fig. 6. The model for the methods to evaluate IC (Source: Areopa slide, 2015)

Starting from this approach Areopa proposes a calculation model, from unstructured to the very structured intellectual capital types.

AREOPA has developed such a model for identifying and quantifying intangibles as components of Intellectual Capital (IC). This model serves to evaluate a company's return on all the capital it employs, helping to explain the difference between book and market value. It also provides guidance as to how and where management should put its attention to grow the organization's overall IC.

Starting from the new IAS 38, Lucurbate Peter Walch mention that „accounting for IC does in fact create a supplementary balance sheet also based on the debit and credit system in the same way as financial accounting standards. Thus IC accounting creates a recognition of otherwise not-reported or off-balance sheet assets. The charts below should be studied carefully”²³.

²³ Lucurbate Peter Welch October 12th, 2018 Magazine article No: 42, October 8th, 2018



International Accounting Standards (IAS) IAS 36 Impairment of Assets / IAS 38 Intangible Assets

SUMMARY OF IAS 36

Objective
To ensure that assets are carried at no more than their recoverable amount, and to defir

Scope
IAS 36 applies to all assets except: [IAS 36.2]

- inventories (see IAS 2)
- assets arising from construction contracts (see IAS 11)
- deferred tax assets (see IAS 12)
- assets arising from employee benefits (see IAS 19)
- financial assets (see IAS 39)
- investment property carried at fair value (see IAS 40)
- certain agricultural assets carried at fair value (see IAS 41)
- insurance contract assets (see IFRS 4)
- assets held for sale (see IFRS 5)

Therefore, IAS 36 applies to (among other assets):

- land
- buildings
- machinery and equipment
- investment property carried at cost
- **intangible assets**
- goodwill
- investments in subsidiaries, associates, and joint ventures
- assets carried at revalued amounts under IAS 16 and IAS 38

the three critical attributes of an intangible asset are: [IAS 38.8]

- identifiability
- control (power to obtain benefits from the asset)
- future economic benefits (such as revenues or reduced future costs)

Identifiability: An intangible asset is identifiable when it: [IFRS 38.12]

- is separable (capable of being separated and sold, transferred, license)
- arises from contractual or other legal rights, regardless of whether thos and obligations.

Examples of possible intangible assets include:

- computer software
- patents
- copyrights
- motion picture films
- customer lists
- mortgage servicing rights
- licenses
- import quotas
- franchises
- customer and supplier relationships
- marketing rights

Intangibles can be acquired:

- by separate purchase
- as part of a business combination
- by a government grant
- by exchange of assets
- by self-creation (internal generation)

Fig. 7. Summary of IAS 36
(Source: Welch, 2018)

On the basis of this model Areopa proposed a model of the balance sheet relating to the intellectual capital to be complementary but integrated to the classical one, as defined over 400 years, an example refining in Fig. 8.

		Closing Date		Balance Sheet			
		Assets		Liabilities and Capital			
LIQUIDITY ↑ ↓ LOW	Current Assets:			Current Liabilities:			SHORT ↑ ↓ LONG
	Total Current Assets	0.00		Total Current Liabilities	0.00		
	Fixed Assets:			Long-Term Liabilities:			
	Total Fixed Assets	0.00		Total Long-Term Liabilities	0.00		
	Total Current and Fixed Assets	0.00		Total Liabilities	0.00		
	Other Assets:			Capital:			
	Total Other Assets	0.00		Total Capital	0.00		
	TOTAL ASSETS	0.00		TOTAL LIABILITIES AND CAPITAL	0.00		

		ABC COMPANY		Closing Date		Intellectual Capital Balance Sheet			
		Intellectual Capital Assets		Intellectual Capital Liabilities and Equity					
STRUCTURED ↑ ↓ LOW	Structural Capital:			Intellectual Capital Liabilities:				CAPTURED ↑ ↓ HIGH	
	Technological Capital	0.00		Tact Internal Intellectual Capital Assets	0.00				
	Organisational Capital	0.00		Tact External Intellectual Capital Assets	0.00				
	Total Structural Capital Assets	0.00		Total Intellectual Capital Liabilities	0.00				
	Human Capital:			Intellectual Capital Equity:					
Total Human Capital Assets	0.00		Explicit Internal Intellectual Capital Assets	0.00					
Total Internal Intellectual Capital Assets	0.00		Explicit External Intellectual Capital Assets	0.00					
	Relational Capital:			Total Intellectual Capital Equity	0.00				
	Business Capital	0.00							
	Social Capital	0.00		Total IC LIABILITIES AND EQUITY	0.00				
	Total External Intellectual Capital Assets	0.00							
	TOTAL IC ASSETS	0.00							

Fig. 8. IC Balance Sheet: Follows the structure logic of the FINANCIAL BS
(Source: Welch, 2018)

Accountability should be connected knowledge and network economy, to cyber world, to face the cyber-threats because the real IC is not protected at all, intellectual property (patents, author rights, trademarks etc.) representing only few percent of the IC.

Cyber-attacks escape only the IC that is captured, stored and made reusable through the computer, the explicit knowledge, which is in the form of data, information, know-how, etc. But they can also attack the tacit knowledge, the development plans, which can be found in emails, R&D, at developers, strategic exchanged of top management etc.

5. Building resilience

Mrs. Sabine Lautenschlager, member of the ECB, mentions²⁴ that for the financial market the information, knowledge and expertise of public institutions and industry will be essential because:

- Close interconnection and complexity of the financial system creates vulnerabilities that can be exploited by cyber attackers.
- The attackers seem to gain an ever deeper understanding of how the financial system operates. This allows them to quickly detect and exploit weaknesses in a more efficient way and should be a concern for all of us.
- Both banks and financial market infrastructures strive to find staff with the skills and experience necessary to prevent cyber-attacks. **Lack of skills extends far beyond the financial sector. All relevant stakeholders must urgently work on strategies to ensure that the workforce has the skills needed for our future economies** and that our society is able to seize the advantages of innovation.
- True innovation is always disruptive. Fintech could disrupt financial markets in positive ways. But it also comes with risks: a more violent competition could lead some market players to adopt and adopt new technologies, services

²⁴ https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_1~5803aca48c.en.html

or methods, before taking full advantage of the associated risks-cyber risks in this case.

In March 2017, the governing Council of the IMF endorsed the Eurosystem's cyber resilience strategy. In fact, we are talking about the resilience of these intangible assets, data, information, knowledge, assets, identities, know-how. These assets have immense value. We must be able to inventory, evaluate, measure, appear in the accounting systems, so that we can secure them.

According to L. Badea (2019), **to identify the risk we should evaluate:**

- The **business processes relevant to the cyber risk, with their assets and their** corresponding values, must be established.
- **Data on weaknesses** must be collected, always **in connection with existing assets, threats and protection methods**. A first potential risk identification indicator can be ensured by the **cyber risk self-assessment**. For example, methods proposed by specialized companies in the distribution of such insurance²⁵. These tools can help determine the risk exposure and awareness of the risk of the company and provide indications for the risks still unidentified. Another aspect would be how an attack of cyberspace can be detected as soon as possible from the time when it happened. A tool for analyzing the consequences of operations is of course the Business Impact Analysis (BIA).

Avoiding risks would mean that the electronic storage of information and the restriction of the use of computer systems. In today's world, this is hard to imagine. **Reducing risk and mitigation are more effective.** These are tools to reduce the likelihood of occurrence (e.g. anti-virus software, firewalls, etc.) or that diminish the size of the losses (e.g. disaster recovery plans).

In general, the **transfer of risk is possible by purchasing an insurance contract.**

²⁵ <http://www.marsh-stresstest.eu/>.

6. Conclusions

In order to achieve the correct positioning of intellectual capital assets of the post-knowledge economy, part of the cognition society, and for a more resilient cyber space, the following **conclusions** are revealed:

- **We are leaving in other economy, in a cognition economy**, and we should define it correctly, including new tools and methodologies
- **The human layer positioning** is essential for a correct set-up of the cyber world and to act against cyber-attacks over knowledge assets. The set-up of **Intellectual Capital Excellence Centers** will promote and keep in country people with knowledge, know-how, expertise.
- **It is vital to formulate and to assume policy and to support the regulation of cyber risk** by reducing political, social and economic impacts²⁶. These policies will have beneficial effects on both demand and supply levels.
- It is essential to establish **a new accounting framework for assessing knowledge and networks economy**. Also, to establish a system for the **reporting of losses generated by cybercrime and policies for cyber insurance**.
- It is necessary **to develop and use evaluation models**, based on **internationally recognized standards and certifications**, in an auditable way, based on new skills in the engineering of cyber risks.
- Cyber risks require the **achievement of a common front to increase the level of cyber-maturity and cybersecurity, application of the principles of risk management** and for combating cybercrime.
- **Human, structural and relational/customer capital should be reflected in balance sheets** and calculated as **knowledge assets** part of Intellectual Capital of companies.

²⁶ L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019

References

- [1] Allianz Global Corporate & Specialty, „Allianz Risk Barometer” 2019.
- [2] Brooking A., 1996. *Intellectual Capital: Core Asset for the Third Millennium Enterprise*. New York: International Thomson Business Press.
- [3] Edvinsson Malone Intellectual Capital, Realizing your Company's true Value by finding its hidden Brainpower. New York: Harper Business, 1997, p. 17.
- [4] F. Stibli, Intellectual capital - the key resource for expanding organisational intelligence, <https://intelligence.sri.ro/capitalul-intelectual-resursa-cheie-pentru-extinderea-inteligentei-organizationale/>. [Accessed: May. 10, 2019].
- [5] Human Capital-The Value of People <https://www.oecd.org/insights/humancapital-thevalueofpeople.htm>.
- [6] L. Badea, C.M. Rangu, "Ensuring cyber risk - a great challenge facing modern economies", RSF No. 6, May 2019.
- [7] Leif Edvinsson Intellectual Capital: Realizing Your Company's True Value by Finding Its Hidden Brainpower Hardcover, 1997.
- [8] Lucubrate Peter Welch October 12th, 2018 Magazine article No: 42, October 8th, 2018.
- [9] Ludo PYIS, AREOPA GROUP, *IS IT WORTH PROTECTING YOUR INTELLECTUAL CAPITAL FOR CYBER INTRUDERS (PPT presentation)*, 2013.
- [10] Ludo Pyse, NO CURE, NO PAY? Would applying this rule bring IT projects failure statistics down? ... and how do we measure sure success?, www.areopa.com.
- [11] Manfred Bornemann, Karl Franzens University Adolf Knapp, Karl Franzens University, 10 June 1999, Holistic measurement of intellectual capital country covered: Austria research.
- [12] OECD (2013), "Introduction and Overview", in Supporting Investment in Knowledge Capital, Growth and Innovation, OECD Publishing, <http://dx.doi.org/10.1787/9789264193307-4-en>.

- [13] Ten Key Questions on Cyber Risk and Cyber Risk Insurance, Geneva Association, Nov 2016.
- [14] THE POWER OF INTANGIBLES BY GARY COKINS, CPIM, AND NICK SHEPHERD, FCPA, FCGA, FCCA, May 1, 2017, <https://sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/>.
- [15] Wissensbilanz, https://www.academy.fraunhofer.de/en/continuing-education/technology-innovation/intellectual_capital_statement.html.
- [16] https://ec.europa.eu/research/innovation-union/pdf/KI-01-14-460-EN-N-IP_valuation_Expert_Group.pdf.
- [17] <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=11602&no=1>.
- [18] <https://magazine.lucubrates.com/intellectual-capital-and-knowledge-management/>.
- [19] <http://www.incd2020.ro/sites/default/files//Analiza%20bune%20practici%20intl%20rapoarte%20CI.pdf>.
- [20] https://www.researchgate.net/profile/Selcuk_Burak_Hasiloglu/publication/28263308/figure/fig1/AS:394353668313091@1471032649090/Edvinssons-Categorization-of-Capital-Resource-Leif-Edvinsson-and-M-S-Malone.png.
- [21] https://asfromania.ro/files/analize/Asigurari_risc_cibernetice.pdf.
[Accessed May. 09, 2019].
- [22] https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_1~5803aca48c.en.html.
- [23] <http://www.marsh-stresstest.eu/>.

Filling the Cybersecurity Skills Gap

Liviu MORON
European Commission
liviumoron@hotmail.com

1. Abstract

Everybody agrees today that there is a skill gap for cybersecurity professionals.

In 2018 the Cyberthreat Defense Report [1] showed that 8 companies out of 10 are impacted by a security talent shortfall.

The European Commission estimates [2] that: “The skills gap for cybersecurity professionals working in industry in Europe is predicted to be 350,000 (globally 1.8 million) by 2022”.

In this paper we would like to discuss about the state of cybersecurity skills in Romania, what could be the causes and how could be filled the Cybersecurity Skills Gap in the future.

2. Context of the research

What are the cybersecurity skills that companies are looking for and how the people are trained to be able to fulfil the requirements?

To discover what are the cybersecurity skills that companies are looking for at a certain moment in time (June 2019) we made a short list with jobs in cybersecurity and the skills that are required. If we are looking at the requirements for these jobs, we will see that they are based on certifications (CEH, CISA, OSCP, CISM, CISSP) delivered by Professional Associations (GIAC [3], ISACA [4]) or companies (Offensive Security [5], EC Council [6]).

You can see below a small list with jobs in IT Security that can be found on internet (June 2019):

1) Security Operations Analyst - Pen Tester [7]

...

- Education: Academic degree
- Certifications: CEH, OSCP, CISSP, Security +, CCNA Security, ITIL certification is an advantage

...

2) Information System Security Officer [8]

...

- Education: Academic degree
- Certifications: **CISA, CISM**, ISO 27001

...

3) Information Security Expert [9]

...

We expect you to have some part of the job related certifications (**CISSP/ CEH/ LPT / ISSAP** (ISS Architecture Pro / CSSLP (Software Lifecycle Pro) / CCSP (Cloud Security Pro), CISA, SANS.

...

As we can see there is only a requirement for a general Academic degree, but there is no academic degree related to security required by the companies that are searching for cyber skills, even if there are many academic programs for cybersecurity proposed by Universities.

A list with some academic programs for cybersecurity found on Internet can be found below:

- Advanced Cybersecurity (Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, Romania) [10] - 2 years / cost NA;
- Information Security (Faculty of Computer Science Iasi, Romania) [11] - 2 years / cost NA;
- Cybersecurity (Faculty of Mathematics and Computer Science, Babeş-Bolyai University, Cluj, Romania) [12] - 2 modules/ 8 weeks per module/ cost 425 euros per module.

There are trainings for cybersecurity on the market delivered by Universities, a certificate is delivered after the training, but these certificates are not required by companies when they want to hire IT security specialists.

There are no cybersecurity classes at the school level that could disseminate knowledge about IT Security among young people.

The certifications that are required by the companies are delivered by Professional Associations or private companies. The trainings required for these certifications are expensive and intensive (1 week in general) but they are preferred to academic cyber programs.

The public companies (hospitals, water suppliers, etc.) don't have the budget to take such expensive trainings, even if they need well trained IT security specialists to comply with legal requirements (NIS directive).

3. Conclusions and recommendations

What recommendations are there to fill the cybersecurity skills gap?

The final point in the training path for a cybersecurity professional, like in any other domain, is to be able to use the skills acquired during the training to deliver value added services to customers.

This activity can be provided as an entrepreneur, in which case a mix of technical and non-technical skills are needed for success, or as an employee in which case the success is based mainly on technical skills.

This paper is focusing on cyber skills required for a professional that wants to work in cybersecurity for a public or private company.

What are the solutions that can be implemented to fill the Cybersecurity skills gap?

1. Cybersecurity program for young people

Starting to learn cybersecurity at an early age can attract more people to this domain.

Cybersecurity classes should be organized at school level.

CTF contests for schools and universities should be organized regularly.

A Private Public Partnership could be established between private and public companies that are interested to fill the cybersecurity skill gap, to contribute to a National Program to support cybersecurity classes in schools.

We have already started a project for a CTF contest for schools and universities this year at the Cybershare Conference, companies interested in supporting this program are invited to contact us.

2. Correlation between offer and demand for cyber skills

Today there is no way to correlate the skills that are needed in Cyber on the market and the Curricula for Cyber in schools and universities. Every year the skills needed on the market should be put in correlation with the Curricula. Cyber classes should be focused on more practical activities, people from the industry should be invited regularly to share experience.

Cybersecurity Certifications delivered by Professional Associations are required by companies when they hire a specialist, but professionals with Cyber Certifications are not allowed to teach Cybersecurity in Universities without a PhD. And cyber skills that are required by companies are acquired after very expensive trainings delivered by Professional Associations.

At the European level, cybersecurity skills that are delivered to students in Universities should be correlated with job profiles and practical exams should be organised regularly to allow people to get different levels of certifications.

Ideally after each course the participant should be able to get a certification based on a practical exam to be able to prove the skill level that was acquired.

3. European Certification System for cyber skills

A trusted and affordable European Certification System for cyber skills should exist.

Today the Cyber Certifications are very expensive, difficult for a student that followed an Academic Cyber Program to afford a Cyber Certification.

4. Women in Cyber

Attracting more women in Cyber could be another way to fill the gap. Private companies should support events that try to bring more women in Cyber.

We have already discussed with public and private companies about Women in Cyber at the Cybershare Conference 2019, companies interested in supporting this program are invited to contact us.

5. Information and knowledge sharing in Cybersecurity

We live in an interconnected world and once that an element that is part of a system is compromised, the whole system is in danger. The cyber defense of a system is dependent on the weakest link.

Putting in place projects for information and knowledge sharing in Cybersecurity could help us to manage to improve the security of our systems.

The importance of Cybersecurity was recognized by the European Parliament, the Council and the European Commission that have reached a political agreement on the Cybersecurity to better support Member States with tackling cybersecurity threats and attacks.

It is now our turn to put Cybersecurity as a priority and to take concrete measures to fill the cybersecurity skills gap in Romania.

References

- [1] <https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf>.
- [2] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centresswd-one-403_en.pdf.
- [3] <https://www.giac.org>.
- [4] <https://www.isaca.org>.
- [5] <https://www.offensive-security.com>.
- [6] <https://www.eccouncil.org>.

- [7] <https://www.bestjobs.eu/en/job/security-operations-analyst-pen-tester?pos=28&list=2>.
- [8] <https://www.ejobs.ro/user/locuri-de-munca/information-system-security-officer/1187342>.
- [9] <https://www.ejobs.ro/user/locuri-de-munca/information-security-expert/1182461>.
- [10] http://acs.pub.ro/doc/master/ro/short_description/SAS-short-ro.pdf.
- [11] <https://www.info.uaic.ro/en/programs/information-security/>.
- [12] <http://www.cs.ubbcluj.ro/cyber/>.

**PART II.
CYBERSECURITY
DIRECTIONS**

**NATIONAL
CYBER SECURITY**

PART II. CYBERSECURITY DIRECTIONS

NATIONAL CYBER SECURITY

Threats and Challenges. A National Cyber Security Perspective

Viorel SÎNPETRU, Cătălina PISARGIAC
National Cyberint Center, Romania
cnc@cyberint.ro

1. Introduction

The rapid growth and development of technologies do not only provide people and states with a better and more efficient way of living, but also poses great security risks and represents a threats amplifier. While we can all agree that the Internet and smart devices have a great impact on our happiness, the potential risks and threats require an efficient response, which can, at times, be achieved only through coordinated efforts.

2. Assessment of the threat to national security

Over the last years, the cyber threat represented one of the most persistent and dynamic threat against Romania`s national security, from a quantitative point of view, considering the number of cyber attacks, and also on the account of the complexity of engaged methods.

Following its designation as national authority in the field of cyber intelligence by the Supreme Council of National Defense (CSAT), the Romanian Intelligence Service`s National Cyberint Center has endeavored to identify, prevent and counter the vulnerabilities, risks and threats to Romania`s cyber security.

CNC manages the National System for the Protection of IT&C Infrastructures of National Interest against Cyber Threats ("ȚIȚEICA"), through which 54 public institutions, since 2015, benefit from support for the security and efficiency of activities in the field of information and communications technology, as well as regarding reporting of cyber security events.

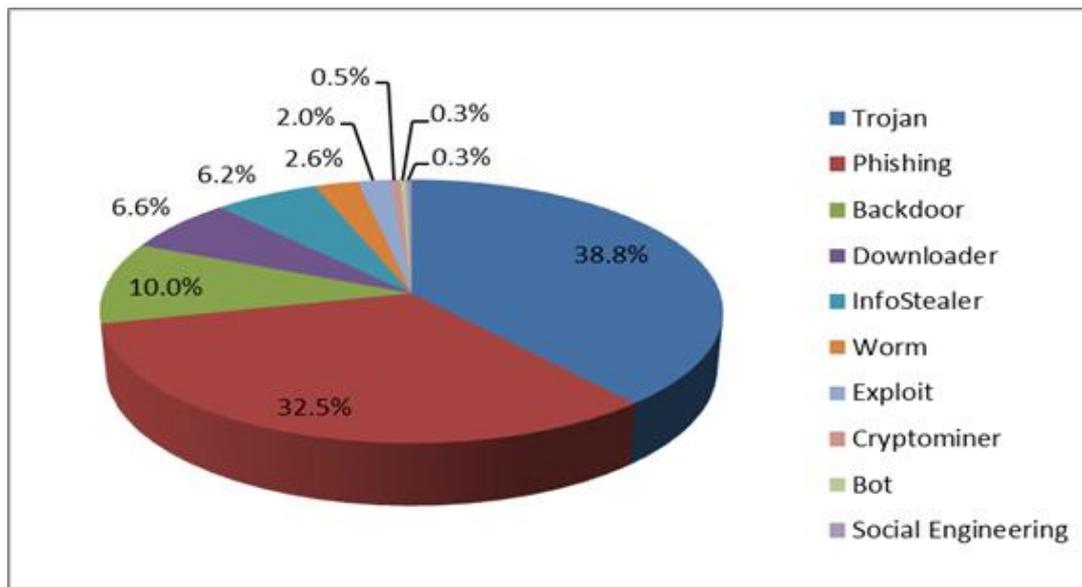


Fig. 1. 10 most frequent campaigns in Romania (Jan - Jul 2019) by malware type

Considering Romania's role as a NATO and EU member, its geographical position and strategic objectives, our country is daily exposed to cyber risks generated by state-sponsored entities, cybercrime groups and ideologically motivated groups [2].

2.1. Strategically motivated actors

The main threats against national security are offensive actions carried out by state actors with strategic motivation. In this context, cyber attacks have become a new weapon of war and the virtual space a new battlefield.

Actions of state actors consist of cyber attacks with high complexity and technological level, which allow the attacker to maintain persistence and untraceability over a long period of time. Most used strategically motivated cyber attacks are Advanced Persistent Threat (APT), which have a significant impact on national security [2].

These cyber attacks are targeting the IT&C networks of national critical infrastructures in sectors such as government, military, national security and economy. The goal is to exfiltrate information, to influence socio-political processes or to sabotage the infrastructure.

Among strategic APT cyber attacks, which targeted Romanian institutions, National Cyberint Center investigated the following ones [12]:

- **APT28** - that has a high level of technology and targeted government institutions in the sectors of foreign affairs, military, NGOs, journalists and political parties of NATO / EU. In the attack were used the following TTP: spearphising, social engineering, watering hole, exploiting vulnerabilities and backdoors.
- **MiniDuke** - that has a high level of technology and targeted government institutions in the sectors of foreign affairs, diplomacy, energy, telecommunications and defense. In the attack were used the following TTP: spearphising, customized backdoor, dropper and modular architecture.
- **Snake** - that has a high level of technology and targeted government institutions in the sectors of foreign affairs, diplomacy, defense, education. In the attack were used the following TTP: spearphising, social engineering and watering hole.
- **Red October** - that has an average level of technology and targeted diplomatic and governmental scientific research organizations. In the attack were used the following TTP: spearphising, social engineering, and trojan dropper.

2.2. Financially motivated actors

Financially motivated attacks are carried on by criminal groups that are interested in gaining significant profits with less work targeting a wide variety of entities, from public institutions, to private companies and to end-users without any discrimination. These kinds of attacks are usually less sophisticated compared to strategically motivated attacks, and they do not require strong technical abilities and knowledge.

Among significant challenges of 2018 we have witnessed the APT attacks targeting the financial-banking system carried out by eastern cybercrime groups.

Members of these groups are highly technically trained and they are seeking to carry out unauthorized transfers through inter-bank networks, unauthorized withdrawals through banks ATMs (the infection of ATM devices) or rising/lifting withdrawals limits.

Romania is also targeted by such attacks with the most recent taking place in the second half of 2018. The attackers tried to compromise the systems through which the networks of inter-banking transfers (SWIFT) and ATMs can be accessed. In order to achieve their goals, the group used Cobalt Strike, an open source tool, normally used in IT&C infrastructure security tests, activities known as penetration tests (pentesting) [13].

Cobalt Strike Platform has been used mainly by those known as Cobalt, Cobalt Group or Cobalt Gang, an eastern cybercrime group. They have generated considerable financial losses through complex cyber-attacks carried out upon banking institutions in Europe and Asia.

Despite of important members being arrested in 2018, as a result of international commune efforts led by law enforcement authorities, the group`s activity has not yet been interrupted, demonstrating that stopping/ countering online illegal operations is a real challenge.

2.3. Ideologically motivated actors

Ideologically motivated cyber-attacks carried out by hacktivist groups, cyber terrorist groups or independent hackers have a low technological level and are targeting low level security systems with exploitable vulnerabilities. Evolution becomes unpredictable if such an actor would gain access to medium or high level technological capabilities in order to exploit vulnerabilities of the IT&C networks of national critical infrastructures.

The evolution of hacktivist groups is a dynamic one, enhanced by the existence of events on the political, economic or social scene, which present interest to these groups. The attacks carried out by these groups are a reaction to such events. Also, these groups have the potential to restore and quickly coagulate around common ideals [2].

These cyber-attacks are characterized by a strong media impact, because the purpose is not to hide the attacks, but to assume and promote it publicly. The targets

are diverse, from IT&C infrastructures to websites belonging to public institutions and government, educational institutions, but also those of private entities.

By carrying out cyber-attacks, attackers aim to illegally access information systems and databases and make it public or change the content of web pages by inserting images and messages. Cyber-attacks carried out are usually defacement, Denial of Service (DoS) and Distributed Denial of Service (DDoS), that don't have a high degree of complexity and don't require advanced knowledge of hacking, most often these groups are using free tools available online [4].

When it comes to terrorist groups, the situation is similar. So far, they didn't achieve cyber-attacks with major impact to our national cyber security, but they use the virtual space mainly for supporting propaganda activities, recruitment and radicalization. They use defacement attacks to affect the availability and integrity of networks, by altering the content of web pages under appeal, in order to promote various forms of propaganda messages and images, also known as cyber graffiti.

The targets of these cyber-attacks, characterized by a low level of complexity, are the websites of private entities, but also of some local institutions, most likely selection criterion is given by the types of vulnerabilities and exploited identified by the aggressors after scanning operations.

3. National cyber security legislation

Since, during the last few years, the cyber threat in our country has been one of the most dynamic threats to national security, cyber security has become an important matter of national security. At national level, there has been a continuous effort to create and adapt national policies and strategies in regard to cyber security given the rapid evolution of cyber risks and threats [11].

3.1. Romanian Cyber Security Strategy (SSCR)

By Supreme Council for National Defense (CSAT) Decision no. 13/2013 and GD no. 271/2013 The National Cyber Security of Romania has been approved. SSCR settles the necessary conceptual and organizational framework for ensuring the cyber

security. It addresses the cyber infrastructure protection according to new concepts and policies in the field of cyber defense elaborated and adapted to Nord Atlantic Treaty Organization (NATO) and EU.

SSCR presents both short and long-term objectives, stating that the state relies on the availability and functioning of networks that structure the lives and economy of citizens. Thus, the goal is to develop a dynamic information environment based on interoperability and on the provision of IT services, while protecting citizens' fundamental right and liberties, as well as national security interests [11].

The objectives included in the strategy include: adjusting the legal and institutional framework to the dynamics of cyber threats; ensuring the resilience of infrastructures; ensuring security by identifying, preventing and countering vulnerabilities, risks and threats to Romania's cyber security; drawing on the opportunities provided by cyberspace; enhancing the citizens' cyber security culture; and more [8].

Cyber security aspects are also treated in the **National Defense Strategy (SNAp)** for 2015-2019 which names among the main threats to national security the cyber-attacks launched by hostile entities, state or non-state, against public or private infrastructure of strategic interest, cyber-attacks performed by cyber crime groups or extremist cyber-attacks initiated by hackers [1].

3.2. NIS Directive

The elaboration, in July 2016, of the 2016/1148 EU Directive Concerning measures for high common level of security of network and information systems across the Union (NIS Directive) confirms the constant concerns of EU forums on improving the resilience of IT&C infrastructure that belong to operators of essential services and digital service providers in Member States.

Moreover, NIS Directive implies that Member States elaborate a National Strategy concerning the security of networks and information systems, which will define the strategic objectives and adequate regulation measures, in order to improve the level of security for these systems. Concretely, Member States will transpose the

security requirements and the incident notification in the case of networks and information systems belonging to operators of essential services and digital service providers [13].

The NIS Directive represents a premiere in pan-European legislation concerning cyber security, its scope mainly focusing on [7]:

- The consolidation of authorities in the field of national cyber security;
- The improvement of cooperation between these authorities;
- The implementation of security requirements for key social and economical sectors.

2016/1148 EU Directive pays special attention to IT&C field, in the sense that it establishes clear stipulations for operators of essential services (OES) and digital service providers, with clear distinction between the two categories.

According to national laws of transposition of NIS Directive, CERT-RO is the national authority as well as unique national contact point (national CSIRT).

The transposition of NIS Directive into national regulation has been achieved through 362/2018 Law concerning measures for high common level of security of network and information systems, promulgated by the President on 28 December 2018 and took effect starting 12 January 2019 [10].

In addressing technological trends and the threat landscape in the cyber space, policies, strategies and the legislation have to be comprehensive and constantly adapted in order to provide an efficient framework for entities with responsibilities in cyber security.

4. Awareness

Cyber-attacks directed against both state institutions and citizens continue to be a significant risk against national security. The threat is growing, both in terms of number and complexity of cyber-attacks conducted.

Recent evolution of cyber-attacks against our country ranks the cyber threat among the most dynamic threats, cyber security issues becoming a priority for all actors.

In this regard, the responsibility for ensuring cyber security returns to all entities involved in the public, private, and citizens alike.

For public institutions is important to implement proactive measures, preventive and reactive which may include policies, concepts, standards and guidelines for security, risk management activities, training and awareness, implementing technical solutions to protect infrastructure cyber identity management and consequence management [12].

It is important that all actors involved in ensuring cyber security know: the impact and effects of a cyber-attack, the exposure to the risk, the amount of sensitive data stored in system and that the partnership with other institutions / companies will increase cyber security.

5. New trends and challenges in cyber security

Development of new technologies, such as artificial intelligence, fifth generation networks, Internet of Things and blockchain, offers a number of opportunities in terms of developing social standards globally by creating instruments and mechanisms that facilitates users interaction with digital environment. However, due to the characteristics of cyberspace - speed, interconnectivity and availability - have resulted a number of risks and threats aimed at a wide range of entities, from individual users to governmental institutions [13].

5.1. Artificial intelligence (AI)

Daily needs of society, but also the desires to simplify the life and scientific progress have led to the development of artificial intelligence, which is no longer a sci-fi movie topic, but a concrete part of everyday reality. With these developments, cyber security should be one of the most important concerns in the IT sector, given the wide range of applicability.

The rapid pace of technological change has led to the inclusion of AI in securing digital environment. Both the public and private sector are interested in understanding how to use AI for data protection and create more opportunities to optimize specific

activities. Given the progress made, a number of cyber security companies have developed solutions based on AI to protect against cyber-attacks [13].

Thus, products developed based on AI provide support for cyber security specialists in the detection and investigation of complex cyber threats, such as APT campaigns. Given that, AI has the potential to provide the capabilities necessary for detection, investigation and mitigation of cyber security risks. Companies have started to invest more and more resources in this area to develop solutions based on this technology, to block, isolate and study malicious activities, which will require minimal involvement of the human factor [13].

In the context of technological progress generated by the development of products and services using AI, it is a matter of time until this technology will be used by offensive actors to develop complex cyber-attacks. An example of this is an experiment which aimed to test who can be more successful in conducting phishing attacks - human or artificial intelligence. The results confirmed that the "AI hacker" proved to be more effective than a human hacker in the writing and distribution of messages with malicious content [13].

Although artificial intelligence is in the process of redefining and discovery of new ways of implementation, it is clear that entities which will invest in this technology will benefit and gain clear advantages, both short and long term.

5.2. Fifth generation networks (5G)

These networks will shape the future fundamental structure of societies and our economies, connecting billions of devices and systems, being included in critical sectors such as energy, transport, banking, health and industrial control systems containing sensitive information and supporting safety systems. Also, democratic processes such as elections are relying more and more on digital infrastructure and 5G networks, highlighting the need to be protected against possible cyber attacks.

The security issue is crucial because of the important role of 5G technology for Internet connected products, from autonomous automobiles and smart cities to

augmented reality and artificial intelligence. If technology is vulnerable, it can allow hackers to exploit such products to spy or to disrupt the activity.

In this context, by the end of June 2019, each state of The European Union shall complete a national risk assessment on 5G network infrastructures. They must update the existing security requirements for network providers and include conditions to ensure public safety networks, especially when granting rights to use radio frequencies in the bands 5G. These measures should include stronger obligations on suppliers and operators to guarantee network security [14].

Risk assessments and national measures must take into account various factors, such as technical risks and risks related to the conduct of suppliers or operators. National risk assessments will be a central element in developing a coordinated risk assessment at EU level. A potential vulnerability in the 5G network that would a cyber attack would affect Romania, highlighting the necessity of measures taken at national level to ensure a high level of cyber security.

5.3. Internet of Things (IoT)

The Internet of Things is a new technology allowing smart objects to communicate and exchange information with one another, while collecting big amounts of data through designated sensors. These sensors are meant to collect important and sensitive data about locations, movement, temperature, lifestyle and behavioral patterns and even preferences in terms of music, movies, food, and hobbies.

As the Internet has evolved tremendously we have witnessed a growth in terms of development and use of smart objects connected in the internet of things, and although innovation provides people with a better way of performing everyday tasks, we have to be aware of the risks implied [3].

In the context of IoT, the main challenge is represented by the lack of standards in terms of security, a very important aspect considering that IoT devices can be both a target and an instrument for carrying out cyber-attacks. Therefore, the rise in IoT technology adoption can cause cyber security risks generating the need for

comprehensive regulations regarding the way smart objects are being designed, manufactured and used.

"As technology and security threats advance, attacks against IoT devices will evolve targeting critical infrastructure that bridges our digital and physical worlds".¹ Integrating smart devices in IT&C critical infrastructure could become a challenge for cyber security institutions that will have to mitigate the risks and counter the imminent threats [5].

Another risk is generated by the short history of the IoT technology, since smart objects are just now making their way to users that are not familiar to such devices and therefore have not yet developed a security oriented digital behavior. In the majority of time, the most crucial aspect of cyber security is related to how users perceive the devices and its security based on the experience and knowledge they have.

In other words, users or consumers are interested in using the devices, manufacturers are interested in making profit out of it and security risks are left to the cyber security responsible institutions that should be supported in their activities by regulations.

5.4. Blockchain

The Blockchain is a form of Distributed Ledger Technology that acts as an open and trusted record of transactions (in the form of actions) from one party to another that is not stored by a central authority [9]. Instead of a central authority maintaining a database, all nodes have a copy of the ledger, and information is validated by a few or all the nodes through complex mathematical algorithms.

The most important inherent characteristics of blockchain applications are anonymity, granted to a certain extent, the distributed nature, creating a trustless environment, immutability, as every transaction/action cannot be modified once it is validated and traceability, making it possible to read all transactions.

¹ Kumar Agarwal, general manager for IoT at Symantec.

From a national cyber security point of view, blockchains can be treated from two perspectives, as a technology that could be implemented in critical IT&C infrastructure and as digital value, cryptocurrencies being the subject of cyber criminal activities.

Given the youth of blockchain technology, governments and even the public sector are struggling to understand its principles and effectiveness, but they are taking actions toward gathering the appropriate knowledge and introducing blockchain concept in some of the services they provide for the citizens [6]. In the context of this technological shift, the cyber security of blockchain based IT&C infrastructures has to be assured and adapted to new challenges.

Furthermore, national cyber security practitioners have to understand what blockchain technology is and how it is being implemented, in order to be able to provide a high level of security for those IT&C systems and best support for policy makers regarding blockchain based technology.

Similarly, blockchain is most known as the technology behind the Bitcoin, and other cryptocurrencies that are currently being used in financial transactions, as a way of transferring value (also known as peer-to-peer payments), investment and not ultimately as a way of payment.

Because of all main characteristics of cryptocurrencies, they are also being used as payment for cyber crime infrastructure and tools, and as a way to monetize their gain like in the case of ransom campaigns. In this case, cyber security experts need to adapt to these challenges, but in order to be able to counter this phenomenon, tools have to be developed and regulations have to be adopted.

6. Conclusion

Given the dynamic characteristics of the technological and cyber threats environments, efforts are necessary in terms of developing cooperation between interested and affected entities and in the direction of creating an adapted legal framework. Only by creating this working framework based on cooperation,

understanding the new trends, and appropriate legislation, we can get close to achieving our goals on ensuring a good level of cyber security.

References

- [1] Administrația Prezidențială, "Strategia națională de apărare a țării pentru perioada 2015-2019," 2015. [Online]. Available: https://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf. [Accessed: May 15, 2019].
- [2] A. Rog, "Gânduri la granițe. Reziliența frontierei digitale," July 03, 2017. [Online]. Available: <https://intelligence.sri.ro/garduri-la-granite-rezilienta-frontierei-digitale/>. [Accessed: May 15, 2019].
- [3] C. Pisargiac, "Dispozitivele inteligente, spionii de acasă," Jan. 03, 2019. [Online]. Available: <https://intelligence.sri.ro/dispozitivele-inteligente-spionii-de-acasa/>. [Accessed: May 15, 2019].
- [4] D. Costan, C. Florea, and O. Iordan, "Cyberterrorism: Status quo în 2015," Oct. 06, 2015. [Online]. Available: <https://intelligence.sri.ro/cyberterrorism-status-quo-2015/>. [Accessed: May 15, 2019].
- [5] D. Roe, "6 security issues that will dominate IoT in 2019," Jan. 14, 2019. [Online]. Available: <https://www.cmswire.com/internet-of-things/6-security-issues-that-will-dominate-iot-in-2019/>. [Accessed: May 15, 2019].
- [6] Deloitte, "Blockchain in public sector - Transforming government services through exponential technologies," Jan. 2018. [Online]. Available: <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf>. [Accessed: May 15, 2019].
- [7] 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. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>. [Accessed: May 15, 2019].
- [8] Guvernul României, "Strategia de securitate cibernetică a României," 2013. [Online]. Available: <https://www.enisa.europa.eu/topics/national-cyber->

- security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf. [Accessed: May 15, 2019].
- [9] J. Berryhill, T. Bourgerly, and A. Hanson, "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector," *OECD Working Papers on Public Governance*, No. 28, OECD Publishing, Paris. [Online]. Available: <https://doi.org/10.1787/3c32c429-en>. [Accessed: May 15, 2019].
- [10] Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. [Online]. Available: <https://lege5.ro/Gratuit/gmytiobyga2a/legea-nr-362-2018-privind-asigurarea-unui-nivel-comun-ridicat-de-securitate-a-retelelor-si-sistemelor-informatice>. [Accessed: May 15, 2019].
- [11] O. Iordan, "Building Cyber Resilient Society in the region of SEE - Cyber Threats to Romanian National Security", RACVIAC - Center for Security Cooperation, June 2016.
- [12] Serviciul Român de Informații, "Buletin Cyberint - Semestrul 1 2018," [Online]. Available: <https://www.sri.ro/assets/files/publicatii/BULETIN-CYBERINT-20x20cm.pdf>. [Accessed: May 15, 2019].
- [13] Serviciul Român de Informații, "Buletin Cyberint - Semestrul 1 2019," [Online]. Available: <https://www.sri.ro/assets/files/publicatii/buletin-cyber-sem-1-2019.pdf>. [Accessed: May 15, 2019].
- [14] Comisia Europeană, "Comisia Europeană recomandă o abordare comună la nivelul UE în privința securității rețelelor 5G," Mar. 27, 2019 [Online]. Available: https://ec.europa.eu/romania/20190327_securitate_cibernetica_tehnologie_5g_ro. [Accessed: May 15, 2019].

CERT-EU: Contributing to a Cyber Secure European Union

Arthur DE LIEDEKERKE, Georgios PSYKAKOS

The Computer Emergency Response Team for the EU Institutions,
Bodies and Agencies (CERT-EU)

arthur.de-liedekerke-beaufort@ec.europa.eu, georgios.psykakos@ec.europa.eu

1. An introduction to CERT-EU

CERT-EU is the Computer Emergency Response Team for the European Union institutions, bodies and agencies (EU-Is), its constituents. It was first established as a pilot scheme in 2011 by the then-Vice-President of the European Commission for the Digital Agenda, Neelie Kroes, as part of the European Union's (EU) commitment to lead by example in the domain of cybersecurity in public administrations¹. In December 2017, CERT-EU's mandate was reinforced through an inter-institutional arrangement with a mission to act as the cyber-security information exchange and incident response coordination hub for the EU-Is. Today, CERT-EU has over 30 experts at its disposal who deploy specialised tools to detect and mitigate increasingly complex threats across a diverse constituency spanning 65 organisations.

In order for CERT-EU to fulfil its mission, it works closely with the national/governmental CERTs of the EU Member States (MS), the European Free Trade Association (EFTA) states and a number of peers in third countries. Among others, it is a member of two multilateral cooperation platforms: the CSIRTs Network (CNW) and the European Government CERTs (EGC) group. The former, established by the European Union's 2016 Network and Information Security (NIS) directive² (the first EU-wide legislation on cybersecurity), brings together the representatives of the EU's 28 Member States CSIRTs and CERT-EU, with the European Network and

¹ http://europa.eu/rapid/press-release_IP-11-694_en.htm

² <https://eur-lex.europa.eu/legal-content/EN/>

Information Security Agency (ENISA) acting as its secretariat. The latter is an association of governmental CERTs in Europe, with a largely technical focus.

Because fostering communication and trust between all stakeholders in the cybersecurity community is vital, CERT-EU also enjoys bilateral ties with a number of other international organisations, such as NATO, as well as leading IT security vendors and sectoral, information-sharing groups like the Belgian Cyber Security Coalition.

2. A growing array of threats and challenges

Cooperation in the cyber domain in the EU has gained momentum in recent years as a result of a number of factors. Chief among these has been the necessity to adapt to a fast-paced and expanding cyber-threat landscape. As a Centre for European Policy Studies (CEPS) report from late 2018 reminds us, “the economic, social, and political costs of Europe’s exposure to cyberattacks are real [1].”

From high profile data breaches to disinformation campaigns seeking to interfere in the EU’s internal democratic processes or the targeting of critical infrastructure - many recent examples have all made clear the serious risks and severe impact information security incidents can have on our societies. In an increasingly digitalising world, the uptake of Internet of Things (IoT) technologies, cloud services and other innovations have considerably expanded the attack surface, offering new intrusion vectors and vulnerabilities to malicious actors. Despite all the technological precautions defenders may take, human action and error are often at the root of cybersecurity issues. Phishing attacks and email-based social engineering (collecting personal information which is then used for identity fraud) tactics are routinely and effectively used by adversaries to circumvent advanced cybersecurity systems. In order to effectively counter these threats, mutual assistance in the detection and mitigation of incidents, pooling of expertise and a timely exchange of qualitative cyber threat intelligence is of the essence.

Next, the desire to do more together has been driven by the increased “ability and willingness of state and non-state actors to pursue their objectives through

malicious cyber activities [2].” Of particular concern are the Advanced Persistent Threat (APT) groups, often state-affiliated or sponsored, who typically engage in the stealthy penetration of an organisation's network and methodically, sometimes over lengthy periods of time, try to obtain sensitive data that can be exploited for political gain or espionage purposes.

The threat of bolder and more competent adversaries in the yet unregulated battlefield of cyberspace has been compounded by systemic changes in the global geopolitical context. European governments are now keen to shore up their ability to protect their strategic interests and values in a more volatile security environment, as the recent adoption of the EU Cyber Diplomacy Toolbox³ testifies.

Finally, the appetite for more EU cooperation has been motivated by the growing realisation that cyberspace does not show respect for national jurisdictions: a cyberattack or crisis is rarely geographically bound, from “its origin, spread, and implications [that] unfold across borders [3].” The need for EU-wide resilience despite differing national capabilities and postures has triggered an interest in setting up mechanisms, common platforms and identifying burden-sharing opportunities to raise the collective level of cybersecurity and avoid lesser-prepared states becoming easy targets. Faced with the challenges previously outlined and in light of the plethora of authorities and structures involved in cyber, the EU has often taken the lead on coordinating legislative efforts, playing a vital role in facilitating European-level cooperation. The section below provides a non-exhaustive list of some of the significant developments that have taken place in this field.

3. New structures and deeper cooperation in the EU’s cyber ecosystem

Strengthening the EU-Is incident-response capabilities

At the level of its constituency CERT-EU, in close consultation with the IT security teams of the institutions, bodies and agencies, has championed the idea of

³ <https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>

developing a mechanism to tackle major cybersecurity attacks. This paper is, first and foremost, a call for formalised coordination among internal incident response teams of the EU-Is, ensuring that robust cyber defence measures and a high level of situational awareness is maintained across the constituency (notably thanks to CERT-EU's cyber threat intelligence products). Regular joint exercises and the nurturing of collective expertise through workshops on emerging techniques, such as machine learning, will seek to reinforce further the culture of cooperation among constituents.

Moreover, in cases where an attack whose scale would require the deployment of resources beyond the ones available by the affected constituent and CERT-EU, two distinct and, if needed, complementary options exist to rapidly increase incident-response capabilities. First, CERT-EU is spearheading the creation of an inventory of expert profiles among the larger constituents from which to draw upon for a collective response in the case of such a major attack. It is also developing an arsenal of cyber tools and procedures that will facilitate a coordinated crisis response in its constituency. In addition, a recourse to external capacities mandated by trusted partners (including the possibility of resorting to the PESCO Cyber Rapid Response Team- discussed in further detail below) is foreseen as a last line of defence.

The European Cyber Security Act: landmark legislation

The Cybersecurity Act, an EU Regulation adopted in 2019 establishes an EU-wide certification framework to ensure products and services are cyber-secure. It also grants ENISA a permanent mandate and considerably bolsters its resources, both financial and human.

The new EU Agency for Cybersecurity, as ENISA will henceforth be known, will be tasked with “actively supporting” MS and relevant stakeholders in achieving “a high common level of cybersecurity across the Union [4]”, including by assisting MS in capacity-building and supporting the implementation of sectoral policies on cybersecurity. In so doing, the Act is careful to stress the need for close liaison among all relevant stakeholders and calls for synergies with existing actors, networks in the

EU's cybersecurity ecosystem, notably CERT-EU whose technical and operational expertise will inform their "structured cooperation [ibid]".

Promoting an effective, EU-wide response to large-scale cyber crises

The European Commission's Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, the so called Blueprint, was developed in late 2017 in order to provide a comprehensive overview of how Europe and Member States can "respond quickly, operationally and in unison when a large-scale cyberattack strikes [5]". CERT-EU is one of the main actors listed in this document: it has a dual role as both a member of the CNW and as the CERT responsible for the EU-Is. In this capacity, it is involved in several of the Blueprint's core objectives including an effective response to large-scale cybersecurity incidents and contributes to a shared situational awareness, thanks to its function as an information hub for the EU-Is.

Key elements of this Blueprint were recently tested during a November 2018 table-top exercise known as "EU HEX-ML PACE (Parallel and Coordinated Exercise)". Its goal was to improve the coordination between NATO and the EU - as part of the PACE concept between the two organisations - as well test the EU's ability to respond to a complex, multidimensional crisis involving significant cyber elements.

Based on lessons learned drafted by all players and on consultations carried out by the NIS directive Cooperation Group, the Blueprint will go through a second iteration intended to further operationalise it. It will notably seek to remedy certain gaps in the interplay between cyber stakeholders and existing information flows and crisis management procedures at various levels of governance - ranging from the technical to the strategic/political through the operational layer.

Building on complementarities between the EU's cyber entities

In May 2018, CERT-EU entered into a Memorandum of Understanding (MoU) with fellow EU-level organisations involved in cyber: ENISA, the European Defence Agency (EDA) and Europol's European Cybercrime Centre (EC3). Born out of a desire to improve their collective ability to support EU initiatives in the cyber domain and

avoid the duplication of efforts, the MoU focuses on mutual invitations to cyber exercises, common education and training, exchange of information, and facilitating collaboration on strategic and administrative matters. In November of the same year, the MoU Signatories agreed on a common Roadmap laying out concrete activities and deliverables that have since been reflected in their respective work programmes.

In addition to ensuring cross-pollination between the law enforcement, cybersecurity and cyber defence communities, this initiative has already yielded tangible results ranging from staff exchanges and enhanced information sharing to joint workshops on topical issues such as threat hunting. It has received praise from the High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission, Federica Mogherini, who has emphasised that the value of this MoU resides in “working together, joining forces, putting the experiences and the knowledge of all at the service of our citizens' security [6].”

Taking advantage of new initiatives

The Permanent Structured Cooperation (PESCO) framework - a voluntary permanent framework for cooperation allowing Member States to jointly “develop defence capabilities, invest in shared projects, and enhance the operational readiness and contribution of their armed forces [7]” - has seen two projects specifically dedicated to cyber but which have military and civilian dimensions.

One of these is Lithuanian-led and involves the creation of Cyber Rapid Response Force teams (CRRTs) that will “provide mutual assistance between participating Member States, and as appropriate to help other EU Member States, EU institutions, including CSDP missions and operations, and eventually Partners [8].” These CRRTs, composed of experts pooled on a rotational basis, will be ready to provide operational support and reinforce the investigation efforts of national or EU authorities in the event of a significant cyber incident.

At the time of writing this paper, the project has already reached operational capability: the 8 participating MS have all signed a Declaration of Intent, Political and Legal Memos detailing key actors and decision-making processes, and the Netherlands

was the 1st rotating Member State for 2019 to offer a team on stand-by. CERT-EU, along with other stakeholders such as the EDA, participates as an observer and has recently taken steps to explore additional modalities of cooperation, including the possibility of benefiting from the support of CRRTs under very specific circumstances linked to its major cybersecurity attacks contingency plans.

4. Conclusion

Significant strides have been made in strengthening the EU's cybersecurity and encouraging cooperation in this field. However, a host of questions and challenges remain.

Despite laudable progress, the EU's cyber ecosystem remains multi-layered and fragmented. With defence and security issues being a core competence of MS, many countries consider cybersecurity capabilities to be an essential part of their national sovereignty and are reluctant to delegate or divulge too much. This problem has material implications: the "EU and its Member States need to know how much is being invested collectively to know which gaps to close but forming a clear picture of this is difficult [9]" in the absence of an overarching cybersecurity strategy.

Equally preoccupying is the topic of strategic autonomy in the digital realm. A recent high-level hearing organised by the European Political Strategy Centre highlighted that the "weakening of the EU's industrial and technological base" has led to "an overreliance on non-EU components in the value chains of certain sectors" giving rise to "concerns over security of supply and the integrity of critical information infrastructure [10]."

Nevertheless, the borderless nature of cyber space, the severity of the threats and the often prohibitive cost of achieving robust cyber defence measures alone all make the case for more EU-level action. The EU has proved to be a promising vehicle for leveraging synergies and burden-sharing in the past and is well placed to do so in the future. As digital security risks continue to grow for the MS and the EU-Is alike, so too must the pace of reform and the commitment of resources that has animated the EU in recent years.

References

- [1] L. Pupillo, M. Griffith, S. Blockmans and A. Renda, “Strengthening the EU’s Cyber Defence Capabilities,” CEPS Task Force Report, Nov. 26, 2018. [Online]. <https://www.ceps.eu/>. [Accessed June 12, 2019].
- [2] European External Action Service, “New tool to address cyber threats: the EU's Rapid Response Force,” June 27, 2018 [Online]. <https://eeas.europa.eu/>.
- [3] S. Backman and M. Rhinard, “The European Union’s capacities for managing crises,” *Journal of Contingencies and Crisis Management*, vol. 26, no. 2, June, 2018. [Online]. <https://onlinelibrary.wiley.com/doi/full/10.1111/1468-5973.12190>. [Accessed: June 14, 2019].
- [4] European Parliament, “European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")”, 2019.
- [5] European Commission, “Press release: State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks,” Sept. 19, 2017. [Online]. http://europa.eu/rapid/press-release_IP-17-3193_en.htm.
- [6] European Defence Agency, “Four EU cybersecurity organisations enhance cooperation,” May 23, 2018. [Online]. <https://eda.europa.eu/>.
- [7] Council of the European Union, “Defence cooperation: Council assesses progress made in the framework of PESCO after first year of implementation,” May 14, 2019. [Online]. www.consilium.europa.eu/.
- [8] Council of the European Union, “Permanent Structured Cooperation (PESCO) updated list of PESCO projects - Overview,” Nov. 19, 2018. [Online]. <https://www.consilium.europa.eu/>.
- [9] European Court of Auditors, “Multiple challenges in EU cybersecurity, warn auditors,” March 19, 2019. [Online]. <https://www.eca.europa.eu/>.
- [10] European Political Strategy Centre, “Strategic Autonomy in the Digital Age,” Dec. 17, 2018. [Online]. <https://ec.europa.eu/>.



CYBER DEFENCE



CYBER DEFENCE

National Implications in Implementing NATO's Cyber Defence Policy Concept

Mihai-Ştefan DINU

Information Systems and Cyber Actions Department,
“Carol I” National Defence University, Romania
mihaistdinu@yahoo.co.uk

1. Introduction

When it comes about Cyber, a vast number of authors refers to William Gibson's novel *Neuromancer*. There is no doubt that modern human life on the XXI century could not be perceive in its entirety without the significant role of technology, especially information and communication technology (ICT). Indeed, ICT permitted in the last two decades a burst regarding not only to professional level of communication and information of human activities, but also to the individual intimate level of every individual. Along with these aspects of human life, research and development activities benefitted of the means provided by the technological development. However, as researchers, educators and professionals we must mentioned the fact that Yoneji Masuda in his work *The Information Society as Post-Industrial Society* depicted the emergence of ICT in human society several years before the appearance of William Gibson's novel [1]. Thus, Masuda promoted information utility as the main production centre of information society. In his perspective, the information utility constitutes of information networks and data banks [2], in other words a public infrastructure based on interconnected computers.

In the same period when Masuda's view was being promote, another significant event was taking place: The Internet emerged public from the military testing laboratories. Initially perceived as a tool that facilitated communication, Internet rapidly expanded its functions along with the implementation on extended geographic areas.

Today, the Internet is not only a technological tool. In 2011, the United Nations declared in a report issued by the Special Rapporteur Frank LaRue on the promotion and protection of the right to freedom, opinion, and expression that by the fact that it facilitates the realization of a range of other human rights [3], the access to internet is a fundamental right. This affirmation comes in the context in which, 11 years earlier, Estonia legislates [4] Internet access as a basic human right, in the year 2009 France Constitutional Council [5] declared it a fundamental right and, similarly, a 2010 decision [6] of Costa Rica Constitutional Court.

Obviously, the free access to internet did not attract only positive actions, but also criminal ones. The vast virtual cyberspace becoming populated not only with actors offering social, educational or professional tools but with diverse criminal actors whose actions lead to decisions taken by vast majority of nation states to legally, politically and technically protect their infrastructures in face of cyber attacks.

2. Cyberspace the 5th operational domain

The existence of cyber acts in 2007 in Estonia as well as in 2008 in Georgia, lead to the conclusion that cyberspace can be a battlespace. Therefore, Internet a generally used tool after its originally development in the military labs, make a return in its starting activity domain, through the opportunities opened by the technological development, and get a militarized dimension. Moreover, the 2014 events in Ukraine were preceding by an orchestrated cyber attack on communications, cell networks jamming and internet connections severing, in a Russian attempt to obtain an information blackout [7].

On this background, military organizations realized the fact that successful results of the conventional military operations are increasingly dependable or enabled by the access to cyberspace that, in many cases grants access not only to military infrastructures but also to civil critical infrastructure within both the national borders and foreign operational theatre. In this sense, most states started to develop cyber security strategies, along with the necessary doctrine to support cyber operations. Cyber Defence concepts were developing both at national and international level.

A very illustrative example is the evolution of NATO Cyber Defence Policy.

3. Evolution of NATO Cyber Defence Concept

As a political-military alliance NATO was always focusing on its communication and information systems, so when an Alliance Web server had been shot, down back in 1999, by a series of attack DDoS type, military leaders understood that bombs can also be logical, as forensic they performed got traces leading to Serbian military [8]. As a result, starting with the 2002 NATO Summit held in Prague, has been developing Alliance's Cyber Defence concept.

Until nowadays we can consider that the development of afore mentioned concept had six successive stages, as follows (Table no. 1).

Table 1. Evolution Stages of NATO Cyber Defence Concept

Stage	Year	Summit	Milestones In Concept Development
1st - Recognition	2002	Prague	NCIRC establishment
2nd - Foundation	2008	Bucharest	NCD Policy 1.0
3rd - Centralization	2010	Lisbon	<ul style="list-style-type: none"> • Capability targets in NATO Defence Plan Process • Information Sharing • NCD Policy 2.0 • Investments
4th - Enhancement	2014	Wales	<ul style="list-style-type: none"> • NCD 3.0 • Legal issues • Creation of Cyber Range • Fostering Partnerships
5th - Adaptation	2016	Warsaw	<ul style="list-style-type: none"> • Cyber Defence Pledge • Cyberspace as the 5th operational domain • Partnerships at national and international level with industry and academia
6th - Operating	2018	Brussels	<ul style="list-style-type: none"> • Integration of cyber effects • Creation of Cyberspace defence centres

Main characteristics of each stage is further discussed.

First stage, RECOGNITION, constituted a pure technological approach, with exclusive focus on protection of key NATO systems as a result of recognition of cyber threats to NATO networks. It is the creation stage of NCIRC (IOC) [9].

Second stage, FOUNDATION, at Bucharest Summit, represents in fact the first step in policy approach by:

- Issuing NCD Policy 1.0;
- Adopting 1st Policy following 2007 cyber attacks in Estonia;
- Establishing objectives and principles (NATO and allies responsibilities);
- Organization of CDMA [10] structure, later CDMB [11].

Third stage, CENTRALIZATION, represents the moment when:

- NCD Policy 2.0 was issued;
- Lisbon Strategic Concept was launched;
- 2nd policy was adopted (June 2011);
- Protection was centralized through NCIRC (FOC) with 80 million euro invested;
- Were agreed cyber defence capability targets in the framework of NATO Defence Planning Process;
- Information Sharing Mandate was issued.

In the fourth stage, ENHANCEMENT represents moment when cyber defence had been directly link to NATO's core task of collective defence, and additionally:

- was recognized the applicability of international law in cyberspace;
- enhanced focus on training, education and exercises;
- was decided the creation of Cyber range;
- enhancing Information Sharing process, including MISP;
- launching calls for partnership, including industry.

ADAPTATION stage, showed a focus on:

- strengthening and enhancing national cyber defence capabilities as a matter of priority by issuing Cyber Defence Pledge;
- recognition of cyberspace as a domain of operation in which NATO must defend itself as effectively as in the air, on land, at sea and on space;
- starting new and enhancing existing partnership with countries, international organizations, industry and academia;

The actual stage, OPERATING, initiated in 2018 is an ongoing task to:

- integrate cyber effects;
- create Cyberspace Defence Centres.

4. Implications of the NATO Cyber Defence Policy Concept at national level

NATO's institutional adaptation means in fact the adaptation of each member of the Alliance as part of the whole, bringing their capabilities to the agreed level of interoperability. The capability target E-6202, assumed by Romanian MoD, stipulate the establishment of a command level entity capable to plan and conduct missions in the 5th battle domain, assuring in the meantime, a unique liaison with NATO in cyberspace operation domain.

4.1. Strategy and governance initiatives

In order to fulfill agreed tasks Romanian legislator amended and supplementing by Law 167/2017 the existing Law 346/2006 on the organization and functioning of MoD. There were introduced new provisions related to the aspects on establishment of cyber defence forces and Cyber Defence Command (CDCCom) and new MoD attributions on developing and optimizing national cyber defence capabilities.

Thus, on 1st of December 2018 is established the Cyber Defence Command following the memorandum approval by National Supreme Defence Council.

The major areas of responsibility of CDCCom are as follows:

- developing, implementing and managing the configuration of information technology infrastructures and services for military users;
- protection and resilience of military information technology infrastructures against cyber threats;
- early warning and response to aggressive actions in the cyber space against the military capabilities;
- specialized training of personnel;
- standardization and interoperability in cyber defence domain.

4.2. Operational efforts

The challenges in the operational field in cyber defence domain are primarily related to the anticipation and identification of technological advances in order to exploit/operationalize emerging technologies and disruptive innovations.

A similar focus has to be oriented towards a highly valuable asset: people. Level of readiness of cyber forces will be reached only with highly trained personnel.

In order to face those two challenges - technological and personnel - CDcom have to develop and operationalize partnerships with academia, industry, services and agencies that understand the threats originating in cyberspace as well as information sharing, operational planning, capability development and joint exercises.

4.3. Educational trends and offers

Academia is a good place to start: first in developing partnerships and second in developing technological capabilities together with the industry partners.

Beside this starting point, academia can and must provide the environment needed for the future highly trained cyber forces.

Carol I National Defence University has been developing in the last few years learning and training programs in domain of information systems and cyber defence, following closely the model of generating the competency level in cyber defence discipline, consistent with EU-NATO Joint Declaration Implementation Plan (JDIP) Action3.2 (strengthen cooperation on training) and JDIP Action3.4 (strengthen cooperation in cyber exercises) [12].

However, Information Systems and Cyber Actions Department (ISCA), manages graduation and post-graduation programs for officers and for the civilian student. Thus, Information systems Graduation program is open to any civilian students who want to attend it, following an exam as the positions are limited to a number of 25 each year.

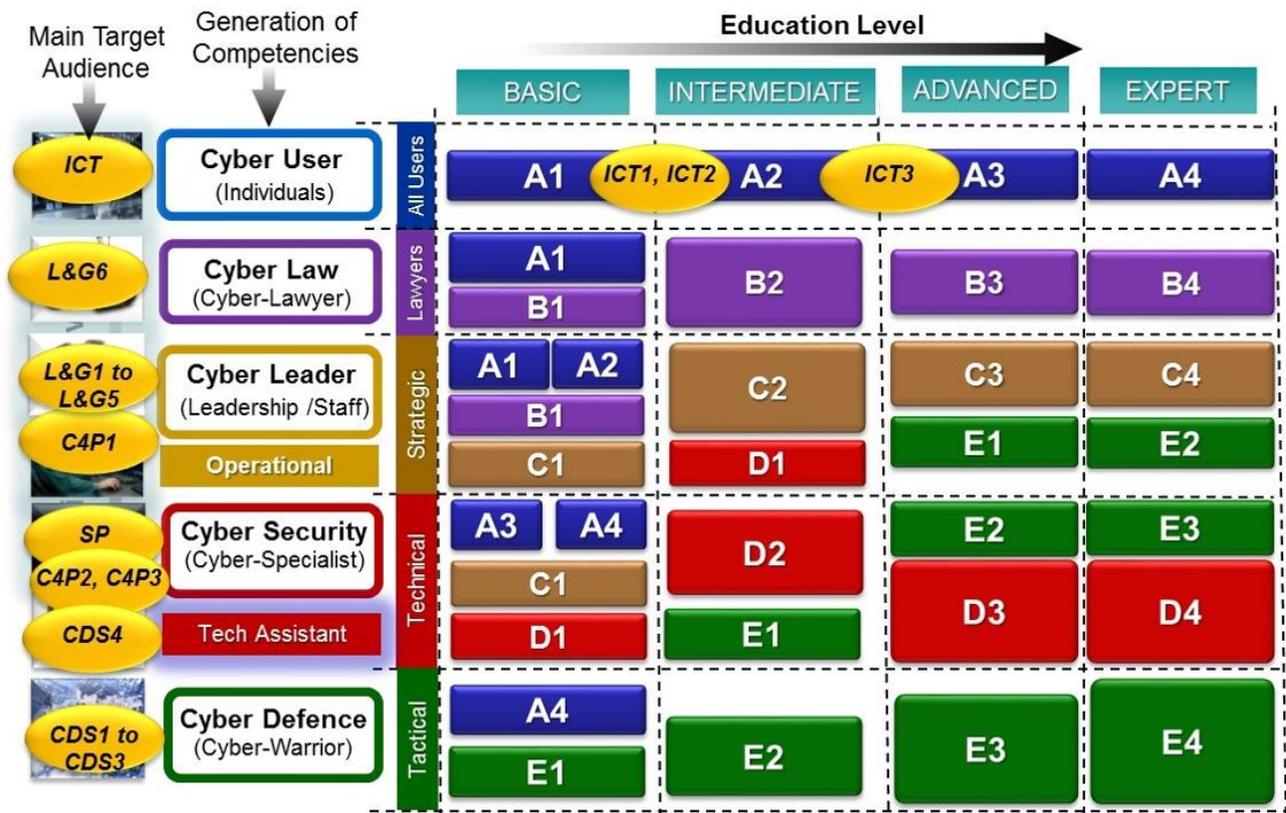


Fig. 1. Generation of competencies level in cyber defence disciplines

Following the admission to Graduation program students benefit from training with the NDU professors and internships in different organizations in the field. Considering the fact that during the three years’ study program the disciplines are gradually developed toward cyber security leadership essentials, many classes are destined hands-on activities in the framework of Cyber Defence Laboratory. In the lab, the students have the opportunity to practice their theoretical knowledge and develop their skills participating to practical exercises on network vulnerabilities, cyber threat detection, active defence and incident response or red team-blue team type of exercises. The main objective of theoretical knowledge and laboratory training is not only to learn about security, they learn about managing the security.

Along with afore mentioned program, ISCA manages a number of 13 post-graduation programs in the department fields of study, and a Master of Art program in the field of communications, IT and cyber defence.

During their study programs, students have also the opportunity to enroll third party specialized courses like Palo Alto Cyber Security Academy.

A solid research dimension grounds all previous educational programs, activities and project. Inspired by the guidelines projected in the Carol I NDU Research Strategy, research is conducted in ISCA by the heads of chair in the field of information systems, communications, intelligence and cyber defence, in the collaboration with the department researchers in the framework of department board.

Outside NDU, the research dimension is developing mainly on four main cooperation efforts:

- Centre of Excellence for Advanced Technologies in Cyber Security (coordinated by the Military Technical Academy) - training courses and exercises, research and innovation to address cyber security challenges, developing best practices and guidelines to identified cyber security solutions, solutions for protecting communication and information system, developing collaboration and information sharing between academia and industry;
- Research Center for Navy - theoretic ground for identification of risk factors in littoral areas, cyber security management policies etc.;
- Private companies which main activity lies in cyber security domain - internships, documentary stages, scientific event, research project competitions;
- Independent think tanks with focus on cyber domain - creating and developing knowledge hubs, fostering dialogue between decision makers and academia, leadership and policy projections etc.

5. Conclusion

In the cyber defence domain NATO focus formally and de facto on the doctrine, which proves to be a defensive one, as NATO does not approach the use of offensive cyber operation.

Romania, as an Alliance member directs its efforts towards acquiring capability targets in cyber defence domain, facing major common challenges of this domain:

- the gap between the rapid technologic advance and military planning process;
- the scarce of highly specialized human resources.

These challenges as well as those rising in cyberspace could find a good response in establishing a solid direction in education, training and exercises. In this respect, CAROL I NDU education and research programs are evolving same time with the NATO Cyber Defence Concept, nowadays professors and researchers grounding the standards for legal evaluation of cyberspace acts, meantime developing a cyber defence culture not only at military organization level but also for the civilian segment.

References

- [1] Yoneji Masuda, *The Information Society as Post-Industrial Society*, World Future Society, Washington D.C., 1981.
- [2] *Ibidem*, pp. 30-33.
- [3] ***, A/HRC/17/27/ - *Report of the Special Rapporteur on the promotion and protection of the right to freedom and opinion and expression, Frank LaRue*, United Nations' General Assembly, 16 May 2011, p. 7.
- [4] Stephen Tully, *A Human Right to Access the Internet? Problems and Prospects*, in *Human Rights Law Review*, Vol. 14, Issue 2, Oxford University Press, pp. 175-195.
- [5] ***, Decision no. 2009-580 of June 10th, 2009 at www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf (14.02.2017).
- [6] Sala Constitutional, *La Sala en la Prensa 2010(2011)*, p. 118 at www.poder-judicial.go.cr/sala-constitutional/documento/salaenpresa2010.pdf (14.02.2017).
- [7] Shane Harris, *Hack attack*, Foreign policy, 3 March 2014 at <http://foreignpolicy.com/2014/03/03/hack-attack/>.
- [8] Ellen Messmer, *Serb supporters sock it to NATO, US web sites*, CNN, 6 April 1999, at <http://edition.cnn.com/TECH/computing/9904/06/serbnato.idg/index.html>
- [9] NATO Computer Incident Response Capability.
- [10] Cyber Defence Management Authority.

- [11] Cyber Defence Management Board.
- [12] ***, Training Requirements Analysis Report on Military Role in Cyber Defence EU Military Training Discipline (EEAS(2019) 154 REV6), at <https://data.consilium.europa.eu/doc/document/ST-7848-2019-INIT/en/pdf>.

Brief Overview over the Converged Security at the Enterprise Level

Andrei IANCU, Mircea BORCAN

General Directorate for Communications and Information Technology,
Ministry of Internal Affairs, Romania
andrei.iancu@mai.gov.ro, mircea.borcan@mai.gov.ro

1. Introduction

As the interconnected world grows, the security risks and concerns must be treated properly with aim of avoiding any breach that could cause damages of the informatic systems. In order to follow the evolution of technology, nowadays it is needed to address the new threats which are found in the cyberspace.

The rise of attacks over the last decade emerged as an ever-growing problem that has become a fruitful criminal enterprise. One can't avoid being a target, but can develop and apply some strong security mechanisms which can minimize the risk of becoming compromised.

2. Converged security

2.1. *The vicious circle*

For a better understanding of the so called cyberspace rules it is simple to take the example of a ransomware. A ransomware is a malicious software used in a cyberattack to encrypt the victim's data with an encryption key that is known only to the attacker, thereby rendering the data unusable until a ransom payment is made by the victim. What if one targeted enterprise is infected by a malware? The organization in question often believes that the right thing to do is to pay the ransom because it seems to be the most cost-effective way. As a matter of fact, for the purpose of recovering their data, it really is the most effective way. But, the problem is that every

institution that pays is a directly funding the empire of malware development. As a result, well-intentioned institutions become the greatest sponsors of this industry.

The more money payed, the more sophisticated the attacks.

Attacks need to be detected and prevented when they are occurring and halted if they somehow reach their target.

2.2. The security artichoke

The analogy of the security artichoke states that one, in order to compromise a network (or to reach the artichoke's core), has to peel away only certain layers of leafs, not all of them. So, in theory, an attacker can chip away the leaf along the perimeter and reach the heart of the network. With a focus on security, the network administrator must use a layered approach assuring that the network will not be compromised in the unlikely case of breaking the perimeter firewall.

2.3. The perimeter firewall

With the aim of mitigating the risks, the firewall technology evolved from the classic Layer 4 firewall to the Next Generation Firewall (NGFW). The use case of a perimeter firewall is illustrated in figure 1.

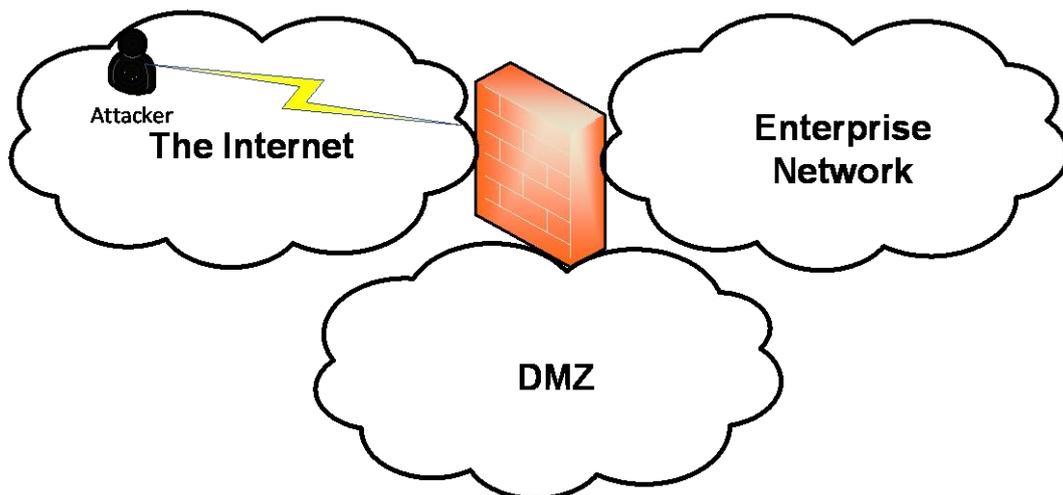


Fig. 1. The perimeter firewall

Besides the traditional capabilities of the Layer 4 firewall, like stateful packet inspection, VPN and NAT, the NGWF introduces many other features such as

application firewall using in-line deep packet inspection, encrypted traffic inspection, website and application filtering, and antivirus protection.

The goal of including these new capabilities is to provide deeper inspection in favor of checking packet content and matching signatures of malware. The NGFW also provides a granular filtering mechanism by using the app control mechanism. With this last feature, the network administrator can decide what parts of o a website to expose to the end users, filtering unwanted sections (e.g. document sharing).

Another essential role of the perimeter firewall is to enforce the security policy for the demilitarized zone (DMZ). In the DMZ is used to accommodate the services exposed to the outside zone of the organization which in most cases is the Internet.

2.4. Connecting the remote sites

Every enterprise-level company has some remote sites which need to access the central resources, so they must be connected to the network. The problem is that the company doesn't have the physical infrastructure to reach the location of each remote site. In order to connect these frontier locations, an organization has 2 approaches. The first one is to use some leased lines which can connect the sites with the headquarters. This measure assures the confidentiality and availability of the network because these lines would be used only by this particular company.

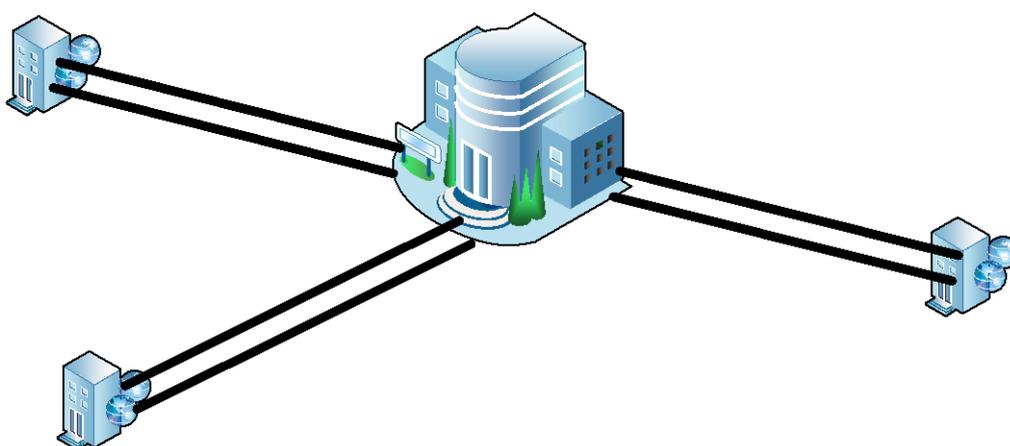


Fig. 2. Connecting remote sites - Leased Lines

The drawback of this layout is the cost. If one organization has many locations to connect, all in different geographical areas, then the payment rises exponentially.

Another issue associated with the use of leased lines is the impossibility to assure the access at the company's network for the detached workers. The solution of using leased lines is illustrated in figure 2.

The second approach used to connect the remote sites is the VPNs (Virtual Private Networks). The VPN concept breaks the limit between private and public networks. It permits the constitution of private networks over the existing public ones, such as the Internet, or the infrastructure of a Service Provider. On one hand, the implementation of VPNs introduces complexity, but on the other hand it provides mobility, as we find ourselves in the BYOD era, and also it reduces the cost. The use of VPNs assures the three elementary concepts which define the information security, which are Confidentiality, Integrity and Authentication (CIA).

The confidentiality of the information is satisfied with the use of encryption algorithms, such as AES or 3DES. One must use encryption in order to avoid the situation when a Man in The Middle (MITM) intercepts the information transmitted over the media and tries to rebuild the initial message. With the use of encryption, even though a MITM can see the packets, he cannot understand the actual content because he is not in the possession of the encryption key.

The Integrity is provided by the use of hash functions. The initial message is hashed and the result is glued to the information which needs to be transmitted. At the recipient, the new hash is computed and compared to the received one. If they are identical, the message was not corrupted on the path. If not, the message is discarded.

The authentication of the communicating parts is done by using keyed hashes. Because only the correspondents have those keys, a MITM impersonation attack cannot succeed. Even though a MITM sends a message to one correspondent claiming that he is someone else, without the key the attacker will not be authenticated by the destination and his message will be rejected.

The VPN solution is illustrated in figure 3.

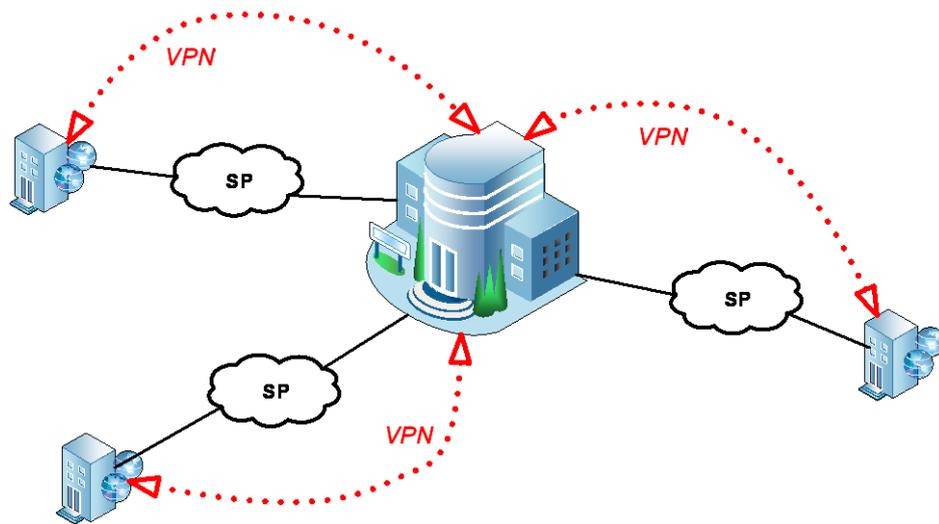


Fig. 3. Connecting remote sites - Virtual Private Network

2.5. End users - the biggest concern

The end users are the consumers of the network resources. On one hand, all the applications that are written and all the network infrastructure which is built, are means used to accommodate the end user's needs. But, on the other hand the end users are the most vulnerable and the most liable points of the network. In order to assure the converged security mechanisms for the entire network, the end users must be authenticated by the system. In addition, after being authenticated, one should not have access to all resources, but only to the ones which are specific to their activity. In other words, the users should be authorized to do certain activities. Finally, the actions of every user must be logged. This refers to the concept of accounting.

In addition to the AAA framework, the user should be postured. An end station connected to the network should have the latest antivirus signatures and up to date patches of the operating system. The posturing of an end point can be done by a centralized server. If the end point isn't compliant with the enterprise's policy, the centralized server blocks the host and triggers the update process for it. When this process is finished, the host is authenticated by the server and gains access to the network.

The implementation of such a solution makes use of 802.1x and Radius open standard protocols, as illustrated in figure 4. The switch acts as an intermediate device which has the function of passing messages between the client and the server.

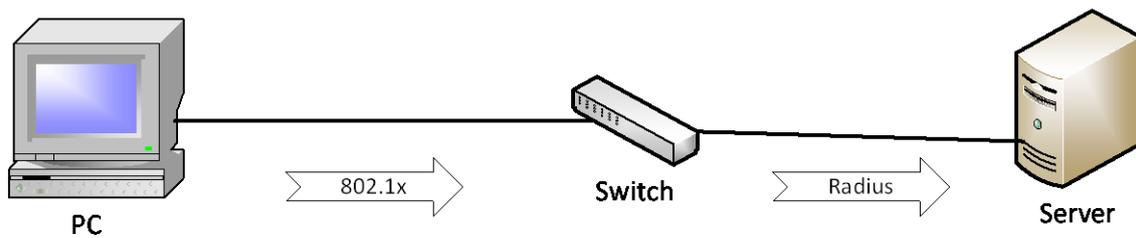


Fig. 4. Authenticating the users

In addition to implementing many security measures, an enterprise must implement an awareness training for its employees. In order to comply with the security policy of the company, on one hand, and to perceive the jeopardy of the cyberspace, on the other hand, the training programs should take place periodically and should be compulsory for all the employees.

3. Conclusions

With the purpose of minimizing the risks in nowadays global cyberspace, each company should use a layered approach. Defending the network against cyberattacks requires constant vigilance and education. Best practices concerning network security combine several activities, including: upgrading patches, stopping unnecessary services and unused ports, using strong passwords and changing them frequently.

At the enterprise level, there are many other things to look at, such as protecting the company's public resources, securing the WANs and authenticating and tracking the end-user traffic flow. It is necessary to educate employees about the risks of social engineering. Unfortunately, the most common attacks on networks are due to unskilled staff. Therefore, strategies need to be developed to validate identity by phone, email, or personally so as to avoid phishing attacks. Developing a written security policy is also a key point in educating staff.

The methods studied in this paper represent a convergent protection and network security management mechanism. Organizations need to remain vigilant at all times and defend themselves against threats that are continually evolving, developing security policies, consistent with malicious software in cyberspace.



CYBER RESILIENCE



CYBER RESILIENCE

Challenges in Cyber Resilience for Public Administration

Costel CIUCHI

Information Technology Directorate,
General Secretariat of the Government, Romania
costel.ciuchi@gov.ro

1. Introduction

Information security has become an important component of today's society, due to the nature of the data that has been given special importance in both managerial decision-making, in close connection with the operational and development strategy of the organization, and in relation with the other organizations. Ensuring information security has become a central area within the organization, applying to all organizational levels, being one of the main activities for decision-makers regarding the organizational environment. Terms such as information security, computer security and data security are interdependent and often share the common objectives of protecting confidentiality, integrity and availability of information. However, there are differences between the above terms, differences that start from the way the subject is being approached, the methodologies used, and the scope of application.

The particular importance of communications networks and services developed over the past decade can also be seen in government policies adopted at the state level in a first phase by cataloguing critical infrastructures according to their importance in blocking workflows of the administration. Depending on the threats that may cause service shortages, steps need to be taken to ensure an acceptable level of performance and security of services, in the event of failures or challenges to normal operation [1].

Thus, a set of concepts and attributes have been developed that characterize the new functional requirements of the systems, with possible models and methods of

implementation or measurement. Along the time, two features have been highlighted as being of great importance for systems: the resilience and survival capabilities [2].

Resilience is the inherent capacity of a system to adjust its operation before, during or as a result of internal or external changes and imbalances so that it can secure and perform the operations for which it was designed under both expected and/or unexpected work conditions (resilience = shock-resistance) [3].

Given the role and importance they have gained in the well-functioning of society, it is recognized that most of the services, applications and communications networks currently used are not resilient, trustworthy and safe to operate/use so that to ensure continuity and a certain level of quality during operation at an acceptable level [4], [5]. Developing new ways to provide network and/or application resilience and survival capabilities require an understanding of threats, vulnerabilities and audit methods, as well as developing alternative proposals on increasing adaptive capabilities in different situations (foreseen or unforeseen).

2. General aspects concerning the concept of resilience (& cyber-resilience)

The field of IT security has made valuable contributions to the protection and integrity of information systems over the last three decades. However, computer security has traditionally been used as a binary term that suggests at any time whether a system is safe or compromised. Such a use of the concept generates approaches that largely overlook the possibility of recovering a system after a subversive action as well as aspects of maintenance services during and after an intrusion.

This approach is not appropriate to support efforts to improve practices in the field of IT systems protection in front of attacks, even if it is done sequentially and/or in detail. Since its inception, the concept of resilience has immediately captured the attention of industry and academia through the opportunities and challenges of putting it into practice. Thus, four essential attributes have been identified for a system to be resilient, namely:

- respond to what is happening;
- monitor critical developments;

- anticipate threats and opportunities;
- learn from experience - from success, but especially from failures.

The attributes related to the concept of resilience are represented in particular by quality assurance modelling and analysis that sums up the confidence level that can be attributed to a service provided by a system (reliability and availability [6], performance [7] and survival [8]).

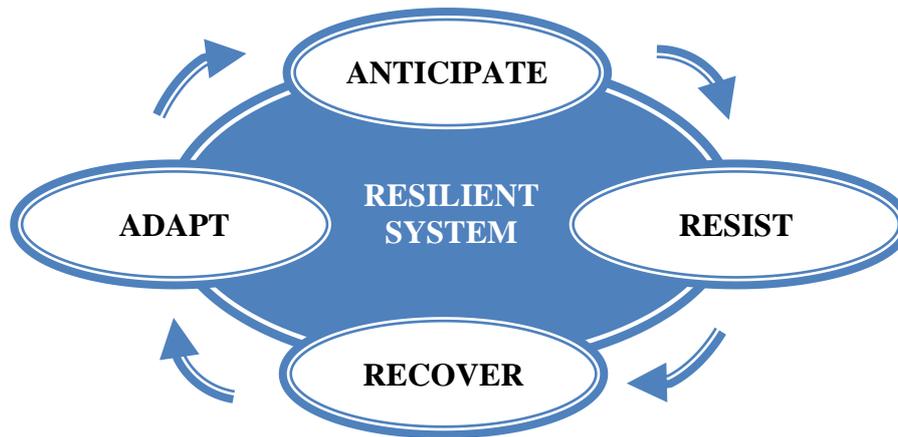


Fig. 1. Objectives of a resilient system

Also, a particular interest is represented by the way resilience is related to other concepts in the field of quality assurance, such as security, reliability, availability, fault tolerance, recovery, etc. Among the fundamental aspects of quality assurance in information systems, **fault tolerance and redundancy** are the most used, concerning resilience. Availability and performance are mandatory requirements for all systems, but security strategies need to be introduced to respond quickly to threats so that they can minimize damage and can continue to work optimally during and/or after a cyber attack.

Fault tolerance is the statistical probability of an accidental failure or a combination of failures and does not address malicious attack actions. For example, an analysis of a system may cause the simultaneous occurrence of two statistically independent defects (F1 and F2) will cause the system to fail. The probability of occurrence of the two independent defects simultaneously, incidentally, may be extremely low, but an intelligent adversary with knowledge of the internal structure of

the system can arrange for the simultaneous appearance of these two defects, generating the system's failure.

Redundancy is another factor that can contribute to system resilience. However, redundancy alone is not enough, because multiple spare systems have similar vulnerabilities. A resilient system requires each spare system to provide an equivalent version of operation but with a fundamentally different applicability. This approach hinders attempts to compromise the base system and all backup systems with a single attack strategy.

Another aspect of the concept of resilience is **multidimensionality**. Any system has three dimensions that need to be considered - people, processes and technology. To build a resilient system, all these dimensions must be considered, otherwise if one fails, then the system has a low probability of survival and there is an increased possibility of occurrence of errors within a system.

Despite efforts to ensure the quality and security of systems, security teams continue to identify up to two-thirds of all attempts to breach computer security measures. With more and more diversified cyber attacks and global deployment, with virtual space offenders using increasingly sophisticated tools (such as the ransomware-as-a-service and DDoS-for-Hire²) and the opportunity to capitalize on these efforts with cryptocurrency is the ideal context in which ensuring system resilience becomes a requirement for any system.

Cyber resilience is the ability to predict, resist recovery and adapt to adverse operating conditions, cyber-attacks, or attacks designed to compromise computer systems. [9] The objective of cyber resilience is to obtain the development of trust systems that are fully capable of backing the support operations for which they were developed while protecting the components of the system at a level of assurance compatible with its risk tolerance. Besides, cyber-resilience is motivated by mission assurance (attaining the goals for which it was developed) and anticipating attacks from intelligent, sophisticated and strongly motivated opponents. It also focuses on the functioning of organizational capabilities and the fulfilment of critical or essential missions despite the possible presence of an adversary in the infrastructure.

However, ensuring cyber resilience implies an approach of an advanced persistent (APT) concealed, evolutionary threat that is capable of discovering (and sometimes even generating) new vulnerabilities. In dealing with advanced cyber threats - persistent, there is a need to develop techniques and procedures based on two fundamental working hypotheses:

- a sophisticated attacker can not be detected quickly or can be quickly removed from the system despite the implemented security measures/solutions and/or the quality of the system implementation process;
- the presence of an adversary in the system can be a persistent, long-term problem, and assumes that the hidden nature of an APT threat hinders the eradication process and the certainty that the error has been removed. The approach regarding the ability of an APT-type threat to adapt involves the certainty that the methods that proved successful in the past, can no longer be effective.

3. The current state of the framework for resilience in Romania and Europe

The capacity to provide critical services for the proper functioning of public administration in the context of disruptions to accidental service operations (disasters, human errors) or following malicious actions (sabotage, coordinated attacks at local, regional or state level); has become a worldwide concern. Technological development and automation of the administrative workflows over the recent decades have highlighted the need to integrate new approaches in the systems development stages that require the integration ever since the design stage of approaches of the "security by design", "interoperable by design" type etc.

In Romania, through GD no. 768/2016 [10], the concept of resilience is defined as "the ability of a system, community, or society exposed to a type of risk to cope, adapt and recover after a disaster by maintaining and rehabilitating its essential structures and functions." The normative act defines the legal and organizational framework regarding the achievement of the objectives of the United Nations (UN) International Strategy for Disaster Reduction as well as the policies and programs

developed at the level of the European Union, NATO and other international bodies and organizations.

Also, "Romania's National Strategy for Sustainable Development 2030" [11], Romania sets its national framework for supporting the 2030 Agenda on three main pillars (economic, social and environmental) as well as a set of 17 sustainable development objectives. The concept of resilience is the main vector of development for the three pillars. The development of "resilient infrastructure", "resilient cities", the cultivation of capabilities to ensure the "citizens resilience", "resilience to climate change and natural disasters" are necessary to attain the sustainability goals for a modern society.

The European Union's cybersecurity strategy, adopted in 2013, defines a set of strategic objectives and concrete actions to be taken by Member States to ensure the resilience of systems:

- developing cyber defense capabilities;
- reducing cybercrime;
- adoption of international policy on cyberspace.

In this respect, measures have been taken at European level to ensure resilience and a high degree of cybersecurity preparedness through the development of legislation and activities in the field of critical infrastructures. Process modelling and accelerated development of systems with a critical role in the well-functioning of vital components of society have led to the adoption of Directive (EU) 1148/2016 (NIS) [12] on measures to achieve a high level of security of networks and information systems. The NIS Directive (Directive on Security of Network and Information Systems) is the first pan-European cybersecurity legislation and it focuses on strengthening cyber authorities at a national level, increasing coordination between them and introducing security requirements for key industry sectors. (energy, transport, banking, health, supply and distribution of drinking water, digital infrastructure).

The Action Plan on the Protection of Critical Information Infrastructure at European level is built around five pillars:

- training and prevention;

- detection and response;
- risk mitigation and recovery after incidents; (here resilience is included too)
- criteria for classifying critical infrastructures in the ICT sector;
- international cooperation.

Article 9 - IT security incident response teams ("CSIRT teams") of the NIS Directive explicitly addresses the Member States' obligation to "ensure that CSIRT teams have access to adequate, safe and resilient communication and information infrastructure at a national level."

Another important aspect of developing an action plan on protection is risk awareness, followed by the development of specific analyzes to combat critical threats to the system. Identifying potential threats and determining their impact on information systems can be achieved by using risk measurement techniques and methodologies. The development of cyber resilience assessment methodologies performs risk modelling by establishing meanings in line with the impact it may have on the system and the modalities of recovery after an incident has occurred.

4. Development of a resilient decisional eco-system at the level of public administration

In the context of the current ever-changing society, global communications, high-speed connections available to most categories of users, and the unprecedented development of software applications and programs, data security has become a major concern. Modern managerial decision-making requires access to large volumes of information and a distributed workflow.

Transmitting data between a broadcaster and a recipient using the Internet network can transit through several communications networks to make the transfer, giving users in the networks whereby data traverses the possibility of intercepting and/or modifying them. Also, through unauthorized access to system resources, users within the network where the broadcaster and/or recipient are located can modify and/or destroy data and information. For an organization, from an operational point of view, the use of information systems requires the provision of a secure and resilient

environment, becoming practically an intense and continuous concern over the possible risks and threats. Due to the high frequency of incidents and the diversity of existing vulnerabilities, an important aspect to be developed in the systems support for decision making is cyber-resilience.

At Government level, tactical decision-making systems are used to make a decision due to the purpose and nature of the activities for which they were developed. **Tactical systems** (also called management systems) [13] are related to the activities performed by decision-makers at the organization's operational level, activities such as short and medium-term planning, organizing and controlling. With a broad scope, the managerial IT systems provide information to support decision-making and have the following objectives:

1. predefined and planned reports - made by information reporting systems;
2. Interactive and ad-hoc support for decision making by managers - made by decision support systems;
3. important information for top management - provided by executive systems.

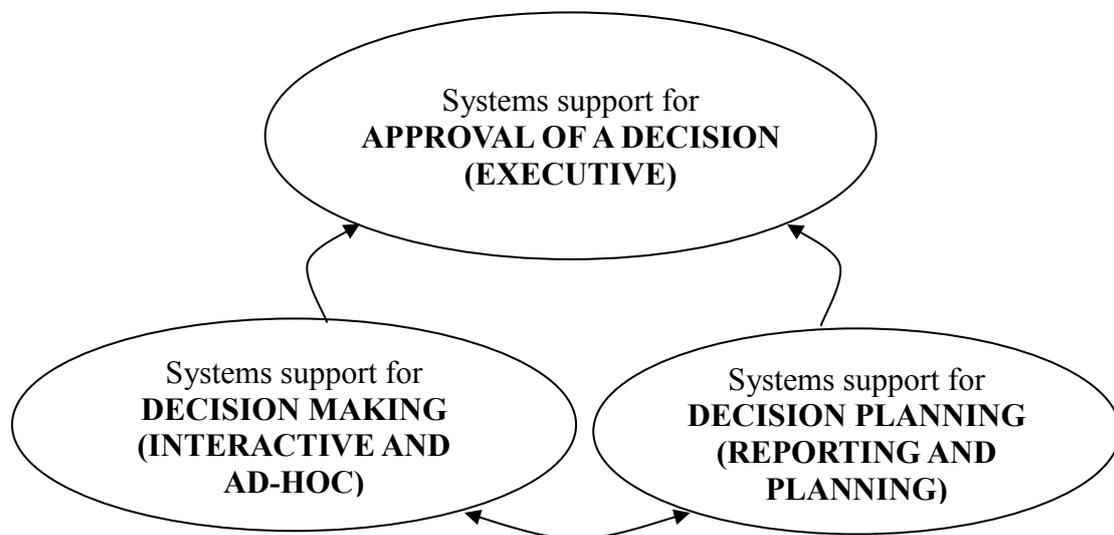


Fig. 2. Government decision - making model

The quality of the ruling act is closely related and depends on the quality, the accuracy of the decisions made at the decision-making level. Thus, keeping services at the optimum level, introducing new analysis instruments coupled with the adoption of

the best decisions implies access to a large amount of data and information, as well as a complex process of modelling and analysis.

Within complex government systems, the ability to collect, process, and analyze data/information needed for decision-making (the human factor) and a large amount of data to be processed over a small timeframe, often exceed the possibilities for immediate analysis. To overcome these limits in the decision-making process, automated means of modelling and information technology are used to support the decision.

Government decision modelling involves the use of support IT systems that require the data/information (sectoral)collection from diversified sources as structure and complexity. Centralization and normalization of data require in most cases the exposure of systems in the Internet environment.

To ensure the security of such systems, it is necessary to ensure cyber resilience given the importance of such support systems for decision -making.

The need for secure access is the central concern, but there are other attributes to be taken into account, such as the availability of services in case of adverse events, the correctness of the collected data and the conclusions of their analysis. The extension of the cyber resilience attributes needed to be considered in cybersecurity audit of government support systems requires the adoption of new measures and development directions such as:

- **legislative measures by defining a national framework on cyber-resilience;**
- **strategic cooperation** through the exchange of relevant information, **capitalizing on the mechanisms** of "cooperation groups" between states and **strengthening coordination in situations where rapid interventions are needed;**
- **enhanced resilience and response capabilities** by strengthening and optimizing co-operation between all **entities** involved (governmental, private or academic) through training and education cybersecurity mechanisms;

- **simplified approaches in assessing cyber incident management** (with focus on operational level) by optimizing the cooperative process to identify and mitigate the impact of incidents;
- **development of cyber-security public policies** [14] that take into account the need for cyber resilience to ensure that the products, systems and services they need, which they intend to provide or have already been implemented, can survive when facing various types of threats;
- **an organized framework for costs and investment** in the field of cyber-resilience at the level of the administration through public policies;
- **developing education/research hubs** between public administration, academia and the private environment to develop resilience by adopting work patterns in line with system requirements.

5. Romanian Presidency of the Council of the European Union

In the context of holding the presidency of the Council of the European Union in the first half of 2019, Romania was at the center of European decision-making process, playing an important role in fostering the development and consolidation of the European project, the negotiation process for the development of the *acquis communautaire*, implicitly, for cooperation between the Member States of the Union [15]. The exercise of the EU Council Presidency represented an opportunity to contribute directly to the good progress of the European project by organizing numerous events (high-level informal meetings, conferences and seminars at ministerial level or at the level of Heads of the Agency, senior officials and experts, with wide external visibility).

In this respect, a series of measures have been adopted at the state level to ensure a high level of performance and availability for governmental systems involved in decision-making with the EU institutions and the Member States. Based on the experience of other Member States holding the Presidency of the EU Council and the Action Plan, a series of actions have been taken by adopting a set of technical and

organizational measures to ensure the resilience of services and information systems through:

- exercises and simulations to anticipate accidental interruptions and cyber attacks on essential organizational services (government applications, e-mail, web sites, etc.);
- testing systems by work scenarios under local service disruption conditions, as well as in the absence of essential services from ISPs;
- adopting possible scenarios on the possibilities of system recovery and the continuation of the mission for which they were implemented;
- developing adaptability capabilities for systems through quick and secure updates.

To ensure high cyber resilience, another important dimension was the human resource with roles in the use and/or administration of systems and applications. Thus, at the organizational level, actions were carried out:

- training decision-makers, operating staff and staff involved in managing working groups and organizing meetings with the Member States;
- awareness, prevention and education in the field of cybersecurity at the level of the institutions.

Another important aspect was to intensify cooperation with designated national authorities by:

- updating work procedures and setting up real time communication and information channels on cyber incidents;
- sending alerts and notifications to identify possible attacks on services and systems.

The exercise of the Presidency of the Council of the European Union represented a good opportunity for Romanian public administration to develop, test and update the institutional capabilities of protection and response. It was also a good time to strengthen operational cooperation, validate mechanisms and adopt new ways of managing cyber crises at institutional level.

6. Conclusions and perspectives

The threats specific to the information systems are characterized by an increased dynamics and a global character, which make them difficult to identify and counteract. Cyber threats have known explosive diversification lately, some of which can be classified as global epidemics due to the high speed of spreading in the virtual environment. Over the past years, specialists in the field noticed an increase in attacks and a higher degree of sophistication of deployment modalities.

Developing an organizational culture of cyber resilience by updating and developing work mechanisms associated with a system can ensure the implementation of proactive elements with impact on all components of a resilient system (human resource, processes, technology).

From the point of view of cybersecurity management, it is a new approach by taking over the initiative and adding new directions to the objectives of a system (anticipation, resistance, recovery, adaptation) by:

- **anticipation** - development of strategies for detection of attacks and damage assessment through continuous professional training, awareness and cooperation;
- **resistance** - Implementing capabilities for systems to reject attacks by diversifying technology and defense mechanisms on levels;
- **recovery** - adoption of operational procedures / measures to maintain essential services and components during an attack, limit damage and complete restoration of the functional capacity of services;
- **adaptation** - to the new threats that occur in the virtual space not only from a technical point of view, but also from the point of view of system administration through education, public policies, public-private partnerships, cooperation).

Flow and process modelling, coupled with consistent cybersecurity management policies, are activities that need to be included in the implementation of the systems. The introduction starting with the design phase, of the basic principles of the concept

of resilience will ensure the smooth running and management of the mission for which a system has been developed.

Cyber resilience is one of the basic attributes needed to be developed in all organizations by introducing it into cyber security objectives. Operationalization perspectives require a strategic approach based on the modeling of cyber security management at the organizational level, and explaining how an organization can build, evaluate, and maintain cyber resistance.

References

- [1] C. Nemeth, M. Nunnally, M. O'Connor, and R. Cook, "Creating Resilient IT: How the Sign-Out Sheet Shows Clinicians Make Healthcare Work", *AMIA Annual Symp. Proc.* 2006. 2006:584-588.
- [2] J. P. G. Sterbenz, D. Hutchison, E. K. Cetinkaya, A. Jabbar, J. P., Rohrer, M. Scholler, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines", *Computer Networks*, vol. 54, no. 8, pp. 1245-1265, June 2010.
- [3] E. Hollnagel, D. Woods, and N. Leveson, "Resilience Engineering: Concepts and Precepts", Aldershot UK: Ashgate, 2006.
- [4] F. Schneider, "Trust in Cyberspace", National Academies Press, 1999.
- [5] S. Goodman and H. Lin, "Toward a Safer and More Secure Cyberspace", National Academies Press, 2007.
- [6] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", *IEEE Trans. On Dependable and Secure Computing*, vol. 1, no. 1, pp. 11-33, 2004.
- [7] J. Meyer, "On Evaluating the Performability of Degradable Computing Systems", *IEEE Trans. on Comp.*, vol. 100, no. 29, pp. 720-731, 1980.
- [8] R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. A. Longstaff, and N. R. Mead, "Survivable Network Systems: An Emerging Discipline", Carnegie-Mellon Software Engineering Institute Technical Report CMU/SEI-97-TR-013, 1997 revised 1999.

- [9] NIST Special Publication 800-160, Volume 2, Systems Security Engineering, Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, October 2018.
- [10] Decision no. 768/2016 on the organization and operation of the National Disaster Risk Reduction Platform.
- [11] <http://dezvoltaredurabila.gov.ro/web/obiective/>.
- [12] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to achieve a high level of security of networks and information systems in the Union, Official Journal of the European Union, 19 July 2016.
- [13] E. Turban, E. McLean, J. Wetherbe, "Information Technology for Management", John Wiley & Sons, New York, 1996.
- [14] I.C. Mihai (Coordinator), C. Ciuchi, G. Petrică, "Current challenges in the field of cybersecurity - the impact and Romania's contribution to the field," European Institute of Romania, Bucharest, 2018.
- [15] Memorandum - Action Plan to Prepare the Presidency of Romania to the EU Council in the First Semester, 2019, <http://gov.ro/>.

Cyber Resilience for the Special Telecommunications Services and Systems from CERT/CSIRT Perspective

Andrei-Sorin JERCA, Alexandru OZARCHEVICI
CORIS-STIS, the Special Telecommunications Service, Romania
andrei.jerca@sts.ro, alexandru.ozarchevici@sts.ro

1. Introduction

In a world that has more cyber security threats than ever and where new challenges arise every day, cyber security experts must be prepared to be one-step ahead of the attacker and act immediately in case of an incident.

Cyber security covers all the technologies, processes and measures used for designing and protecting an infrastructure consisting in internal systems, networks and assets from intrusions and a wide range of possible attacks. All of these security threats can disrupt the normal activity of different entities and organizations and can generate long-term impact on hardware and software components, major economic losses or public image damage.

Complementary, the cyber resilience is a relatively new field of action, focused on risk mitigation and accommodation to a changing environment where the attackers have the advantage of element of surprise, even if it is about new innovative attacks and techniques that might be successful in creating disruptions.

The term "resilience" represents the ability to prepare for, to evolve to changing conditions, to withstand and recover rapidly from disruptions; it includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents [1].

To create cyber resilience, every organization, must identify their current cyber risks and develop strategies and services that aim to strengthen the infrastructure and security processes, before the detection of any security incident or event. The main

objectives are to be more agile on handling attacks, to avoid incidents and to decrease the impact surface in case of occurrence.

At national level, some systems and assets, whether physical or virtual, are defined as critical infrastructures and they are standing out by their importance being vital on public health, safety, security or economy and any disruption or destruction would have a significant impact at national level as a result of the failure to maintain their functions [2].

In this context, the Special Telecommunications Service is the public authority responsible with critical telecommunications infrastructures under its administration, related to “IT&C” and “National Security” sectors, according to current legislation [2].

Penetration, disruption and destruction of special telecommunications networks, as well as the interception of communications in these networks are threats to national security [2].

The critical infrastructures categories operated by Special Telecommunications Service include information technology and communication infrastructures, data centers, computer systems and services, 112 emergency service and services provided by special networks and cooperation networks.

Furthermore, the Operational Response Centre for Security Incidents (CORIS-STIS) is the CERT (Computer Emergency Response Team) entity designated to prevent and respond to security incidents related to information and communications systems owned by Special Telecommunications Service or by its clients.

2. Cyber Resilience and Critical infrastructures

In order to protect and increase cyber security resilience for the managed infrastructures, Special Telecommunications Service implemented a thoughtful security strategy that aims to minimize the risk of cyber security incidents or events, ensuring a high-level of protection and confidentiality.

At CERT level, the cyber security and resilience strategy is in fact a framework based on several steps, organized in a multi-layered approach that encompassed people, processes and technology [3] based on NIST Framework [4].

The framework consists of five concurrent and continuous functions, generically defined as Identify, Protect, Detect, Respond and Recover. This approach has the advantage to overcome the traditional security measures that are failing to deliver the expected results.

The **identify** function consists in thoroughly understanding the organization cyber security risks, implementing policies and procedures, staying focused and prioritizing the efforts in accordance to current organizational cyber security risk management strategy.

First step consists in auditing IT&C infrastructure, which requires hardware, software and data communications configurations assessment, designation of cyber security roles and responsibilities, vulnerabilities scanning and assessments, penetration testing on owned systems and networks.

Next step focuses on design and implementation of cyber security policies and procedures in concordance with National and European legal and regulatory requirements in the IT&C field. In the same time, it is very important to define and implement the right response and recovery plans and strategies.

Complementary, a best practice type assessment, based on interviews with staff, network administrators, system or security administrators, determines whether the methods and workflows comply with security policies and other security standards [2].

Furthermore, the threat intelligence services and tools play an important role in understanding the threat landscape as a whole and helps the organization to proactively predict and strengthen the infrastructure and the ongoing security processes. The main objectives are to avoid incidents and to decrease the impact surface in case of an occurrence.

The **protect** function is about developing and implementing safeguards for critical infrastructures and services in order to detect an intrusion, limit the impact of an attack and mitigate the risk [3].

At this stage, security services associated to special telecommunications and cooperation services must guarantee the confidentiality, integrity and availability of information. Here, the implementation of authentication, authorization and access

control systems including network segregation and segmentation, remote access and device policies are mandatory.

In particular, the focus is on protecting networks and websites that are publicly available over the Internet and on protecting organizations endpoints, gateways and online users from targeted attacks and advanced persistent threats.

In the same context, cyber security training and awareness programs are used to provide information through seminars, workshops, courses and documentation so internal users and clients can protect, detect, report and respond to a security incident and perform their cyber security related duties and responsibilities.

Finally, the information protection processes and procedures must be in place, managed and tested, including backups of systems, response and recovery plans, vulnerability management and information and communication systems checking and updating procedures.

The **detect** phase provides the necessary activities to rapidly identify an attack, assess the system that is being targeted and provides a timely incident response. Another function of this phase consists in continuous monitoring of network and applications events for potential attacks or breaches, with an emphasis on the network border of the organization.

These days, the status of being constantly informed of global threat landscape is a necessity and is achieved by continuous monitoring of endpoint activity, accessed data and login information. The biggest challenge in this phase is to correlate the events from internal network of the organization with external threats and evaluate the amount of gathered and analyzed information. At this point, the use of Big data and analytic tools is a necessity.

A proactive CERT/CSIRT department that has data-level visibility across the whole environment and respond to attacks, which become more advanced, can increase the cyber resilience of the organization [3].

The **respond** function involves all the required actions and activities that must be in place, in order to mitigate the impact of a potential cybersecurity incident as soon

as possible. Usually, this phase is executed by the CERT/CSIRT department within the organization, in cooperation with internal or external stakeholders.

The first step in the response function is *initial notification of security incident* generated using automated detection systems, the results of internal monitoring and research activities or external notices, followed by a *primary evaluation* where notifications are investigated and prioritized according to severity and then a case is opened. An incident is evaluated using one of the following priorities: urgent, high, medium and low.

In the next step, a *detailed analysis* is conducted to establish the impact of the incident, the advanced forensics are performed, and the current case information about the incident is enriched with additional details, such as time and source of attack, type of vulnerability, affected system, known sensitive data compromised and primary mitigation measures.

Based on available case information, *mitigation, notification and escalation activities* must be performed in order to prevent expansion of the event and resolve the incident as fast as possible [4]. These activities should be executed according to the identified level of priority and impact. Each affected internal division or external client is notified about the incident. In the same time, all in place procedures and response strategies should be updated.

After all mitigation activities are finished, the incident is *closed*.

The final step is the **recovery**. This stage is composed by all the activities, processes and procedures needed to restore any data and services that may have been impacted during an incident. Depending on the incident type, the recovery phase is executed during or after the incident. Furthermore, recovery plans need to be updated regularly, incorporating all the lessons learned during the past incidents and improve all the risk-related aspects as long as new threats appear quite often.

3. Romanian Presidency of the Council of the European Union

The Special Telecommunications Service provided cyber security services for the protection of communications infrastructure and information technology services

used during the activities and events in the context of the Romanian Presidency of the Council of the European Union, between January and June 2019. The same measures were implemented for the Informal Summit of Heads of State or Government of the European Union, which took place on 9th of May, in Sibiu, Sibiu County.

The implemented measures were defensive and guaranteed a high level of cyber security and resilience and ensured confidentiality, integrity and availability of information and communications.

The Internet connections and related services, in the locations, where the specific events and activities took place, were enforced by strict cyber security policies and a high degree of availability was ensured for all applications used to manage the events and for information cooperation systems used by all the organizations involved in the activities. Security audits were performed, including penetration tests against the IT&C infrastructure, best practice type assessments and specific technical configurations were implemented at infrastructure level and applications servers.

The management of cybersecurity events was performed using monitoring tools for all the components of the infrastructure, including the main portal of the Romanian Presidency of the Council of the European Union, www.romania2019.eu.

Another active measure was the management of cyber security incidents and vulnerabilities, along with the setup and implementation of risk-assessment plans and procedures.

During this period, specialized personnel provided dedicated technical support, and so every moment it was possible to take immediate action for preventing, fixing, warning and alerting of any potential cyber security threat, vulnerability, event or incident. This important event was an opportunity for our institution to test and verify all the cyber security and resilience capabilities.

4. Future directions and conclusions

To increase cyber resilience and strengthen cyber security, every organization must be prepared to learn continuously, accept the changes and stay in line with latest technology trends.

The cyber security awareness, education and training are important activities to improve the general security climate of an organization. Here, we can use the acquired experience in handling the security incidents, along with the guidance concerning the best security practices to help the organization to update the security policies and better identify new opportunities for increasing the awareness on cyber security matters and prevention measures.

In recent years, terms like Artificial Intelligence, Machine Learning, Deep Learning or Neuro-Linguistic Programming have been in the spotlight and almost any new cyber security solution implements algorithms and techniques to automate and improve the detection, aggregation and response actions to imminent threats.

The applications of artificial intelligence in the cyber security field could be more and more extensive as technology evolves and so far, the main identified directions are:

- protection of national critical infrastructures, including special telecommunications services and applications provided over the Internet;
- integration, correlation and enhancement of information and alerts across networks by centralized management of cyber security policy violations;
- improvement of cyber security incident response and investigation capabilities in case of attack, ensuring interoperability and the shortest possible reaction time for decision-making.

Artificial intelligence based tools can act autonomously and block advanced cyber-attacks in a short time without the need for human factor intervention. Examples include spam filters, image filters, malware detection, homomorphic cryptography, hate speech recognition and fake news detection.

All solutions and techniques based on artificial intelligence are important in the context of new cyber security attacks, both at national and international level.

Artificial intelligence solutions for cyber security events detection allow the decrease of human resource involvement, eliminate the possibility of human manual processing errors and considerably decrease response time to security incidents.

Nowadays, the resilience is an important pillar for every organization and the winning strategy is not only about reacting to present attacks but also anticipating future threats [5].

Cyber security has no geographic boundaries, and organizations need to be prepared to accept the new challenges in the field of cyber security and look into the future focusing on new technologies.

References

- [1] Presidential Policy Directive -- Critical Infrastructure Security and/PPD-21, The White House, USA, February 2013 [Online]. Available: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>. [Accessed May 10, 2019].
- [2] Official website of the Special Telecommunications Service [Online]. Available: <https://www.sts.ro/en/>. [Accessed May 10, 2019].
- [3] White Paper: The Cyber Resilience Blueprint: A New Perspective on Security, Symantec, 2014.
- [4] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, USA, April 16, 2018. [online document] Available: NIST website, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>. [Accessed May 05, 2019].
- [5] Nelson Santini, “The Art of War: A cybersecurity take”, October, 2016 [Online]. Available: <https://www.envistacom.com/art-war-cybersecurity-take/>. [Accessed May 20, 2019].



CYBER CRIME



CYBER CRIME

Romanian Law Enforcement Involvement in Fighting Cyber Crime

Ioan-Cosmin MIHAI¹, Cătălin ZETU²

¹ “Al. I. Cuza” Police Academy, cosmin.mihai@academiadepolitie.ro

² The Romanian Police, catalin.zetu@politiaromana.ro

1. Introduction

Nowadays there are various legislative and technological developments in the field of cybersecurity, such as the General Data Protection Regulation (GDPR), the Network and Information Security (NIS) Directive and the 5G technology. All these developments are making a positive impact and create excellent opportunities, but they will affect the investigation of the cybercrime phenomenon. This underlines the need for law enforcement to closely cooperate with policy makers, legislators and ICT companies, in order to foster a safer cyber environment.

2. The challenges for international cybercrime investigations

The level of digitalization is increasing every day and so is the cybercrime phenomenon, and that's why the law enforcement and prosecution practitioners must adapt their tools and methods to respond to all the changes.

The current challenges for international cybercrime investigations can be grouped into five areas:

- *Loss of data*: the possibility of obtaining electronic data, vital for successful investigations, has been significantly limited;
- *Loss of location*: it is very difficult to establish the physical location of the perpetrators, the infrastructure or electronic evidence;
- *Different national legal frameworks*: the differences in legal frameworks often proves to be an impediment to international investigations;

- *Obstacles to international cooperation*: there is a need for better mechanisms for cross-border communication and a fast exchange of information;
- *Challenges of public-private partnerships*: there are no standardized rules for establishing public-private partnerships [1,2].

3. The current threats in the field of cybercrime

The number of threats in the cyberspace continues to increase, while law enforcement has to battle against innovative and persistent forms of cybercrime. The most important threats in the field of cybercrime are financially motivated malware attacks, the Distributed-Denial-of-Service attacks, the production of Child Sexual Exploitation Material, Skimming and card-not-present frauds, and the Darknet markets.

3.1. Financially motivated malware attacks

The main forms of malware that affect the computer systems all around the world, in financial attacks, are *ransomwares*, *banking Trojans* and *cryptojacking*.

The ransomware represents the top malware threat in both law enforcement and industry reporting [3]. Ransomware is a type of malware that restricts access to the computer system or infected files and requires a ransom to remove the restriction. Some types of ransomware encrypt data on the system's hard drive, while others may simply block the computer system and display messages to convince the user to pay [4].

Even as the rate of ransomware attacks begins to decrease, cybercriminals continue to use them in the financially motivated malware attacks. The most commonly reported ransomware families are *Cerber*, *Cryptolocker*, *Crysis*, *Curve-Tor-Bitcoin Locker (CTB-Locker)*, *Dharma* and *Locky* [3]. Most ransomware attacks are untargeted, but there are some cases where the reports showed that some attack campaigns are tailored to specific companies or individuals, suggesting professional attacks.

Banking Trojans continue to represent prominent malware threats to banks and financial institutions. A banking Trojan is a piece of malware designed to get financial or confidential information stored or processed through online banking systems. [4]

To develop this malware, cybercriminals must make significant social engineering efforts to develop custom-made phishing emails or web injection in order to adapt their cyber-attacks [3]. In case of a successful operation, the cybercriminals can monetize the stolen information or cash out the compromised accounts or payment cards, which may require employing third parties for the laundering process. That's why, a new form of malware – cryptojacking – is in the rise, thanks to its easier process of development.

Cryptojacking refers to any set of actions that uses the processing power or bandwidth of a device to mine cryptocurrencies without the user's permission [4]. The cybercriminals need a script running within an infected website that will use the visitors' processing power to mine cryptocurrencies. The industry reporting underlines an explosion in the volume of cryptominers [3], especially because the damages to victims are usually hard to quantify and difficult to investigate.

3.2. The Distributed-Denial-of-Service (DDoS) attacks

The Distributed Denial of Service (DDoS) attacks are one of the most commonly reported cyber-attacks. DDoS attacks have the effect of compromising the operation of certain Internet services. One of the most common DDoS attacks is the flood packet attack whereby a large number of packets is sent to the victim's system with the goal of blocking open connections and overloading network traffic, leading to interruption of services offered by the target system [4].

Cybercriminals continue to use these attacks as a tool against private business and public sector, not only for financial gains but also for ideological, political or malicious reasons [3]. DDoS attacks have started being used to target critical infrastructures from different countries.

Because Cybercrime-as-a-Service offers a lot of malware and tools for cyber-attacks in the Darknet markets, DDoS attacks have become more accessible, low-cost and low-risk. Within the future 5G networks, the number of the interconnected devices will increase exponentially and, if many of these are compromised, DDoS attacks will be even stronger.

3.3. The production of Child Sexual Exploitation Material (CSEM)

Child Sexual Exploitation Materials (CSEM) refers to the sexual abuse of a persons below the age of 18, as well as to the production of images and videos of such abuse and the sharing online through Peer-to-Peer (P2P) platforms and Darknet markets. Online Child Sexual Exploitation Material is constantly evolving due to technology changes. Growing Internet coverage, mobile connectivity, the development of streaming solutions, the popularity of social media platforms, the Darknet markets that provide a high degree of anonymity, all serve to amplify the trend in the commerce of child sexual abuse.

The investigation process of these cases is difficult and complex, due to the technologies and jurisdictions involved. The great level of anonymity and the encryption tools used by offenders make the detection of CSEM more challenging.

3.4. Skimming and card-not-present (CNP) frauds

Skimming fraud is a type of crime that involves taking the cash prior to entering it into the accounting system and *card-not-present (CNP) fraud* is a type of credit card scam in which the offender does not physically present the card during the fraudulent transaction [3].

Skimming will continue to be a common issue in most countries for as long as payment cards with magnetic stripes are in use. A considerable amount of skimmed card data is sold on the Darknet markets and cashed out in areas where MasterCard and Visa adoption is either slow or non-existent [3]. Card-not-present fraud also represents a top threat because it can occur with transactions that are conducted online or over the phone.

3.5. Darknet markets

The Darknet markets provide criminal vendors the opportunity to sell any kind of illicit goods and services, acting as key enablers for other crimes. Most of those goods are drugs, weapons, fake documents and cybercrime tools.

In the last few years, law enforcement succeeded in shutting down many important marketplaces. The closure of these major market led to the migration of customers and vendors to new or existing markets within the Darknet. Some vendors abandoned web shops and moved their business to encrypted communications applications, running their shops within private channels or groups.

4. Romanian law enforcement involvement in fighting cybercrime

Today's world is more interconnected than ever before. The increased connectivity brings a lot of advantages, but also many risks of theft, fraud, and abuse. The cyber-attacks become more complex and difficult to detect, so law enforcement capabilities are critical to safeguarding and securing cyberspace.

The Romanian Service for Combating Cybercrime is the specialized structure of the Romanian Police with competence in the prevention, investigation and mitigation of cybercrime, and functions within the Directorate for Combating Organized Crime. The Service acts as a central structure, with tasks of coordinating and controlling the activity in the field, at the level of the whole country.

Furthermore, the Service carries out evaluations and analyzes of the cybercrime phenomenon in Romania, while providing training programs and the necessary equipment for police officers working in the field of prevention and investigation of cybercrime. It is organized in four different bureaus: Internet Frauds and Non-Cash Means of Payment Fraud, Child Sexual Exploitation, Cyber Attacks and Digital Forensic. The Service has a 24/7 point of contact to ensure international cooperation and emergency measures in cybercrime, together with the Cybercrime Service within the Directorate for the Investigation of Organized Crime and Terrorism (DIICOT).

At an operational level, priorities were set up representing the natural evolution of the cybercrime phenomenon in Romania. A high number of ransomware attacks are targeting the Romanian citizens and companies; therefore, one of the main priorities of the Service is to efficiently tackle this threat, together with different public and private partners.

Between February 2018 and June 2019 five decryption tolls for GandCrab ransomware were released by the Romanian Police together with different partners, helping more than 35.000 victims worldwide to recover their encrypted data. In August 2018, only 7 months after its official appearance, GandCrab had managed to acquire a share of more than 50% of the ransomware market. Access was sold on underground markets to affiliates who were responsible for infecting victims and extorting money from them [5]. In exchange, the affiliates gave 40% of their profits to the original GandCrab developers.

The Romanian Service for Combating Cybercrime cooperates with different entities from national and international level, in order to fight and combat the cybercrime phenomenon.

4.1. Europol Project against ransomware

Because more and more forms of ransomware make victims all over the world, law enforcement and cybersecurity companies have joined forces to disrupt cybercriminal businesses with ransomware connections. The “No More Ransom” project is an initiative by the National High-Tech Crime Unit of the Netherlands’ police, Europol’s European Cybercrime Centre and McAfee, with the goal of helping victims of ransomware retrieve their encrypted data without having to pay the criminals [6].



Fig. 1. The No More Ransom Project

The Romanian Police is an Associate Partner in the project “No More Ransom” project, helping the community with the development of new decryption tools for the ransomware victims. The portal can now decrypt more than 100 different types of ransomware infections, a number that keeps growing on a monthly basis.

4.2. EU Policy Cycle - EMPACT

The European Union set up a four-year policy cycle in order to create a greater measure of continuity for the fight against serious international and organized crime. This multi-annual Policy Cycle aims to tackle the most important threats posed by organized and serious international crime to the European Union in a coherent and methodological manner through improving and strengthening cooperation between the relevant services of the Member States, EU institutions and EU agencies as well as third countries and organizations, including the private sector where relevant [7].

One of the priorities adopted by the Council of the EU for the fight against organized and serious international crime was cybercrime. The aim of this priority is “to fight cybercrime, by disrupting the criminal activities related to attacks against information systems, by combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, and by targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities” [7].

EMPACT is a structured multidisciplinary cooperation platform of the relevant Member States, EU institutions and agencies, as well as third countries, international organizations and other partners to address the prioritized threats of organized and serious international crime [7].



Fig. 2. EU Policy Cycle - EMPACT

Romanian Police is actively involved in EMPACT project and, thanks to the expertise and the hard work of all the people engaged, Romania is:

- *Driver* for the priority “*Payment card fraud*” between 2014-2017 and 2018-2021;
- *Co-driver* for the priority “*Attacks against information systems*”, between 2014-2017 and 2018-2021.

Romanian Police was highly appreciated for the results obtained in during the first four-year policy cycle, 2014-2017, so Romania continues to be *driver* for the priority “*Payment card fraud*” and *co-driver* for the priority “*Attacks against information systems*” for the second four-year policy cycle, 2018-2021, helping other countries to fight against the cybercrime phenomenon.

4.3. The Romanian Centre of Excellence for Cybercrime

The Romanian Centre of Excellence for Cybercrime (CYBEREX-RO) was founded as part of a European project, coordinated by the General Inspectorate of the Romanian Police (GIRP) in partnership with the Prosecutor's Office attached to the High Court of Cassation and Justice, “Alexandru Ioan Cuza” Police Academy, the National Institute of Magistracy and the University College of Dublin (UCD). The associated partners of this project were the National Association of Internet Providers in Romania, the National Computer Security Incident Response Team (CERT-RO), the Computer Training Center, the Military Technical Academy, and Bitdefender SRL [8].

The aim of this Center is to enhance the capability of combating cybercrime in the Romania, by conducting training courses for law enforcement officers, prosecutors and judges. The Romanian Center of Excellence for Cybercrime facilitates the promotion, development and implementation of methods and tools for investigating cybercrime. The courses developed by the Romanian cybercrime experts cover the following topics:

- Forensics with focus on analysis of computers, mobile phones, gathering online evidence from networks, malware analysis, encryption, programming, network security and use of specific forensic tools;

- Criminal investigation, focused on cybercrime and gathering of specific evidence from open or closed sources;
- Legal issues regarding criminal investigation and trial.

The Romanian Centre of Excellence for Cybercrime brings together the main actors involved at national level in preventing and combating the phenomenon of cybercrime: law enforcement institutions, research centers, associations and private companies. In addition to national coordination, the Center emphasizes international cooperation, through the input of the University College of Dublin (UCD), emphasizing good practices and lessons learned by other institutions at the European level [8].

The Romanian Center of Excellence for Cybercrime is part of the European strategy to prevent and combat cybercrime, being part of the European network 2CENTRE. This network helps the dissemination of accredited training courses to fit within a structured and sustainable framework. 2CENTRE identified a concept and delivery plan for the development of academically accredited cybercrime training for the law enforcement communities within the EU Member States.

5. Future perspective in fighting cybercrime

The cybercrime phenomenon is continuously changing and evolving, putting law enforcement agencies to the test. It's clear that the cybercrime phenomenon is consistent in all the countries and needs to be addressed with proper resources in order to efficiently fight against it.

There are many challenges in the process of cybercrime investigations, like loss of data, loss of location, and different national legal frameworks. But with strong international cooperation, public-private-partnerships and awareness campaigns, the law enforcement can deal with all the challenges. Increasing cyber capacities is important in order to build state-of-the-art laboratories for research, as well as training police officers, prosecutors and judges in this field. Law enforcement, the private sector and the academic environment have to work together closely, in order to prevent and combat the cybercrime phenomenon.

References

- [1] Europol, *Setting the Scene for Cybercrime: Trends and New Challenges*, [Online]. <https://www.europol.europa.eu/newsroom/news/setting-scene-for-cybercrime-trends-and-new-challenges>. [Accessed July 23, 2019].
- [2] Europol and Eurojust, *Common challenges in combating cybercrime*, 2019, [Online]. <https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime>. [Accessed July 23, 2019].
- [3] Europol, *Internet Organised Crime threat Assesement (IOCTA) 2018*. [Accessed July 22, 2019].
- [4] I.C. Mihai, C. Ciuchi, and G. Petrică, *Current challenges in the field of cybersecurity - the impact and Romania's contribution to the field*, Ed. Sitech, 2018, [Online]. Available: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf. [Accessed July 12, 2019].
- [5] Europol, Fourth decryption tool neutralises latest version of Gandcrab ransomware [Online]. Available: www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware. [Accessed June 12, 2019].
- [6] Europol, *No More Ransom Project*, www.nomoreransom.org/en/about-the-project.html. [Accessed July 5, 2019].
- [7] Europol, *EU Policy Cycle - EMPACT*, www.europol.europa.eu/empact. [Accessed July 15, 2019].
- [8] European Commission, The Romanian Centre of Excellence for Cybercrime, https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2011_ISEC_AG_INT_4000002223_en. [Accessed July 17, 2019].

Cyber Crime - Challenges and Evolution

Mircea-Constantin ȘCHEAU

The Institute of Financial Studies, Romania

mirceascheau@hotmail.com

1. General Overview

A simple overlooking of the current state of affairs shows that the subject raises interest in the context in which the relationship of dependence between society and innovation becomes more and more evident. It would be a mistake to assume that there are completely isolated infrastructures and to think only to particular associations of specific terms with computerized subdomains. Interoperability involves interconnectivity, automation, and not for few times, remote control systems. Devices whose exploitation is accessible to the domestic environment are used for real-time monitoring and allow addressing resources with a regulated status or belonging to a zone classified as a dark component (e.g. dark web). In a simple smartphone, technology is more advanced than in a spaceship in the 1970s.

In the view of actors who are faced with each other on multiple plans, escalating economic conflicts to seize market shares justifies calling for procedures that could easily fit into the gray area of international law. Research laboratories and strategic teams are the main targets of competitors. Virus strains are reinvented to bypass protection solutions. Modern techniques complement old-fashioned manipulations.

Financial crime and the necessary activities to combat it are different from those associated, for example, to cybercrime in telecommunications, but intersection points and overlapping areas call for measures to respond in a coordinated manner to aggression. In an anonymous poll of over 700 security professionals in the UK, Australia, the United States, Mexico, Germany and Japan, nine out of ten respondents said the organization they worked for was "successfully" affected by at least one cyber

attack between 2016 and 2018 and approximate half of the attacks resulted in the recording of some non-functioning intervals of critical considered systems [4].

I believe that one of the major problems faced by security structures for a long time is generated by a lack of culture of ordinary consumers, the tangible impact reflected in personal data exfiltration, compromising credentials and, implicitly, possible financial losses. The apparent security, dismantled without too much effort by black hat hackers or gray hat hackers, reveals vulnerabilities classified at first instance as harmless. An expert group discovered at the end of 2018 that exist malware that actively scan Web services and Internet-connected devices [16] to discover possible exposures and default passwords. The Xwo Python script, linked to malware families previously known as Xbash and MongoLock, combines different features, specific ransomware, cryptocurrency miners, worms, backdoors etc. Malware has been attributed to a criminal group, Iron Group, whose activity has been reported since the beginning of 2016.

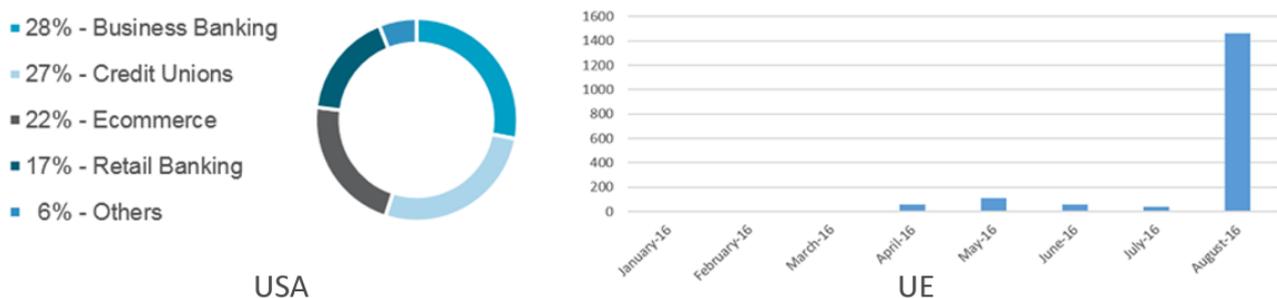


Fig. 1. The GozNym effect

Viruses that have affirmed themselves globally, malwares which have reached the expectations of the initiators and have gathered a sufficient number of appreciations to be declared successful will never be abandoned, no matter of the security methods developed by security teams against. Their reinvention aligned with the new technological realities. The source code is modified, combined with other source codes and adapted to bypass improved firewall versions. Preferred targets will be the same on which the maximum effect was recorded or adjacent to them. An eloquent example is the Trojan originally discovered in 2007 and involved between 2016 and 2018 in strong campaigns against financial banking institutions, insurances companies and not

only. GozNym combines the features of Gozi ISFB and Nymaim. On the right side of the picture in figure 1 are detailed the sectors affected in 2016 in North America and on the right side the activity in Europe [8], [9]. In 2018, Gozi (Ursnif) ranked first in the list of most active financial malwares after a third place occupied in 2017.

Another example is Kronos banking Trojan, whose new variant targeted more states in 2018, the main improvement being the Command & Control system, which used the Tor anonymization network. Even if a re-labeling was attempted under the name Osiris, the similarities with the old version are obvious: the same WebInject format, Zeus malware format, the same protocol and C & C encryption mechanism, extensively overlapping codec and last but not least 350 Kb size, comparable with the 351 Kb of a previous version [13]. Also in the context that we referred to, an underminer exploit kit created at the end of 2017 and released in early 2018 delivered a bootkit and a cryptocurrency-mining malware generically called Hidden Mellifera, and included asymmetric encryption functionality, URL randomization etc. [14].

Another bank Trojan, known as BackSwap, appeared in March 2018. Even though it has novelty elements related to WebInjection, its features are very similar to those of another Trojan known as Tinba. The way of action highlights the importance of authorization and authentication mechanisms, with the negative effects being more successful in the situation of institutions whose structures of protection did not respect international standards in the field. A suggestive image presents a list of the top ten financial malware, noting that this ranking may differ, depending on the company that conducted the study [10].

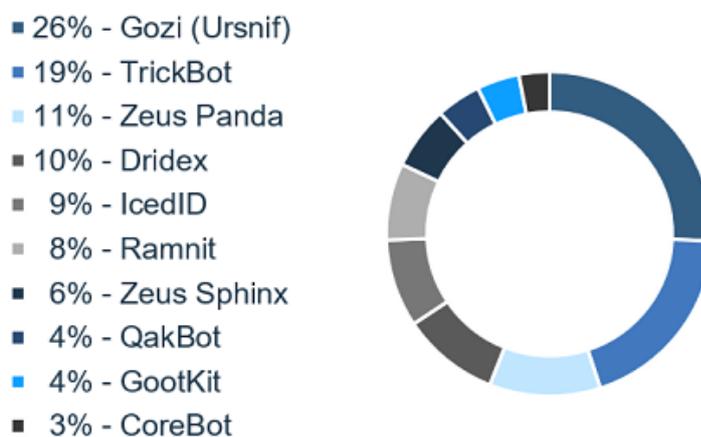


Fig. 2. Most Relevant Families of Financial Malware in 2018

Another interesting episode was the relaunch of the Ratopak / Pegasus spyware, known to be engaged in 2016 in attacks against financial-banking institutions. It was announced in underground forums that it is a new version containing the source code of the malware used by the Carbanak group, but ultimately assigned to the Buhtrap group, the decision being determined by the identification of a signing certificate that appears in binary code and which was used in the aforementioned aggressions. The action mode, the use of a sideways module, a customized, updated version of Mimikatz to "harvest" credentials, the injection of the code through "WriteProcessMemory" technique, PowerShell broadcasting, SCM, WSH Remote or RDP Scripts, different techniques which provide the ability to run a script on a remote machine and take control of it, are just some of the high-similarity features identified by researchers [15].

The above-mentioned ones induce the idea that the financial area is the predilect target of the attackers and must be given due attention. It can be simply assimilated to sectors for which protection and stability have to be ensured.

2. Transformations and Responses

In order for transactions to become safer, whether we talk about modest payment orders or international transfers subject to a standardized regime, efforts are being made to identify solutions that will lead to the consolidation of defense blocks. Biometric authentication methods were considered safer until millions of profiles began to be sold on the black market with prices ranging from five to several hundred US dollars. At the beginning of 2019, a cybersecurity company that has been operating for more than 21 years, has published the results of an investigation into the sale of about 60,000 units via an online Genesis Darknet marketplace. Access was based on an invitation and were offered to the buyers all the information they needed to use the products [7]. Crime-as-a-Service (CaaS) is no longer just an expression in a dictionary. Malware trunks can be concatenated, it is possible to gain access to customer databases for whom the weak points are known and accurately indicated, zero-day vulnerabilities can be auctioned, or can be "hired" teams ready to perform malicious work against a private or governmental target. The palette is quite wide, from custom viruses to living-

off-the-land (LoTLs) or shared criminal infrastructures. Are underground markets in continuous development, because supply is correlated with demand also in this case.

Of course, the level of protection can be increased and there are companies willing to invest in constructions capable of processing complex functions. Machine Learning (ML) is no longer an unknown. It is stated as an important branch of Artificial Intelligence (AI). As an example, we can refer to the primary identifying elements of a person, who are loaded into information processing systems. Behavioral analysis, involuntary gestures during the crossing a monitored aisle, facial expressions, reactions to external stimuli, or vocal fragments is the classified basis by categories from which it starts. All of these are compared to real-time ML sequences and corroborated with those injected later by the human operator. Any inadvertently sends an alarm signal to the surveillance team, which decides whether the impulse should be assimilated to the original or shall immediately applied the stipulations of the security plan.

It is indisputable that periodic assessments are particularly useful in identifying internal security policy weaknesses and contribute to updating existing programs. Red team and penetration tests can provide an overview of the key objective of assessing the effectiveness of detection, prevention and response capabilities. A phishing email produces residual proofs and direction are sometimes oriented to social engineering scenarios based on harder-to-detect calls. As an example, after studying the client's infrastructure and its connection to the online public environment, can be clone the authentication portal and even fake the entire structure, including the IT support phone number. An information is sent according to which emails have been migrated to a new server and employees are required to connect to the cloned OWA portal. To avoid any suspicion, communications are immediately redirected after authentication to the legitimate OWA portal, but using this method red team captures enough credentials to establish a support point in the internal network. The compromising of privileged accounts, corroborated with the lack of judicious segmentation, provides full access in a short time [1]. Such exercises are recommended to be performed simultaneously for all connected structures. Can be highlighted common and particular vulnerabilities, including those that can migrate.

Industry	Users Targeted (%)
Mining	38.4%
Wholesale Trade	36.6%
Construction	26.6%
Non-classifiable Establishments	21.2%
Retail Trade	21.2%
Agriculture, Forestry & Fishing	21.1%
Manufacturing	20.6%
Public Administration	20.2%
Transportation & Public Utilities	20.0%
Services	11.7%
Finance, Insurance & Real Estate	11.6%

Fig. 3. Malicious Email per User by Industry

Under ideal conditions, detection of malware is impossible, and the presence can only be signaled due to the effects. This involves the occurrence of losses in the interval between the time of the infection and the implementation of the solution [5]. Victims can be simple users, multinational companies or state organizations: ministries, military intelligence agencies, energy producing groups etc. No one should consider themselves fully protected. Anyone can be attacked directly or through a third party collaborator. The risk of contamination is quite high. The same infection vectors and the same techniques can be used for different environments, as can be seen from the statistic in figure 3, valid for 2019. Web platforms are used more intensely and environments with pre-installed systems are much more accessed because it is difficult to be identified the operators behind the action.

It's predicting a \$ 1.5 billion increase obtained from cybercrime profits and reaching the 70% threshold by 2021 from the volume of cryptocurrencies allocated to the underground industry. Losses will exceed \$ 6 trillion annually, under the circumstances than 146 billion registrations expected to be exfiltrated by 2023 [3]. The financial impact, total cost, frequency and intensity of attacks increase and implicitly must be incremented the level of information and training. Although there are differences in cybercrime losses, a study highlights common issues surrounding the prevalence of attacks and the cost of recovery [6]. In the present case, the interest indicators of the aggressors represent short, medium and long-term projection

landmarks. The reports are dynamic and the graphs can record medians with different values, making it even more difficult to draw the predictive coordinates.

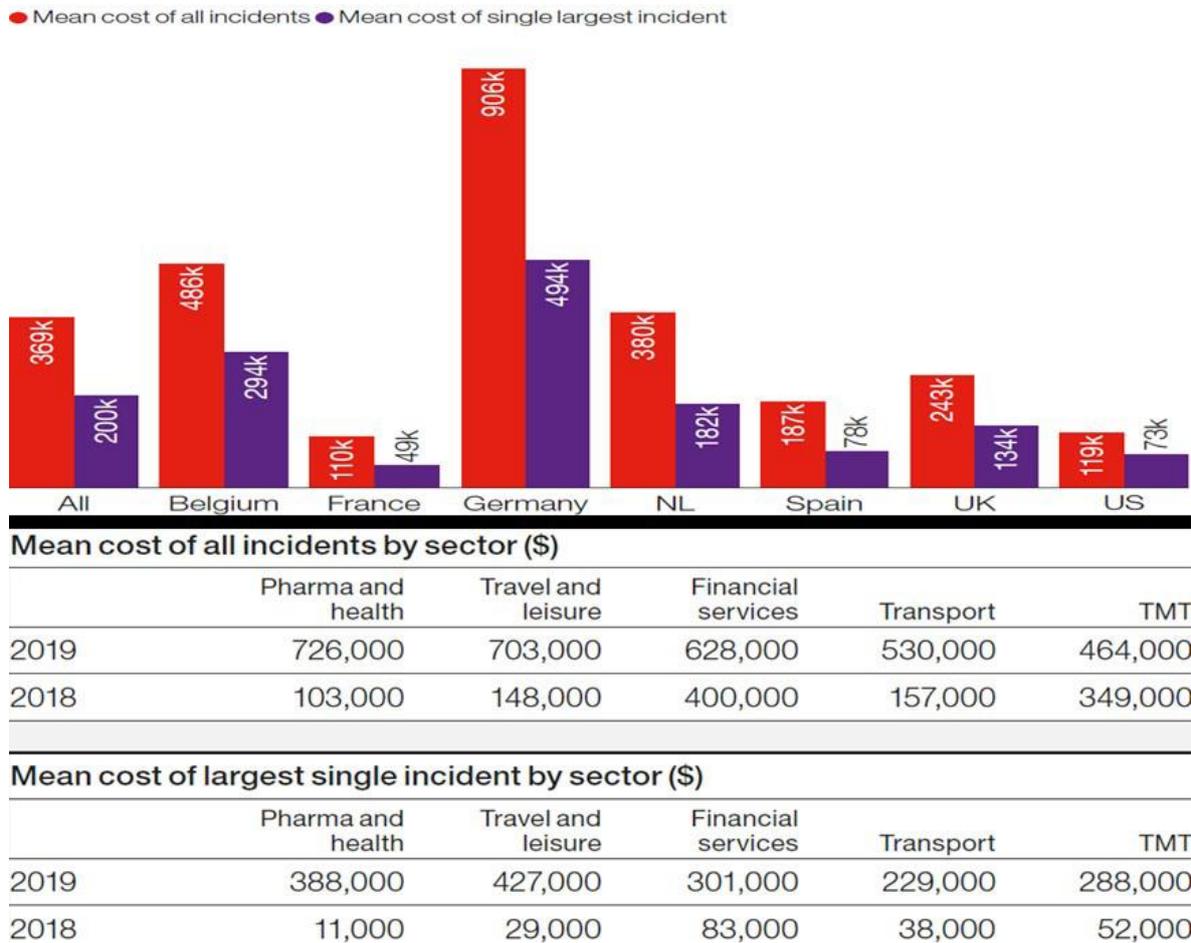


Fig. 4. Mean cost of cyber incidents (\$)

It is true that the rise of Artificial Intelligence / Machine Learning now allows for accurately examining and identifying the coding style of a person or even a group of people who work together on the same project, but the outcome may be more useful in reactive sense than anticipatory. Even if standardization or unanimous acceptance of an established method can not be discussed, anonymization and plagiarism about programming may soon become just a theoretical phrase. Tests revealed that the level of experience of an IT engineer, in combination with the number of products developed and their degree of difficulty, is directly proportional to the degree of precision of his identification. Specifically, the more experience an IT engineer has, the more he participated in the construction of more products, and the higher their difficulty was, the higher the percentage of accuracy of unveiling his anonymity. Stylometry claim

itself to be a sphere of activity that can be embedded in several subdomains, with the answers being some of the most surprising [11]. Computer security enthusiasts, who have developed their skills and are willing to make an effort that meets the challenges, sometimes need only a few clues to help them formulate a ‘Kickback’ counter. Depending on the aggression, after identifying the starting fragments, the approach strategy is being implemented together with the law enforcement agencies [12].

3. Conclusions and Proposals

Viewed from outside, scenarios can be perceived as apocalyptic and looks more like science-fiction novels than cruel reality. And the criminals rely on that. On the feeling that ”It can't happen to me” or ”Why should it happen to me if I do not show any interest to anyone?”. Each of us can become a simple piece in a GO game or we can be attracted in a whirlwind of geometric figures that change their shape and placement continuously. All we can do is not give up for a second trying to prevent and change the mentality of those around us. Twenty years ago we use to lock the door with the key and opened it only to people we knew. Not so long ago, when we only knew the currencies we could buy ordinary goods with, we didn't think the time would come when cryptocurrencies would try to impose themselves as an alternative. But the lack of regulation in the field favors the underground economy and without coherent policies, it is difficult to be combated the criminal phenomenon. The border of cybercrime can be considered to be synonymous with the limit of imagination, and in this case, it is good to be aware as soon as possible that the aggressors, who once upon a time attempted to invade our personal space through crude methods, now can do this invited even by us.

Each manufacturer recommends updating as part of the product security enhancement processes or preventive vaccination, metaphorically speaking, and changing initial passwords with some that meet length criteria and key combinations, thus lifting a first barrier to attackers. The Internet of Things (IoT) is basically the support for Internet of People (IoP) and together evolving rapidly to the Internet of Everything (IoE). Wifi Protected Access (WPA), a protocol launched by Wi-Fi

Alliance to authenticate connected devices without physical data transmission support (wireless) using the Advanced Encryption Standard (AES), has been shown to have security flaws, despite the increase in cryptographic power and in the conditions that it becomes increasingly difficult to separate personal by professional activity, a company can easily become a victim. An attack could be successful with the help of an employee who does not properly treats a phishing email or violates another internal security rule. An episode of this kind may be categorized as a human failure. In these circumstances, specific motivations must be valued to narrow the penetration channels as much as possible and to reduce the areas exposed to possible aggressions. The rationales for increasing degree of risk intolerance must be placed in the foreground and sustained.

To resist competitive pressure, companies need to understand disruptive trends with a clear influence on markets, on customer behavior and expectations, as well as on employees. Growth opportunities stimulate efforts for modernize infrastructure and open new perspectives for digital transformation. Are established priorities in the construction of an innovative culture and in this context, must be recognized the special importance of the human factor in the development of cross-border collaborations [2].

At European Union level, it is necessary to set up joint working groups to analyze and elaborate best practice for each area or ministry in order to be implemented, calendar basis, alignment measures to the same standards. Calls addressed to primary support services or teams prepared to respond to computer-related incidents, even those from the civil area, should be supported throughout the European Union, be monitored and reported in such a way as to lead to a faster identification of attack patterns and of aggressors. The concept of a (secure) communications structure with European coverage, with a centralized Artificial Intelligence system or managed on modules, can be developed only in the conditions of legislative unification, which to set the exchange of inter-institutional, interstate information and the model of collaboration between service providers and authorities [17]. In this context, fast forwarding to competent bodies of information on any cybercrime event is vital to ensuring resilience and must be a priority for official bodies or private legal entities regardless of the industry in which they operate.

In order to implement the above proposals, I also believe that it's necessary to be initiated at European level, in the educational environment, a concept of familiarization with the primary notions of computer security and even of their deepening. In addition to the general information programs held in public-private partnerships, starting from the gymnasium cycle until the completion of the average, high school courses, the school curricula should allow the inclusion of chapters specific to this topic. A well-informed society as a whole can react to aggressions and contribute actively to limiting and even preventing losses.

References

- [1] A. Rahman and C. Antolik, "Finding Weaknesses Before the Attackers Do," *Threat Research*, FireEye, 08 April 2019. [Online]. Available: <https://www.fireeye.com/blog/threat-research/2019/04/finding-weaknesses-before-the-attackers-do.html>.
- [2] B. Solis, "Seven Priorities To Accelerate Digital Transformation Maturity and Success," *Forbes*, 09 January 2019. [Online]. Available: <https://www.forbes.com/sites/briansolis/2019/01/09/seven-priorities-to-accelerate-digital-transformation-maturity-and-success/amp/>.
- [3] C. Crane, "80 Eye-Opening Cyber Security Statistics for 2019," *The SSL Store*, 10 April 2019. [Online]. Available: <https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/>.
- [4] D. Simmons, "Cyber-attacks 'damage' national infrastructure," *BBC News, Technology*, 04 April 2019. [Online]. Available: <https://www.bbc.com/news/amp/technology-47812479>.
- [5] F. Cohen, *Computer Viruses - Theory and Experiments*, Computers & Security, vol. 6, pp. 22-35, 1987.
- [6] Hiscox Ltd, "Hiscox Cyber Readiness Report 2019," [Online]. Available: <https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf>.

- [7] Kaspersky Lab, “Kaspersky Lab uncovers Genesis: The underground e-shop with tens of thousands of digital doppelgangers for sale to bypass financial anti-fraud solutions,” Press Release, 09 April 2019. [Online]. Available: https://usa.kaspersky.com/about/press-releases/2019_kaspersky-lab-uncovers-genesis-new.
- [8] L. Kessem, “GozNym’s Euro Trip: Launching Redirection Attacks in Germany,” *SecurityIntelligence*, IBM X-Force, 23 August 2016. [Online]. Available: <https://securityintelligence.com/goznym-euro-trip-launching-redirection-attacks-in-germany/>.
- [9] L. Kessem and L. Keshet, “Meet GozNym: The Banking Malware Offspring of Gozi ISFB and Nymaim,” *SecurityIntelligence*, IBM X-Force, 14 April 2016. [Online]. Available: <https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/>.
- [10] L. Kessem and T. Agayev, “BackSwap Malware Now Targets Six Banks in Spain,” *Analysis and Insight for Information Security Professionals*, *Security Intelligence*, IBM, 22 August 2018, [Online]. Available: <https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/>.
- [11] L. Matsakis, “Even Anonymous Coders Leave Fingerprints,” *Wired*, 10 August 2018. [Online]. Available: <https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/machine-learning-identify-anonymous-code/amp>.
- [12] M. Ramilli, “Hacking The Hacker. Stopping a big botnet targeting USA, Canada and Italy,” *Cyber Crime, Hacking*, Security Affairs, 31 August 2018. [Online]. Available: <https://securityaffairs.co/wordpress/75782/cyber-crime/hacking-hacker-botnet.html>.
- [13] P. Paganini, “Kronos Banking Trojan resurrection, new campaigns spotted in the wild,” *Cyber Crime*, Security Affairs, 26 July 2018. [Online]. Available: <https://securityaffairs.co/wordpress/74764/malware/kronos-banking-trojan-variants.html>.

- [14] P. Paganini, “Underminer Exploit Kit spreading Bootkits and cryptocurrency miners,” *Cyber Crime, Security Affairs*, 29 July 2018. [Online]. Available: <https://securityaffairs.co/wordpress/74860/malware/underminer-exploit-kit.html>.
- [15] Tanya_K, “Source Code of Ratopak/Pegasus Spyware Targeting the Financial Sector Recently Leaked,” *Cyber Threat Insider Blog*, 27 August 2018. [Online]. Available: <https://blog.sensecy.com/2018/08/27/source-code-of-ratopak-pegasus-spyware-targeting-the-financial-sector-recently-leaked/>.
- [16] T. Hegel, J. Blasco and C. Doman, “Xwo - A Python-based bot scanner,” *AT&T Business*, 02 April 2019. [Online]. Available: <https://www.alienvault.com/blogs/labs-research/xwo-a-python-based-bot-scanner>.
- [17] Trend Micro Research, Europol’s and European Cybercrime Centre (EC3), “Cyber-Telecom Crime Report 2019,” Report, 2019. [Online]. Available: <https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019>.

Cybercrime - Legal and Strategic Elements

Virgil SPIRIDON

Cybercrime Programme Office of the Council of Europe (C-PROC)

virgil.spiridon@coe.int

1. Capacity building on Cybercrime

The Council of Europe as an international organisation standing for human rights and rule of law helps to protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime and its Protocol on Xenophobia and Racism, the Cybercrime Convention Committee (T-CY) and the technical cooperation programmes on cybercrime.

The Convention on Cybercrime of the Council of Europe known as the Budapest Convention, is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty.

The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.

The Cybercrime Convention Committee (T-CY) represents the State Parties to the Budapest Convention on Cybercrime. Based on article 46 of the Convention, the consultation of the Committee aims at facilitating the effective use and implementation of the Convention, the exchange of information and consideration of any future amendments.

Cybercrime has become a global phenomenon, hand in hand with the economic, technological and social progress facilitated by the global interconnectedness of the Internet. Furthermore, the pervasive use of technology in everyday life has increased the number of criminal cases involving evidence on computer systems, that is, electronic evidence.

Adequate legal provisions are needed to facilitate the investigation of cybercrime and related crimes, as well as to allow effective and efficient international cooperation for the exchange of electronic evidence. National legislation in accordance with international standards is a condition for international cooperation and thus a necessity for criminal justice authorities to be able to investigate, prosecute and successfully adjudicate such crimes.

The approach of the Council of Europe - supported also by the European Union - is built on the Budapest Convention on Cybercrime which provides a guideline to any country for the development of criminal legislation on cybercrime and e-evidence and which offers Parties to this treaty a framework for international cooperation.

The international community has reached broad agreement on capacity building as an effective approach to help societies meet the rising challenge of cybercrime. The Council of Europe has been assisting societies worldwide in the implementation of the Budapest Convention through a range of projects since 2006.

Therefore, the establishment of Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania provides the Council of Europe with the infrastructure to respond to growing demands for assistance in an effective manner. All capacity building activities on cybercrime of the Council of Europe worldwide are managed from this Office.

Therefore, C-PROC is an important part of the international response to cybercrime and electronic evidence on the basis of the standards of the Budapest Convention on Cybercrime. This includes support for:

- Strengthening legislation on cybercrime and electronic evidence in line with rule of law and human rights (including data protection) standards;
- Training judges, prosecutors and law enforcement officers;
- Establishing specialized cybercrime and forensic units and improving interagency cooperation;
- Promoting public/private cooperation;
- Protecting children against sexual violence online;
- Enhancing the effectiveness of international cooperation.

C-PROC, with its capacity building function, complements the work of the Cybercrime Convention Committee (T-CY) through which State Parties follow the implementation of the Budapest Convention. The evolution of information and communication technologies - while bringing unprecedented opportunities for mankind - also raises challenges, including for criminal justice and thus for the rule of law in cyberspace. While cybercrime and other offences entailing electronic evidence on computer systems are thriving and while such evidence is increasingly stored on servers in foreign, multiple, shifting or unknown jurisdictions, that is, in the cloud, the powers of law enforcement are limited by territorial boundaries.

The Parties to the Budapest Convention have been searching for solutions for some time, through working groups that the following specific issues be addressed:

- the need to differentiate between subscriber, traffic and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations;
- the limited effectiveness of mutual legal assistance for securing volatile electronic evidence;
- situations of loss of (knowledge of) location of data and the fact that States increasingly resort to unilateral transborder access to data in the absence of international rules;
- the question as to when a service provider is sufficiently present or offering a service in the territory of a Party so as to be subject to the enforcement powers of that Party;
- the current regime of voluntary disclosure of data by US-providers which may help law enforcement but also raises concerns;
- the question of expedited disclosure of data in emergency situations;
- data protection and other rule of law safeguards.

Further to the results of one of the working groups, the T-CY adopted the following recommendations:

1. Enhancing the effectiveness of the mutual legal assistance process by implementing earlier Recommendations adopted by the T-CY in December 2014.

2. A Guidance Note on Article 18 Budapest Convention on production orders with respect to subscriber information. This Note explains how domestic production orders for subscriber information can be issued to a domestic provider irrespective of data location (Article 18.1.a) and to providers offering a service on the territory of a Party (Article 18.1.b).

3. Full implementation of Article 18 by Parties in their domestic law.

4. Practical measures to enhance cooperation with service providers.

5. Negotiation of a 2nd Additional Protocol to the Budapest Convention on enhanced international cooperation.

In June 2017, the T-CY agreed on the Terms of Reference for the preparation of the Protocol during the period September 2017 and December 2019 with the following elements to be considered:

A. Provisions on more efficient mutual legal assistance (such as expedited MLA for subscriber information, international production orders, joint investigations, emergency procedures etc.).

B. Provisions on direct cooperation with providers in other jurisdictions.

C. Framework and safeguards for existing practices on transborder access to data.

D. Rule of law and data protection safeguards.

2. Cybersecurity vs Cybercrime Strategies

Cybersecurity strategies are setting policy goals, measures and institutional responsibilities in a fairly succinct manner. Generally, the primary concern is to ensure the confidentiality, integrity and availability of computer data and systems and to protect against or prevent intentional and non-intentional incidents and attacks. Priority is given to critical information infrastructure protection.

Some of these strategies contain also measures against cybercrime. Indeed, measures against cybercrime provide a criminal justice response to attacks against computers and thus complement technical and procedural cybersecurity responses. Concepts, aims or definitions of “cybersecurity”, therefore, combine political (national interest and security) and technical dimensions whereby cybersecurity is typically

defined as the protection of the confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT.

Cybersecurity strategies tend to focus on technical, procedural and institutional measures, such as risk and vulnerability analyses, early warning and response, incident management, information sharing, setting up of Computer Emergency Response Teams or Computer Security Incident Response Teams, increased international cooperation and other measures to ensure protection, mitigation and recovery.

However, cybercrime comprises also offences committed by means of computer data and systems, ranging from the sexual exploitation of children to fraud, hate speech, intellectual property rights infringements and many other offences. These are not necessarily part of cybersecurity strategies.

Furthermore, any crime may involve electronic evidence in one way or the other. While this may not be labelled “cybercrime”, a cybercrime strategy would nevertheless need to ensure that the forensic capabilities be created that are necessary to analyse electronic evidence in relation to any crime, or that all law enforcement officers, prosecutors and judges are provided at least with basic skills in this respect.

Strategies and measures against cybercrime (“cybercrime control”) thus follow a criminal justice rationale. They are linked to broader crime prevention and criminal justice policies and they are (or should be) aimed at contributing to the rule of law and the promotion of human rights.

While cybersecurity strategies address the issue of cybercrime only to some extent and while only few countries adopted specific cybercrime strategies, a wide range of measures has been taken by governments, institutions, the private sector or international organisations that could form part of cybercrime strategies.

These range from reporting and intelligence systems, specific legislation, high-tech crime or other specialised units and forensic capabilities, to law enforcement and judicial training, law enforcement/service provider and other types of public-private cooperation, and international cooperation. Special attention has been given to the protection of children, in particular against sexual exploitation, and is increasingly being given to financial investigations.

In short, while strategies on cybersecurity and cybercrime control are interrelated, intersecting and complementary, they are not identical. A cybersecurity strategy does not address the full range of cybercrime issues, and a cybercrime strategy not the full range of cybersecurity issues. Governments may therefore want to consider the preparation of specific cybercrime strategies or enhance cybercrime components within cybersecurity strategies or policies.

3. Cooperation with Multinational Service Providers

Often a prosecution or police authority (a “law enforcement authority”) of a Party to the Budapest Convention requests a service provider in another jurisdiction for data in relation to a specific criminal investigation. Typically, subscriber information is sought from multinational service providers with their headquarters in the USA (“US service providers”). Some of them have subsidiaries in Europe or elsewhere.

Transparency reports published by US service providers indicate that they respond positively to about 60% of such requests “on a voluntary basis”.

In several Parties, the authorities have concluded agreements or made arrangements to improve cooperation with US service providers. This includes the use of agree upon templates for requests, procedures to be followed and the establishment of single points of contact. Examples are France and Portugal.

In Parties where such arrangements are in place, larger numbers of requests are sent and information received. Both, criminal justice authorities and service providers underline that such good practices can make a difference.

The voluntary disclosure of subscriber information by US service providers is most valuable to criminal justice authorities in Parties to the Budapest Convention. Nevertheless, a number of issues and concerns have been raised.

Provider policies are volatile and lack foreseeability for law enforcement as well as customers. Service providers may change their policies unilaterally at any time and without prior notice to law enforcement.

Adding to this, policies and practices not only differ widely between providers but also with respect to different Parties to the Budapest Convention. One provider may respond to many requests from one country but to none or a few requests only from another country, while the practices of another provider may be exactly the opposite.

Overall, provider policies and practices are volatile and unpredictable which is problematic from a rule of law perspective.

With respect to the cooperation between US service providers and law enforcement authorities of other Parties, it would seem that with regard to requests for subscriber information, the actual location of the data or servers is of limited relevance. Conditions for access to subscriber information seem to be determined by (a) the location of the service provider and the regulations that govern the service provider, and (b) whether the requesting law enforcement authority has jurisdiction over the offence investigated. Under certain conditions, US service providers tend to disclose subscriber information to law enforcement authorities in countries where they are offering a service as foreseen in Article 18.1.b Budapest Convention.

European providers seem to be bound by rules of territoriality, including the location of data.

With regard to content data, US providers are unclear. In some instances, they may argue that content is stored in the US and thus voluntary disclosure is not possible (unless in emergency situations). In other instances, where data may be stored in Europe, they still require a mutual legal assistance request to be sent to the US Government.

US service providers are able to disclose subscriber and traffic data directly and voluntarily to foreign law enforcement authorities upon request. Content may also be provided in emergency situations. This is permitted under US law (Electronic Communications Privacy Act).

It would seem that European providers are not disclosing data directly to foreign authorities and only respond to orders received via domestic authorities following mutual legal assistance requests.

The reasons are not entirely clear. While providers of “electronic communication services” in Europe are normally under a strict regime regarding the disclosure of traffic data, providers of “Internet society services” should in principle be able to disclose subscriber information under legitimate, vital or public interest considerations.

The consequence is a one-way flow of data from US service providers to the law enforcement authorities of Parties in Europe and other regions, while service providers in Europe or other Parties do not disclose data directly and voluntarily to the authorities in the US or other Parties. Increasingly, US service providers are represented within the European Union - for example through subsidiaries in Ireland - and are thus subject to European Union law, including data protection regulations. This may restrict possibilities for direct and voluntary transborder cooperation in the future.

On the other hand, one may ask why what is possible for US service providers located or represented within the European Union - namely the voluntary disclosure of subscriber information or, in emergency situations also of other data - would not be possible for European service providers.

US service providers - when receiving requests for data from foreign law enforcement authorities - consider the domestic legal framework of the requesting authority, including whether the requesting authority would have the power to request a certain type of data from a service provider at the domestic level.

In order to overcome the difficulties of getting data from abroad and not knowing the exact location of the data, solutions have been sought primarily by US and European Union. While US law enforcement is struggled with the requests addressed to US service providers and data is not clearly where is stored for European Union countries and others getting data from US service providers is still an issue.

In 2018 US adopted US Cloud Act to allow US law enforcement to obtain data in the possession and control of US service providers no matter where data is located.

For European Union countries the solution, although is not easy to get an agreement, is the digital evidence package to allow authorities to send directly preservation requests and production orders to service providers from another EU country.

These approaches of US and EU will not cover the all cooperation with multinational service providers (outside US or EU) and hence the Protocol under negotiation of the Parties to the Budapest Convention would reinforce the international cooperation and promote the necessary instruments to be accessed by countries worldwide.

4. Cybercrime as Transversal Challenge

Cybercrime and electronic evidence are transversal challenges, and that, therefore, stronger capacities to meet these challenges will contribute to the prevention and fight against organised crime, terrorism and other crime area all over the world.

The provisions of the Budapest Convention do not specifically focus on terrorism. However, the substantive crimes in the Convention may be carried out as acts of terrorism, to facilitate terrorism, to support terrorism, including financially, or as preparatory acts. In addition, the procedural and international mutual legal assistance tools in the Convention are available to terrorism and terrorism-related investigations and prosecutions.

In fact, the specific procedural measures can be very useful, for example in terrorism cases, if a computer system was used to commit or facilitate the offence or if the evidence of that offence is stored in electronic form or if a suspect can be identified through subscriber information, including an Internet Protocol address. Thus, in terrorism cases, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

Acts of violence against individuals committed by means of or facilitated by information and communication technologies (“cyberviolence”) have become a primary concern for societies and individuals.

While cyberviolence may be targeted at any individual or group and may entail a wide range of acts, in particular on children and women, who are often the victims of cyberviolence. The experience and solutions with regard to these victims should modus

modendi be applicable to other categories of victims while taking into account the specificities of violence against different categories of victims.

It is critical to recall that many forms of cyberviolence are already covered in domestic or international law by “physical world” provisions, and investigations may not have to wait for new legislation. For example, when computers are used to cause or facilitate violence through the transmission of messages that cause psychological harm, or through advertisement for murder, rape, kidnapping or trafficking in human beings, such cases may be prosecuted (depending on their facts) as assault, violation of privacy, illegal threat, extortion, solicitation of rape or murder, illegal distribution of content (such as photographs), domestic violence, and so on.

Furthermore, given the dependence on computer systems - including psychological, physical and economic dependence - some types of cybercrime (illegal access to intimate personal data, the destruction of data, etc.) may also be considered acts of cyberviolence.

In practice, acts of cyberviolence may involve different types of harassment, violation of privacy, sexual abuse and sexual exploitation and bias offences against social groups or communities. Cyberviolence may also involve direct threats or physical violence as well as different forms of cybercrime.

There is not yet a stable lexicon or typology of offences considered to be cyberviolence, and many of the examples of types of cyberviolence are interconnected or overlapping or consist of a combination of acts.

Not all of forms or instances of cyberviolence are equally severe and not all of them necessarily require a criminal law solution but may be addressed by a graded approach and a combination of preventive, educational, protective and other measures.

References

- [1] Cybercrime strategies.
- [2] Guidance Note #11 -Terrorism.
- [3] Mapping study on cyberviolence.
- [4] Action against cybercrime, [Online]. Available: www.coe.int/cybercrime.



CYBER DIPLOMACY



CYBER DIPLOMACY

Perspectives on Cyber Diplomacy

Carmen-Elena CÎRNU, Adrian-Victor VEVERA

National Institute for Research and Development in Informatics ICI Bucharest
carmen.cirnu@ici.ro, victor.vevera@ici.ro

1. Introduction

Globalization has led to a massive blurring of traditional boundaries and authorities, a reality that has also contributed to the proliferation of risks and vulnerabilities unknown before.

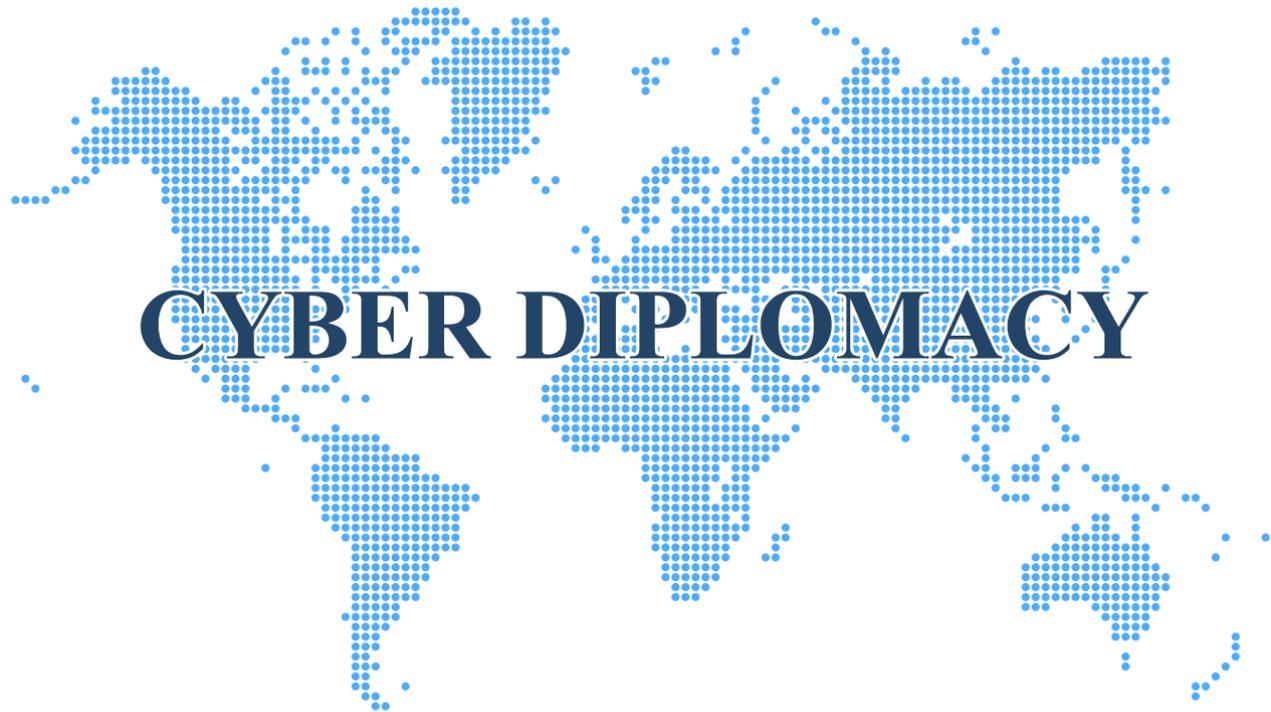
The digitalization of society prompted phenomena like those of *`de-territorialization`* and *`re-territorialization`*, where conventional boundaries are continuously negotiated and altered. Z. Bauman and D. Lyon (2016) note that the digital society we live in is primarily characterized by *`distance and remoteness`*. In this context, cyber-diplomacy has emerged as a tool dedicated to states as well as to other international stakeholders in order to properly manage cyber-related risks and threats and to advocate best governmental practices.

In this paper, we seek to identify different perspectives on this new domain from related research literature and showcase various initiatives in this area, both at international and national level. In essence, cyber diplomacy is traditional diplomacy applied to cyber-related issues, therefore it uses diplomatic tools to solve cyber-related matters, also marking an important shift in the political paradigm. Internet governance, development of the legislation regarding the prohibition of cybercrime, proper responses to cyber threats and critical infrastructure protection are areas in need of specifically formulated strategies, norms and actions.

In the last years, the international diplomatic agenda has suffered amendments, cyber related issues becoming a top priority. Cyber diplomacy cannot be limited to the afore-mentioned issues, also entailing economic and military applications. Being an emergent field, new intersections and applications will occur.

2. Cyber diplomacy: distinction from related concepts

Melissen [1] highlights that *‘the evolution of diplomacy, namely the technological developments implicit in such terms as cyber-diplomacy, linking the impact of innovations in communications and information technology (CIT) to foreign policy and diplomacy’* have a specific impact on the general evolution of diplomacy.



The concept of cyber-diplomacy is often related to *‘digital diplomacy’*, but the two should not be confused, as they are not interchangeable terms. The latter, also known as electronic/computer/e-diplomacy, refers to the use of digital tools in order to promote diplomatic strategies and goals. It should be regarded more as a means and not an end in itself, dedicated both to governmental and non-governmental actors. The diplomatic agenda greatly affects the development of strategies and policies, therefore requiring digital tools that are suitable for the implementation of diplomatic strategies. In its practice, cyber diplomacy is using digital instruments for the development of its specific techniques/actions, but this is not a restrictive characteristic nor is it a definition of this concept.

The essential characteristic of cyber diplomacy is that it uses tools and frame of mind specific to traditional diplomacy. As a consequence, cyber diplomacy is related to digital diplomacy but they remain two separate operations.

Another important and related notion is that of `cyber deterrence` or `deterrence in cyberspace`, which is defined by American researchers as responding to a *`vast range of coercive activities directed against the United States and its allies`* [2]. Deterrence can be divided into two components: *`deterrence by denial`* (passive deterrence) and *`deterrence by punishment`* (active deterrence) [3]. The first type of deterrence is defined as *`reducing the perceived benefits an action is expected to provide a challenger`*. [4]. *`Deterrence by punishment`* (active deterrence) refers to the threat of using retaliation and severe penalties such as significant economic sanctions and the use of nuclear weapons if an attack is initiated by the enemy. Brantly [5] notes that *`in the physical world it often includes hardening targets by building higher walls, adding security mechanisms, or other tactics to reduce the susceptibility of targets to attack`*. He adds that *`commonly used forms of deterrence by denial in conflict zones include land mines, razor wire, surface to air missiles (SAMs) and fortifications.`* In cyberspace, this type of deterrence includes all security strategies and attempts to prevent attacks or to reduce their impact. Although it is sometimes referred to as *`passive deterrence`*, Brantly warns that *`denial strategies are not passive. They require continuous modification relative to adversary capability development. Static denial strategies in cyberspace or in conventional conflict are likely to have limited credibility over time. Similarly, punishment strategies also require constant updating in relation to adversary capabilities and geopolitical considerations. In cyberspace, this involves adapting denial strategies to technological advances such as artificial intelligence, polymorphic malware and the Internet of Things, to name just a few.`*

The concept of cyber deterrence faces many challenges identified by specialists, such as the following:

- Cyber weapons are easily available, therefore cyber-attacks are facilitated;
- Cyber-attacks are difficult to link with their perpetrators;

- The wide range of cyber-attacks and the mixture of state and non-state actor who are engaged in them or targeted by them;
- The controversies and obstacles in formulating and implementing norms and policies regarding the behavior in the cyber field at an international level.

3. Cyber diplomacy acts and initiatives

The development of policies and norms related to international cybersecurity is promoted by the Global Commission on the Stability of Cyberspace (GCSC). This entity supports understanding among different communities in the field of cybersecurity. The GCSC operates as a promoter and facilitator, connecting governmental actors with emerging communities from cyberspace. Recently, on 9th April 2019, the Council of the European Union adopted the European Union Cybersecurity Act which includes an important norm established by GCSC - `The Protection of the public core of the Internet`. This Act is an important threshold in the development of cybersecurity-related policies. It supports the creation of a `EU-wide cybersecurity certification framework and promotes the current European Agency for Network and Information Security (ENISA) to a permanent EU Agency for Cybersecurity.` [6]

UN also firmly supports cybersecurity, developing an important framework for international cooperation in this field. So far, the UN group of governmental experts drew up several reports in the field of Information and telecommunications in the context of international security, in 2010, 2013 and finally in 2015. They contain recommendations on norms, principles and proper behavior of States in order to promote cooperation for a safe, peaceful, open and resilient ICT field.

The Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - published on 24 June 2013 (UN GGE 2013), includes recommendations from the UN-governmental expertise group from 15 different countries analysing ICT-related threats from different state and non-state players. As the act shows, security is a matter of central importance for UN. The set of recommendations is interlinked with the

existing international law on ICT security, highlighting the fact that ICTs are delivering immense benefits for the society, but they are also carrying great risks related to international security (e.g. cybercrime), and this issue requires to be carefully treated.

Since the launch of the 2010 report (the building block for the present 2013 report), the dialogue on matters related to international cooperation in the cyber security domain has been intensified and multiple initiatives (bilateral, at regional level and multilateral) are the proof that ICT-related issues are treated with responsibility. The report underscores that: *‘It is in the interest of all States to promote the use of ICTs for peaceful purposes. States also have an interest in preventing conflict arising from the use of ICTs. Common understandings on norms, rules and principles applicable to the use of ICTs by States and voluntary confidence-building measures can play an important role in advancing peace and security.’* [7]

The Member States agree that active cooperation oriented towards countering threats related to illicit and malicious use of ICTs is an essential priority on the common security agenda. The main objectives should be the improvement of global stability, peace and security. The specific legislation must be commonly understood and applied by all states. Also the citizens and private sectors are expected to participate in addressing these challenges, following the lead of State actors. The role of the United Nations in this cooperation should be a leading one, acting as the facilitator of the dialogue between Member States so they can develop common security framework and actions related to the use of ICTs.

The progress of the secure use of ICTs at international level is going to be continuous and recurring, *‘with each step building on the last’* [8], due to the rapid developments of the fields and its applications. This report should stimulate Member States to strongly join their efforts and act towards this common goal. All these recommendations should serve as a basis for further developments at national and international level.

Efficient cooperation among States is essential for diminishing risks related to ICTs, risks that threaten global peace and security. The aim of the 2015 Group of Governmental Experts on Developments in the Field of Information and

Telecommunications in the Context of International Security is to address these risks by analysing existent and possible threats and develop common actions to reduce them (e.g. norms, regulations, standards, measures for confidence-building). Also, the UN GGE 2015 Report evaluates the application of existing international legislation at national level. The report builds on the previous UN GGE 2013 and has made relevant progress in these specific areas:

- The discussion about norms has been extended, calling for increased cooperation among States in order to prevent and limit malicious/terrorist use of ICTs on their territories. The Group recommends they should unite their efforts in order to prosecute the criminal use of these technologies.
- Critical infrastructures must be protected by the States and they must not support or worse, lead ICT activities that could deliberately harm these infrastructures. Proper measures must be taken to defend the operability of critical infrastructures and protect them from ICT-related threats. The States should also promote awareness in relation to the necessity of reporting critical infrastructure potential vulnerabilities and the responsible use of ICTs.
- The cooperation and transparency promoted by confidence-building measures limit the prospect of conflict. The Report proposes some transparency measures and the States have the responsibility to consider them and also develop new ones. The Group recommends official dialogues under the patronage of the UN and by establishing periodical bilateral, multilateral, regional forums.
- Another important point made by the Group is the necessity of building capacity. The UN GGE 2013 addressed the need of enhancing the protection of critical ICT-related infrastructures, assistance in developing appropriate technical abilities and offer recommendations regarding the proper law, regulations and strategies. These conclusions are reinforced by the UN GGE 2015, highlighting that States can learn from one another, by sharing knowledge and exchanging good practices.

The report aims to support common understanding in the field of ICT use in the context of global security, assess existing and emerging threats related to ICT and promote cooperation-oriented measures to tackle these issues. Cyber diplomacy may be better understood if we look at the main international agreements/coalitions in the field:

- In 2009, China and Russia signed The Agreement among the Governments of the Shanghai Cooperation Organization (SCO, also known as the Shanghai Pact) Member States on Cooperation in the Field of Ensuring International Information Security. This important act identifies the major threats in providing information security (e.g. development/use of information weapon, preparation/conducting information war, information terrorism, information crime) and sketches the main directions for a cooperation framework necessary to fight against them. The parties agree to enforce cooperation on different levels: coordination/implementation of common efforts to guarantee international information security, the development of a monitoring system and harmonized response to the specific identified threats, the joint formulation of rules and policies for the restriction of the use and distribution of information weapon, limiting the use of information-related technologies for terrorist ends.
- The 2015 U.S.- China Cybersecurity Agreement: This cybersecurity agreement was reached in response to the prolonged issue of cyber espionage accusations from both parties, starting with the early 2000s. In 2015, former president Obama and president Xi Jinping reached an agreement guaranteeing to stop government cyberspace-related sponsored economic espionage. This bilateral agreement vouches to cease the economically-driven cyber espionage between the two states, especially by preventing the theft of confidential trade data.
- In September 2011, four member states of the SCO (China, Russia, Tajikistan, and Uzbekistan) submitted a Draft of the International Code of Conduct for Information Security to the United Nations General Assembly, regarding the

controversial concept of `cyber sovereignty`. The draft was followed by an updated version in January 2015, advanced by six member states of the SCO: China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. This document represents common efforts to create and implement behavioral norms to be applied in cyberspace. Their main interest was regulating the notion of `cyber sovereignty`, with regard to the possibility that it implies security threats. In the same time, democratic states were concerned that such a regulation may threaten the human freedom of expression.

On the national level, The **Cyber Diplomacy Center - ICI Bucharest** (National Institute for Research and Development in Informatics) was founded in March 2019 as a unique Romanian initiative. Its main goal is strengthening the diplomatic agenda in the cyber field, serving as a necessary complement to the technological, economic and social dimensions of the cyber domain. The Center is cooperating with relevant national and international ministries/authorities with responsibilities in the diplomatic sector and in cyber security.



The main objectives of the Cyber Diplomacy Center are:

- Managing the risks related to collective security and supporting good governance by using specific tools dedicated to relevant state and non-state actors;
- Promoting the interests of relevant stakeholders from the cyber field by applying traditional diplomacy resources;
- Proposing and implementing strategies, initiatives, actions that enhance cyber security and promote peace and stability;

- Drafting norms and strategies in areas like: Internet governance, prohibition of cyber criminality, the adequate response to cyber-threats and the protection of critical infrastructures.

The establishment of this Center is the first step of an envisioned collective strategy, to be followed by the launch of an international initiative on `cyber diplomacy` and then of a global Alliance.

As the diplomatic agenda is constantly changing and evolving and as its reorganization places the necessity to enhance cyber security on top of the list, cyber diplomacy must be a flexible tool, capable of adapting to this intense rhythm through the development of new applications and intersections: ICI's Cyber Diplomacy Center emerged as a response to these specific needs.

4. Conclusions

Cyber diplomacy is a natural response to the reconfiguration of the diplomatic agenda and to the more and more acute necessity of ensuring cyber security to promote peace and stability at national, European and global level. As traditional boundaries are challenged by new technologies (ICTs), international cooperation is essential. That is why cyber diplomacy must advance and prospective measures/initiatives need to be taken into consideration and implemented, such as: common and individual consolidation by States of notions for international stability, peace and security in the field of new technologies at the technical, political and legal levels, enhanced regional/multilateral cooperation aimed at accommodating common understandings on the possible threats to international peace and security represented by the harmful use emergent technologies on the security of critical infrastructures, as well as promoting national/regional initiatives on cyber diplomacy.

The further developments of the regulatory framework related to cyber security and diplomacy must take into account all the existing initiatives / acts / norms / recommendations, which should be the building blocks for all future work in this field.

References

- [1] Jan Melissen (ed.), *the New Public Diplomacy*, Palgrave Macmillan, 2005.
- [2] James A. Lewis, *Deterrence in the Cyber Age*, 2014.
- [3] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, 2009.
- [4] Wilner, Alex S. “Deterrence Theory: Exploring Core Concepts”, in *Deterring Rational Fanatics*. Philadelphia: University of Pennsylvania Press, 2005.
- [5] Brantly, Aaron F., *The Cyber Deterrence Problem* in 2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects T. Minárik, R. Jakschis, L. Lindström (Eds.) NATO CCD COE Publications, Tallinn, 2018.
- [6] <https://cyberstability.org/news/european-union-embeds-protection-of-the-public-core-of-the-internet-in-new-eu-cybersecurity-act/>.
- [7] UN Report: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security from 24 June 2013, p. 6.
- [8] UN Report: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security from 24 June 2013, p. 11.

Cyber (Security) Diplomacy

Mihai SEBE

European Institute of Romania

mihai.sebe@ier.gov.ro

“‘Cyberspace’ as a term is sort of over. It's over in the way that, after a certain time, people stopped using the suffix '-electro' to make things cool, because everything was electrical. 'Electro' was all over the early 20th century, and now it's gone. I think 'cyber' is sort of the same way.” (William Gibson)

Abstract

When we speak about the issue of cyber diplomacy, we must first of all manage the diverging meaning this term has amidst the experts and the general audience. We must then understand that it is not about technical measures as such but it rather about creating the political and institutional ecosystem that would allow that the above-mentioned measures be taken and to make sure that they can be implemented by all the relevant actors.

1. Introduction. Terminological clarifications

“What’s in a name? That which we call a rose / By any other name would smell as sweet” (William Shakespeare)

The question arises even more prominent when we speak about the cyber- and digital- realms and their connection with the diplomacy world. The current debate has seen the birth of several terminological debates concerning what terminology should be the proper to use.

First of all we are currently having the so-called “e-diplomacy” defined “as the use of the web and ICT to help carry out diplomatic objectives.” [1] Another definition in use is that of “e-diplomacy” as “the virtual conduct of public diplomacy, using digital

information and communications technology (ICT), namely cyber-tools such as Social Media (Twitter, Facebook, Youtube, etc.), in order to communicate and to project a nation's image into both the national and international public sphere.” [2]

The digital tools described here are not an end by themselves but are merely means of a public or private sector entity to achieve a goal.

In accordance with other authors the cyber-diplomacy is another kind of “beast” by itself. It refers “to the use of diplomatic tools and mindsets in resolving, or at least managing, the problems in cyberspace” [3]. We are dealing with the application of diplomacy in the cyberspace, and how the diplomatic approach can be of assistance in helping the management of cybersecurity issues. The premise from which this approach starts is that in accordance with whom the cyberspace is not as distinct from the physical space as we may think. The technical approach in this case is not enough, the technical solutions are not a panacea for all issues. Believing that is similar to the belief that the military solutions are the only solutions in the physical space [4].

This approach is similar to others in the scholar literature where cyber diplomacy “can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace. Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance.” [5]

2. International regulations / organizations

Having a legal framework that regulates the cyberspace is of utmost importance as the cyberspace is often independent from the physical boundaries of countries. Thus, the agreements between nations and the rules and regulations of various international organizations create a general common basis in order to take the necessary measures.

The cybersecurity is rather a new area of the international regulations due to its relative novelty on the historical scale of regulations. Step by step, we are witnessing

an increased international cooperation in regards to issues concerning cybercrime, cyber defense, etc. yet at a different pace and intensity.

For that purpose, a critical role is being played by the United Nations in its capacity as a key international organization with worldwide reach.

For that purpose I need to mention that the question of cybersecurity has entered the UN agenda since 1998 when the Russian Federation envisaged a draft resolution on the topic which was adopted by the General Assembly as Resolution 53/70 called *Developments in the field of information and telecommunications in the context of international security* [6]. Amidst the most recent resolutions we can count the December 2018 Resolution 73/266 *Advancing responsible State behavior in cyberspace in the context of international security* [7].

This has been supplemented by the work of the Groups of Governmental Experts (since 2004) which have focused on the following topics: Existing and emerging threats; How international law applies in the use of ICTs; Norms, rules and principles of responsible behavior of States; Confidence-building measures; Capacity building. Also we can mention the annual reports by the Secretary-General to the General Assembly with the views of UN Member States on the issue (since 1998) [8].

The UN also has a key role through its Agencies, such as the International Telecommunication Union (ITU) that, in 2007, launched the Global Cybersecurity Agenda (GCA) “a framework for international cooperation aimed at enhancing confidence and security in the information society” which “is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts” [9].

Amidst other relevant international organizations I would briefly mention just some such as: INTERPOL (relevant for the coordination of law-enforcement agencies and legislations), NATO (on the topic of cyber defence policy), etc.

3. USA cyber case

When we speak about the best examples no discussion can avoid the case of the United States and its use of cyber diplomacy. Therefore I would briefly mention here

the so-called “21st Century Statecraft” initiative of the U.S. Department of State meant to put to best use the “internet moment” in foreign policy as “the disruptive social, political and economic changes that information networks have unleashed demand that diplomats ask new kinds of questions and reckon with new kinds of challenges” [10]. It envisaged changes in four major arenas: 1) diplomacy - the use of new communication technologies that allows the diplomat to speak and to listen to new audiences; 2) development - to match the development policies and programs to the fact that a majority of people are now connected to the Internet (e.g. “Civil Society 2.0” initiative meant to help the civil society organizations to use the connection technologies for their advantage); 3) policy - focus on the international Internet policy (Internet freedom, Internet governance, cybersecurity, etc.) and 4) Institutional change - ways to change the business practices, to attract new talents and use new management techniques, etc. [11].

Currently the Department of State is the front runner of US government policies regarding the cyberspace and has a dedicated department - *Office of the Coordinator for Cyber Issues (S/CCI)* that “coordinates the Department’s global diplomatic engagement on cyber issues, coordinates with the White House and federal departments and agencies on these issues, and acts as liaison to public and private sector entities in these areas” [12].

Their activities have the ideatic and legal support of a cluster of key legislative issues like the *2018 National Cyber Strategy of the United States of America* which regards the cyber diplomacy objectives wants to *preserve peace to strength* by enhancing cyber stability through norms of responsible state behaviour and to attribute and deter unacceptable behaviour in cyberspace while also want to *advance American influence* and promote an open, interoperable, reliable and secure Internet while building an international cyber capacity [13].

This document may be supplemented by the *Cyber Diplomacy Act of 2019* intended to support United States international cyber diplomacy and “the policy of the United States to work internationally to promote an open, interoperable, reliable, unfettered, and secure Internet governed by the multi-stakeholder model” [14].

4. EU cyber diplomacy toolbox

When we speak about the EU we need have in mind the complexities of the region and the different perceptions of the Member States on the issue of the cyberspace.

We must therefore mention the Council of the European Union conclusions on cyber diplomacy of 11 February 2015. It states the need of a common EU approach for cyber diplomacy at the global level. It specifies the principles and the objectives that EU should try to respect: promotion and protection of Human rights in cyberspace; norms of behaviour and application of existing international law in the field of international security; Internet governance; enhancing competitiveness and the prosperity of the EU; cyber capacity building and development; strategic engagement with key partners and international organisations, etc. [15].

It was be supplemented in February 2017 another series of Council Conclusions on a framework for a joint EU diplomatic response to malicious cyber activities (“cyber diplomacy toolbox”). This documents provides the main principles behind the EU diplomatic responses to malicious cyber activities: serve to protect the integrity and security of the EU, its Member States and their citizens; take into account the broader context of the EU external relations with the State concerned; provide for the attainment of the CFSP objectives as set out in the Treaty on the European Union (TEU) and the respective procedures provided for their attainment; be based on a shared situational awareness agreed among the Member States and correspond to the needs of the concrete situation in hand; be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity; respect applicable international law and must not violate fundamental rights and freedoms [16].

All this must also be look in the context of the *Cybersecurity Act* [17] and other relevant documents and actions [18].

With the title of example we can mention the fact the cybersecurity issues have become almost a “compulsory” mention on the agenda of any EU meeting with various international cooperation formats. It has become a “mantra” of almost all negotiations and it implies a change of attitude amidst the negotiators as the question of “cyberspace”

with all its implications generated the need for a new approach and a new thinking pattern.

For instance the *Joint statement of the 22nd EU-ASEAN ministerial meeting* of 22 January 2019 mentioned “cyber-” in various formats for 3 times, all in the context of ongoing negotiations. The *Statement* welcomed “the outcome of the eleventh EU-ASEAN Information and Communication Technologies Dialogue, which can play an important role in promoting an open, secure, stable, accessible and peaceful cyberspace” while spoke for the need of cybersecurity (2 mentions out of 3) [19].

5. What about Romania?

Romania is active on the cybersecurity agenda with important results in that area. As regards the specific topic of cyber diplomacy as an EU Member State we are following the EU guidelines in the area. The Romanian MFA plays a role in the area by ensuring the communication and interface between Romanian diplomatic missions, the concerned authorities and the nations authorities in the area [20].

Romania has adopted the Cybersecurity Strategy in 2013, adapted to the EU tendencies with the purpose to “define and maintain a safe cyberspace with a high degree of resilience and confidence”, one of its objectives being related to cyber diplomacy: “carrying out information and public awareness campaigns on threats and cyber risks and developing cooperation between the public and private sectors at national and international level” [21]. We see a strong focus on developing cooperation on cybersecurity as the international cooperation is a *sine qua non* for the area.

Speaking about cyber diplomacy and cybersecurity the Romanian Presidency of the Council of the European Union is a positive example of how the cybersecurity talks can be used in order to create a culture of international cooperation as stipulated by the official documents mentioned above. Having as one of the main pillars the idea of “A safer Europe” the question of cybersecurity was in forefront one of the objectives of “protecting the safety of the citizens, companies and public institutions in the cyberspace and improving the overall resilience of the Union to cyber-attacks” [22].

During our Presidency the “cyber-“ was present on a regular basis, and other than the Cybersecurity Act mentioned above, what strikes out as an important element for cyber diplomacy was the ability to impose sanctions in case of cyberattacks. A prerogative of the “traditional” diplomacy was therefore extended to the digital area as the European Union can from now on “impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, including cyber-attacks against third States or international organisations” [23].

Romania also had an active role in shaping the Digital Single Market for Europe as measures and decisions were adopted which stressed the need for transparency obligations for online platforms, the vision of a future of a highly digitised Europe beyond 2020 where no one is left behind, and updated copyright rules to make them fit-for-purpose in today's digital environment [24].

Romania has also more to offer in the area of cyber diplomacy than the EU framed activities as the question of cybersecurity is top on the MFA’s agenda. We can mention as a title of example the fact that Romania plays an active role within NATO initiatives in the area. Romania has become a key cybersecurity ally for the international community and had overseen for instance the Ukraine Cyber Defense Trust Fund, a program funded by NATO member countries meant to help strengthen embattled Ukrainian defenses that ended in 2017 [25].

Another important example is that of bilateral cyber diplomacy activities. The 20 August 2019 visit of Romania’s president Klaus Iohannis to the White House had on the agenda of bilateral issues the technological component and ended up in a Joint Statement and subsequent Memorandum addressing the 5G issue.

“We also seek to avoid the security risks that accompany Chinese investment in 5G telecommunications networks.” [26]

This “simple” phrase can be seen, in this author’s opinion, as a turning point in the cyber diplomacy activities underwent so far. Why does it matter? First and foremost it signals the strategic support toward the United States of America policy toward China. It signals Romania’s willingness to enter the complicated trade dispute between

the two world economic giants. Moreover it sends a clear signal that this alignment would also impact the EU internal dynamics as one of its Member States is taking a clear stance in this dispute. Also it may entail important economic costs as Romania and China have an important economic relationship. Also it can affect the national plans for the implementation of the 5G network in Romania and the business plans of important telecommunication players. That would require a contingency plan and additional measures to prevent any negative impact for our partners.

6. Conclusions

“We are now living on Internet time. It's a new territory, and the cyber equivalent of the Oklahoma land rush is on.” (Andy Grove)

When we speak about the area of cyber diplomacy we need to have in mind the fact that it not about cybersecurity as such nor about technical measures but it is about values, norms and principles. It is about the creation of a normative framework and about the institutions needed to provide a safe and free cyberspace. Cybersecurity is just one of the tools that can be used by cyber diplomacy in achieving these goals.

We need cyber diplomacy as the new technologies transform the traditional diplomacy into a more open space. They create opportunities for the governments to interact with the audiences thus the cyberspace is no longer the realm of “geeks” or private affairs but a public arena open to international interferences. “As our increasingly networked world becomes more interconnected, challenges continue to arise daily requiring governments around the world to work together to create new measures of cyberspace policy. Cyber diplomacy is necessary in order to protect national interests, while enhancing security for citizens of the world.” [27]

We have in front of us a brave new world as the trend toward the digital world, the new technological revolution and the related trends would have a deep social, economic and political impact that we are just starting to perceive. The digital revolution is ending up in a digital age “marked by the widespread use of digital technologies in different aspects of human activity” [28].

It is therefore imperative to change first and above all the educational system. Besides the introduction of digital competencies and of basic courses on what digitalization really represents, developing the ability to adapt to an unpredictable environment would be key assets for all the generations.

This would help us face the new threats that arise in front us from significant, well-coordinated disinformation campaigns, the widespread of fake news, deep fakes and related aspects [29]. This generates reactions at all levels and requires more and more a true private - public partnership as we are in all this together and no one can be on its one in this new frontier.

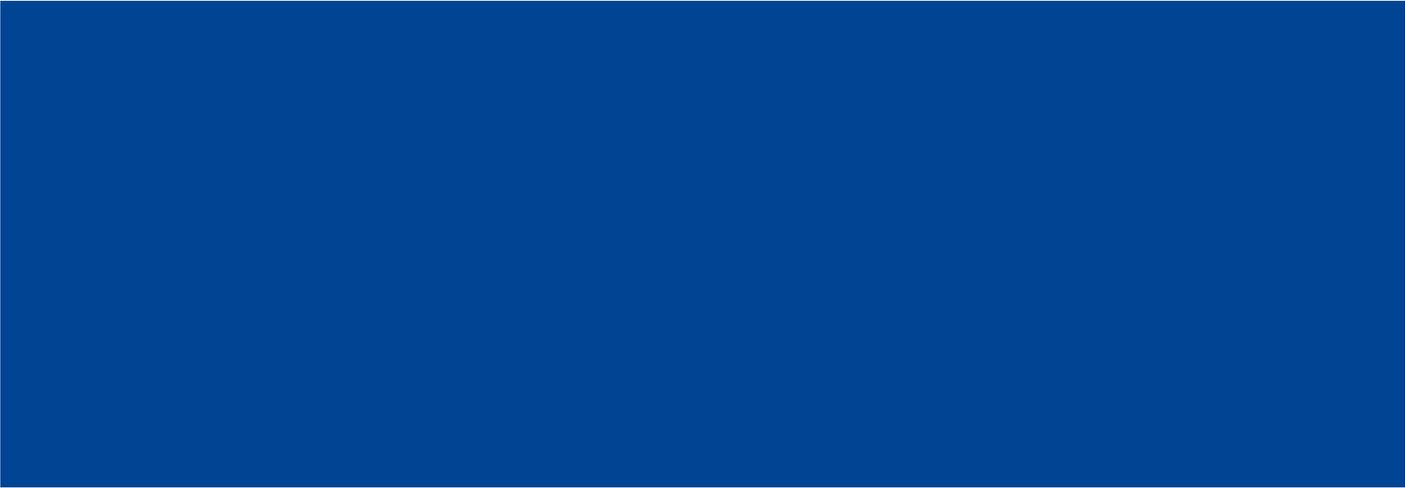
References

- [1] Hanson, Fergus, *A Digital DFAT: Joining the 21st Century*, Lowy Institute for International Policy, November 2010. Available at: https://web.archive.org/web/20101214094902/http://lowyinstitute.richmedia-server.com/sound/A_digital_DFAT.pdf [Accessed: 20 August 2019].
- [2] Tutt, Alexander, *E-Diplomacy Capacities within the EU-27: Small States and Social Media*, Master's Thesis, 2013. Available at: <https://www.grin.com/document/274032> [Accessed: 20 August 2019].
- [3] Shaun Riordan, *Cyberdiplomacy: Managing Security and Governance Online*, Polity, 2019, p. 5.
- [4] Riordan, Shaun, *Cyberdiplomacy: Managing Security and Governance Online*, Polity, 2019, pp. 5-6.
- [5] Barrinha, André & Thomas Renard, "Cyber-diplomacy: the making of an international society in the digital age", *Global Affairs*, 2017, p. 4.
- [6] United Nations General Assembly, *Resolution adopted by the General Assembly - Developments in the field of information and telecommunication in the context of international security A/RES/53/70*, 4 Jan. 1999. Available at: <https://undocs.org/A/RES/53/70> [Accessed: 20 August 2019].
- [7] United Nations General Assembly, *Resolution adopted by the General Assembly on 22 December 2018 - Advancing responsible State behaviour*

- in cyberspace in the context of international security A/RES/73/266. Available at: <https://undocs.org/A/RES/73/266> [Accessed: 20 August 2019].
- [8] United Nations Office for Disarmament Affairs, Developments in the field of information and telecommunications in the context of international security. Available at: <https://www.un.org/disarmament/ict-security/> [Accessed: 20 August 2019].
- [9] International Communication Unit (ITU), Global Cybersecurity Agenda (GCA). Available at: <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx> [Accessed: 20 August 2019].
- [10] U.S. Department of State, 21st Century Statecraft. Available at: <https://2009-2017.state.gov/statecraft/overview/index.htm> [Accessed: 20 August 2019].
- [11] U.S. Department of State, 21st Century Statecraft. Available at: <https://2009-2017.state.gov/statecraft/overview/index.htm> [Accessed: 20 August 2019].
- [12] U.S. Department of State, Policy Issues. Cyber Issues. Available at: <https://www.state.gov/policy-issues/cyber-issues/> [Accessed: 20 August 2019].
- [13] National Cyber Strategy of the United States of America, September 2018. Available at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> [Accessed: 20 August 2019].
- [14] H. R. 739 - Cyber Diplomacy Act of 2019. Available at: <https://www.congress.gov/bill/116th-congress/house-bill/739/text> [Accessed: 20 August 2019].
- [15] Council of the European Union, Draft Council Conclusions on Cyber Diplomacy, Brussels, 11 February 2015. Available at: <http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf> [Accessed: 20 August 2019].
- [16] Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber

- Activities ("Cyber Diplomacy Toolbox"), Brussels, 7 June 2017. Available at: <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> [Accessed: 20 August 2019].
- [17] Council of the European Union, EU to become more cyber-proof as Council backs deal on common certification and beefed-up agency, 19 December 2018. Available at <https://www.consilium.europa.eu/en/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/> [Accessed: 20 August 2019].
- [18] European Commission, Digital Single Market. Policy. Cybersecurity. Available at: <https://ec.europa.eu/digital-single-market/en/cyber-security> [Accessed: 20 August 2019].
- [19] Joint statement of the 22nd EU-ASEAN ministerial meeting, Council of the European Union, 21 January 2019. Available at: https://www.consilium.europa.eu/en/press/press-releases/2019/01/21/joint-statement-of-the-22nd-eu-asean-ministerial-meeting/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Joint+statement+of+the+22nd+EU-ASEAN+ministerial+meeting [Accessed: 20 August 2019].
- [20] Ministry of Foreign Affairs of Romania, Rolul MAE în domeniul securității cibernetice pe plan national [The role of the MFA in the area of cybersecurity on the national area]. Available at: <http://www.mae.ro/node/28366> [Accessed: 20 August 2019].
- [21] Mihai, Cosmin-Ioan, Costel Ciuchi, Gabriel Petrică, Current challenges in the field of cybersecurity - the impact and Romania's contribution to the field, European Institute of Romania, Bucharest, 2018. Available at http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf [Accessed: 20 August 2019].
- [22] Priorities of the Romanian Presidency of the Council of the European Union 1 January 2019 - 30 June 2019. Available at: <https://www.romania2019.eu/priorities/> [Accessed: 20 August 2019].

- [23] Cyber-attacks: Council is now able to impose sanctions, Council of the European Union, 17 May 2019. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/> [Accessed: 20 August 2019].
- [24] Digital single market for Europe, Council of the European Union. Available at: <https://www.consilium.europa.eu/en/policies/digital-single-market/> [Accessed: 20 August 2019].
- [25] Ministry of Foreign Affairs of Romania, Problematika securității cibernetice în cadrul organizațiilor internaționale și implicarea României ca membru al acestora [The issue of cybersecurity within the framework of international organizations and Romania's involvement as a member of them]. Available at: <https://www.mae.ro/node/28369?page=2> [Accessed: 20 August 2019].
- [26] Joint Statement from President of the United States Donald J. Trump and President of Romania Klaus Iohannis, 20 August 2019. Available at: <https://www.whitehouse.gov/briefings-statements/joint-statement-president-united-states-donald-j-trump-president-romania-klaus-iohannis/> [Accessed: 20 August 2019].
- [27] The increasing need for Cyber Diplomacy, Norwich University Online. Available at: <https://online.norwich.edu/academic-programs/masters/diplomacy/resources/infographics/the-increasing-need-for-cyber-diplomacy> [Accessed: 20 August 2019].
- [28] Sebe, Mihai, A Youth Strategy for Europe's future. The impact of the Digital Revolution on the European youth. Case study: Romania, Institute of European Democrats, Brussels, 2018. Available at: <https://www.iedonline.eu/publications/2018/sebe.php> [Accessed: 20 August 2019].
- [29] Bârgăoanu, Alina, #FAKENEWS Noua cursă a înarmării [#FAKENEWS The new arms race], Evrika Publishing, Bucharest, 2019.



DATA PROTECTION



DATA PROTECTION

GDPR - Enemy or Friend

Răzvan BĂRBIERU

“Alexandru Ioan Cuza” Police Academy, Romania
razvan.barbieru@academiadepolitie.ro

The European Parliament and the Council adopted on 27 April 2016 Regulation (EU) 2016/679 on the protection of individuals 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 - RGPD). It shall be binding on all Member States as from 25 May 2019.

Regulation (EU) 2016/679 imposes a unique set of rules on the protection of personal data, replacing Directive 95/46 / EC and, implicitly, the provisions of Law no. 677/2001 which regulates the personal data domain at national level.

As temporary benchmarks that can define the stages that led to the creation of the regulation we can remember:

- On January 25, 2012, the first proposals on GDPR materialization were developed;
- 21 October 2013 - The EU Parliament's Committee on Civil Liberties and Internal Affairs (LIBE) voted for this proposal;
- 15 December 2015: The EU Parliament, the Council of Europe and the European Commission concluded the negotiations and agreed on the terms of the proposal;
- 17 December 2015: LIBE Committee voted in favor of terms obtained through previous negotiation;
- April 8, 2016: The Regulation is adopted by the Council of the European Union with one vote against, Austria, which argued that the 1995 directive had some stronger aspects than the current regulation;
- April 27, 2016: EU Parliament adopts the regulation;

- May 24, 2016, 20 days after publication in the "Official Journal of the European Union", the regulation enters into force. Its rules will be directly applicable in all Member States two years after the date of publication.
- May 25, 2018, all Member States will begin to apply the regulation (cf. (Wikipedia)).

For a better understanding of what is wanted by creating and applying the GDPR, we should draw attention to 2 definitions as they are presented in the regulation.

"Personal Data" means any information relating to an identified or identifiable natural person ("the data subject"); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more many specific elements that are physically, physiologically, genetically, psychologically, economically, culturally or socially related (General Data Protection Regulation, 2016); Therefore, we can consider excluding other categories of data as being under the GDPR: name, surname, personal numeric code, email address, correspondence address, anthropometric data, genetic data, health data, geospatial data, data on online identification such as the IP offered by the Internet Service Provider, various accounts associated with online social media platforms, etc.

"Processing" means any operation or set of operations performed on personal data or on personal data sets with or without the use of automated means, such as collecting, recording, organizing, structuring, storing, adapting or modification, extraction, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (General Data Protection Regulation, 2016); From this definition we can see that processing our personal data is already part of our daily life: from receiving bills for various services provided to us, hiring in various companies, enrolling children at school, registering a vehicle, providing us with medical services, the conclusion of contracts, etc., all these activities involve in one form or another the processing of our personal data. In order to ensure the legality of the processing of these data, the legislator clearly defined the legal grounds on which it could perform these operations:

- the data subject has consented to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to the conclusion of a contract;
- processing is necessary to fulfill a legal obligation incumbent upon the operator;
- processing is necessary to protect the vital interests of the data subject or other natural person;
- processing is necessary for the performance of a task which is in the public interest or which results from the exercise of the public authority with which the operator is invested;
- processing is necessary for the legitimate interests pursued by the operator or a third party, unless the interests or fundamental rights and freedoms of the data subject that require the protection of personal data are prevalent, in particular where the data subject is a child.

It is essential and obligatory that prior to any collection and processing of personal data, consent is obtained and the correct information of the data subject is overcome: the right of access to data, the right to be deleted, the right to port the data.

In order to ensure compliance with the GDPR measures from the IT perspective, several measures are needed without, however, limiting us to them again. Below, I will illustrate some of the measures that I personally consider necessary to ensure a good protection of sensitive data at an organization level.

I. Measures relating to physical access

It is recommended that access to the places where personal data is processed be carefully monitored and monitored. Access can for example be made on the basis of access cards with other authentication devices. We can also provide video surveillance of access to the data processing terminal area and control access to data storage areas, whether we are talking about the server room or the archive where data is stored on

physical support. Sensitive sites such as server rooms or archives must be secured against unauthorized access. Installing an alarm system is also recommended. Also, consideration should be given to equipping rooms containing sensitive information with means of fire prevention and extinction detection. Installing automatic fire extinguishers can be costly, but an alarm and detection system has a reasonable cost for any company.

II. Measures concerning the electronic security environment

Unified management of accounts and access rights on company computers

Creating user accounts based on a request and a confidentiality engagement signed by the Holder and endorsed by a designated Managing Director. It is also necessary to instruct the user about the rights and obligations that he / she has in his / her current activity.

Establish common policies on all stations in the company regarding the length of the password used, the degree of complexity, the number of previous passwords retained.

Activate intrinsic operating system audit mechanisms and collect and save audit files for a sufficiently long period of time. This helps the investigator to detect breaches and provides real support in identifying unauthorized access mechanisms in the system.

Analyzing the integration of computers in Active Directory

Active Directory allows centralized storage of user information (including login credentials on each PC), devices and access rights. Unlike a decentralized PC network, where credentials are stored at the level of each station, storage of users and passwords in a single protected location brings major security benefits. It is much easier to protect a single location (Active Directory servers) than it is to protect users and passwords saved on each PC on the network. Using a single user password can generate access to multiple shared resources from its own computer network via Active Directory.

Define security policy and Group Policy settings on your network PCs.

The centralized definition of security policies ensures uniformity in ensuring a level of security across the network. Although security templates can be defined and used individually on networked stations, AD use the help of administrators by providing them with a powerful tool.

Any IT security deployment in a computer network starts from establishing PC security policies, defining them in Active Directory, and automatically deploying them on all computers in the network. You can set templates about password size, complexity, number of allowed attempts, deactivated services, software allowed to run, Internet access or not.

Active Directory can be used alongside other services such as DNS server or file server, which allows the creation of secure storage in which the rights to folders and files can be easily managed.

Create a list of Hardware and Software approved for use at the organization level

Effective management of hardware and software resources is essential to ensure an efficient use of IT infrastructure, IT services and security. It is essential to have an up-to-date inventory of all network hardware components. This allows for prompt intervention in case of vulnerabilities of various equipment.

From a security perspective, software inventory helps the company identify and address potential threats by ensuring that end-of-life products are decommissioned and that products and patches are updated in a timely manner. (A good example is to avoid using the Windows XP operating system on Internet because the connected PCs it has no support from the manufacturer).

Encrypting data

To ensure data security, encryption mechanisms are typically defined around the two states where data can be located:

- At Rest (Rest): This brings together all information storage media, and types that exist statically on physical media, either magnetic or optical discs. "At

rest encryption" means that the data is stored encrypted. So to get access to them you need a key. This mechanism represents a defense method against an attacker who manages to gain physical access to the data stored on the computer.

- In-Transit: When transferring data between components, locations or programs, such as in a local network or the Internet, it is considered to be moving. It is recommended to use secure communication protocols over the Internet or network: TLS, SSL, HTTPS.

In terms of the GDPR regulation, data encryption is not mandatory but is referred to as the recommended protection measure. Additionally, implementing the GDPR-mandated Data Protection by Design and Default principle involves encrypting sensitive data.

Another advantage of data encryption from the GDPR point of view is to avoid the obligation to notify the data protection authority, for example, if a laptop is lost, if the data on it is protected by encryption. The encryption measure is within reach of the user when using the Windows 10 professional operating system by enabling the bitlocker function. There are also a number of commercial and free solutions available on the market that can ensure a strong enough encryption.

Today's smartphones or Android and iOS tablets have implemented data crunching features. They can both encrypt the internal data stored on the device memory and the Ex memory card. When you store sensitive organization data, it is recommended that you activate these features.

If a mobile device used in the interest of the organization contains sensitive data, it is important that the implicit functions used to find it remotely and delete the data are activated. Also, you may need to activate the functions of automatic locking and unlocking with pin or fingerprint. "Find my device" app allows to locate the device and possibly delete data from a distance. There are also commercial solutions that allow remote deletion of data from terminals in case of loss or theft. The value of the terminal itself is small for the company but most of the times the data stored on these terminals are either sensitive or valuable to the competition.

It is also recommended to use other encryption for sensitive data stored on server systems and database systems.

Encrypting in-transit data:

SSL certificates

The use of SSL certificates is recommended for all company web properties, whether websites or applications. The use of SSL certificates provides encryption of data in transit through the Internet and / or local area network. Also, when using e-mail servers, it is recommended to use secure connections for POP3, IMAP and SMTP protocols, or to use webmail versions of HTTPS connections.

VPN networks

A virtual private network (virtual private network, abbreviated VPN) expands a private network over a public network such as the Internet. Allows a computer or a network-connected device to send and receive data over public or shared networks as if it were connected to the private network while benefiting from functionality, security, and public network policies. It is recommended to deploy a VPN solution that implements advanced encryption protocols (eg L2TP, IPSEC, or OpenVPN), and avoiding the use of PPTP variants.

VPNs can also be used to protect sensitive data communications between servers from external data centers or from cloud and client stations. In these cases, it is recommended to deploy a site to site VPN solution to securely link the server network to the client network.

If we collect data via SNMP it is recommended that you change the default community and you restrict SNMP to read-only. Where it is possible, always try to use SNMPv3.

Disaster recovery implementation

Depending on the importance of the company's server infrastructure, data processing within the company requires the development and implementation of a Site

Recovery policy to a lesser or greater extent. It is recommended that there be minimal backup sets for important company data, possibly physically relocating these backups to different locations, which would allow successful data recovery in the event of a disaster. A variant to consider is a backup solution in the cloud. There are commercial solutions that provide secure and encrypted storage space.

Since the implementation phase, it is important in our opinion to test a disaster recovery scenario. This meant testing the backups, restoring the databases from them, restoring the applications and infrastructure of the active directory from the backup in an alternative location, testing the functionality of the entire infrastructure.

Although the GDPR regulation was conceived as a measure of protection of the citizens of the European Union against the excessive processing of personal data, of the tendency of the big companies of profiling their data, we consider that this brings a profit and the organizations because for the first time they force them to take measures technical and organizational to respect the collection, processing, storage and manipulation of personal data. Without elaborating and applying this regulation, it is difficult to specify if the organizations would have taken measures that would lead to the respect of the rights of the citizens of the Union regarding personal data.

Areas of Challenge in Data Protection for IT Systems

Larisa GĂBUDEANU
Babeş-Bolyai University, Romania
larisagabudeanu@gmail.com

1. Approach of companies towards data protection compliance

Recent legislative changes in the data protection area have resulted in changes made by companies in the private sector to their internal processes, client documentation and IT systems.

As most companies also have an IT component, a significant amount of internal policies, procedures and measures related to data protection within the life cycle of data in IT systems have been updated, from collection of data from individuals or from other entities, analysis of data, transfer of data to other entities (within or outside the same group of companies) and storing/archiving.

In view of guiding companies in this respect, there have been various researches and guidelines in recent years focusing on privacy management program (such as OASIS [1]), development of software taking into account the privacy by design and privacy by default principles (such as ENISA for software development [2] and for big data solutions [3], OASIS [4], the PRIPARE project [5]) and identification of privacy risks (LINDDUN project [6]). Nevertheless, further research and standardisation on these points is ongoing, together with an increase in the maturity of privacy compliance in organisations.

Out of the steps to be implemented for privacy compliance, we are outlining below certain challenges that have to be correlated with IT security measures implemented within the company, either concerning IT systems (Section 2) or at the organisational level (Section 3). Section 4 summarises the main directions of future research in relation to the challenges identified herein.

2. Data protection challenges concerning IT systems

The challenges in terms of IT systems differ between legacy IT systems and software/IT solutions in the process of being developed, while some common types of challenges for the two situations exist as well.

Most companies have legacy IT systems in place, which have been changed over the years based on the business needs of the company. These types of systems require significant time and entail costs to be modified in order to address matters such as deletion of personal data (upon request or at the fulfilment of the retention period), data minimisation, and information security measures (or update thereof based on latest state of the art in this respect).

In addition, in order to identify the cases of changes to the IT ecosystem requiring a data protection analysis, an internal trigger in the approval process for the change (if the change is a change in the flow of data or a change in the technical solution) could be implemented.

For new IT systems being developed, as per the privacy by design principle, data protection can be embedded into the software or IT solution from the outset, during the development process. This entails, for the cases where data protection impact assessments are required, for the measures established under this assessment in view of minimising risks toward individuals to be taken into account as well during the development process. Internal methodology for data analysis can have as starting point guidelines issued by EU [7] or local authorities [8].

Privacy by design entails a multidisciplinary effort from the departments related to software development, data protection, information security and the business owner for the project (to complete the business logic and data flow specifics). These should be analysed as having the role of main stakeholders to be involved in the data protection analysis. When third party entities are involved in the development process, they have to participate in the data protection analysis as well.

The internal organisational steps to establish such cooperation throughout the development process requires controls being set in place in this respect in correlation with IT security and data protection requirements.

To some extent, the development team should have knowledge of the main data protection and security requirements when preparing the architecture of the IT system.

In this respect, in order to ensure efficient risk analysis and risk management, steps in the data protection analysis may be distributed between the development team (including business owner) and the privacy/information security teams.

For the development team, certain guidelines can be provided based also on prior experience with development within or outside the company. Such guidance should focus on the main types of data processing and data sharing: collection, analysis, transfer/disclosure to third parties, storing and archiving.

Nevertheless, there are some aspects that should be analysed from the outset by privacy team together with the security team. One approach in this respect can be the creation of triggers for such escalation. The triggers may be defined based on the activity of the company and may include matters such as: certain types of data being processed (for example, health data, data of children), automated decisions, profiling, transfer of data to a state not having an adequate level of protection of personal data.

In addition, after the initial analysis of the IT solution is developed, the data protection analysis (together with the security analysis) has to be repeated throughout the life cycle of the IT solution, respectively, during the implementation of the solution, the testing the implementation, the maintenance for the software and the implementation of change requests for the software.

However, the requirements for implementation of privacy by design should be established from the outset of the development process [9]. In addition to integration with existing IT systems, this approach ensures also integration with existing privacy policies and end-to-end privacy compliance. Some data protection requirements may entail technical developments (such as additional infrastructure, additional specifications to be included in the source code). By a constant updating of the privacy team on the envisaged architecture, the company can avoid delays and changes to the initial architecture.

Of course, the above aspects might be implemented slightly different, depending on the development methodology used. For waterfall, data protection analysis may be

conducted on the initially agreed architecture of the solution. However, for agile (including scrum), the changing architecture of the solution with each sprint (and sometimes within the sprint) has to be taken into account. Depending on the timeframe for the project and flexibility in adjusting the source code, more frequent or less frequent interactions with the privacy team within the company are useful.

As mentioned above, for involvement of third parties, specific internal policies have to be set in place. These should address the development of software by third parties or by the company together with third parties.

In addition, third parties providing specific IT solutions can have a significant impact on privacy management. For instance, the use of cloud service providers has also increased in companies from various sectors. In such cases, data protection requirements and controls have to be adapted to the specifics of the IT solution and correlated with the information security legal requirements.

In both cases, of existing or of projected IT systems, there are certain aspects that have to be correlated with the internal cyber security policies and procedures:

a. The amount of data processed in the IT system and access to this data. This relates to the data minimisation and need to know principles under data protection legislation, but also to IT security principles related to access management.

In general, the implementation of these principles involves some software development, acquisition of new IT systems or re-use of IT systems implemented for IT security, changes to the amount of data shared with third parties in order to reflect only the data needed for the sharing purpose.

On the data minimisation, [10] the main implementation challenges refer first to the collection of only data relevant for the purpose of the data processing. Subsequently, once stored in the IT systems, for a specific purpose only the data needed for such purpose should be used. Further, for any subsequent purpose, legal basis for such subsequent processing should be identified [11]. The same approach is applicable in case of transfer of data to third parties who are acting as data controllers or data

processors. In this manner, the implementation of the data minimisation principles also contributes to the security of the personal data stored in the IT systems.

In some cases, it may be possible to use pseudonymised or anonymised data for a particular purpose, especially in the case of data analytics aimed at providing statistics. The legal doctrine ([12], [13]), technical researches ([14], [15], [16]) and technical capabilities at a given point in time on this topic have to be taken into account when determining if steps taken on a dataset result in anonymised or pseudonymised data.

Further, from an access management perspective, these principles entail the creation of internal processes for granting of access to the IT systems, for having traceability on decisions to grant access rights and mechanisms in place for removal of access rights when these are no longer needed. This process relies on the prior identification of the individuals that are requesting access to the IT systems.

b. Security measures under data protection legislation. Aside from the measures mentioned under item (a) above, for data held in IT systems, technical and organisational measures relating to the confidentiality, integrity, availability and resilience of personal data has to be implemented for both data at rest and in transit (including encryption and pseudonymisation of data where the case). Effective monitoring of these measures is essential in view of identifying any incidents relating to personal data, together with proper logging in view of investigation and documentation of any such incidents. Further, the incident investigation, documentation and consequence analysis has to be correlated with other legal obligations in this respect (such as the NIS Directive or business sector requirements).

Further, under the data protection legislation, a particular emphasis is made on the availability of access to personal data. In this case, steps have to be taken in order to ensure the availability of services offered to individuals. For this reason, planned outages for updating of software should be performed when used less by individuals and announced in advance, with alternatives to the online service being provided to individuals.

IT monitoring solutions are also usually implemented (such as web application firewalls, data loss prevention solutions, IPS, IDS) in view of ensuring information protection. Such tool may also be considered for the implementation of some of the security requirements under the data protection legislation. However, as the use of such tools may involve analysis of personal data, creation of profiles and automated decisions towards individuals, the implementation of the IT monitoring solutions (including rules and consequences on individuals) should be analysed from a data protection perspective. Auditing and penetration testing of IT solutions have been expressly referenced in the data protection legislation. In this respect, a company should correlate its IT security measures in this respect with the data protection angles as well. This approach may be useful in view of streamlining the analysis and documentation for the two perspectives (IT security and data protection). Further, this dual approach has begun to be contemplated by authorities as well (Ministry of Communication for internet banking, data protection authorities when assessing the implementation of security measures for data processing [17]).

Certain guidelines have been published in this respect by ENISA (general security measures [18] and specifics for SMEs [19]) and by local professional associations [20] provide a starting point for updating the internal set of policies and procedures in terms of security measures from a data protection perspective.

c. Logging. Logging is essential in ensuring traceability of actions performed in relation to personal data. Aside from identification of access to personal data and integrity of personal data, this is useful when investigations are needed, either in case of data breaches or investigations from authorities or courts. Thus, logging can be used for investigations relation to confidentiality, integrity and availability of data. Triggers may be created in case specific events affecting the personal data occur. In addition to the above, logs themselves may include personal data. Thus, an analysis on the implementation of privacy principles for logs should be made at the moment the types of logs are established, such as retention period, access management to logs.

3. Organisational data protection challenges

From an organisational perspective, implementation of data protection requirements should be adapted to the specifics of the company and to its interactions with third parties.

In terms of third parties, the data protection legislation places certain obligations on the company that involves third party data processors in the data processing. Some of the below aspects may be useful to be analysed for transfer to other data controllers or to joint data controllers.

Further, such recent legislation imposes directly or indirectly certain obligations on vendors providing services and processing personal data (for example, processors under GDPR, NIS directive).

In relation to these obligations, companies can set in place risk assessment methodologies for choosing data processors and audit procedures for such third parties. Companies can require cyber insurance policies from data processors (which usually contain some components of data protection related insurance) and can request processes to be established for data subject requests and for privacy by design for IT systems involved in the data processing. In view of proper implementation, processes and activity flows are to be integrated with vendors for smooth implementation of compliance.

This approach raises implementation issues, especially in case of SME vendors and vendors having a large number of clients, with potential solutions on this topic including standardisation and certification.

Firstly, the implementation by vendors of security measures required by their clients leads to inconsistencies in approaches by the vendor and additional costs for vendors. In this respect, standardisation of security measures in a specific sector or certification schemes may prove useful to minimise the impact in terms of costs and time required for implementation of security measures.

Secondly, auditing vendors requires additional time and costs for clients and vendors, including reducing time staff spends in production or additional staff hired for auditing. In addition, multiple audits from clients of vendors may result in different

measures established to be implemented for the vendor. Further, for data protection, industry wide standardisation in auditing methodology has not been reached at present.

When data processors are included in the data processing, there are other aspects that should be established from the outset on the sharing of data and on the cooperation between the two entities, with some of these aspects to be implemented also in the IT systems used for the data processing and data sharing. The access management procedure mentioned in Section 2 above has to be extended to the data processors and, if the case, to the sub-processors. Matters relating to exercise of data subject rights, implementation of retention periods and data breach investigations may have an impact on the architecture of the IT systems of both the company and its data processor for establishing a correlated approach in this respect. For assistance during investigations from authorities and during litigation related to data processing, swiftness in communication of relevant information is essential.

The use of sub-processors by the data processor involves a replication of the obligations and warranties given by the data processor. In terms of security of personal data, usually the obligation for verification of level of security measures of the sub-processor is undertaken by the data processor. However, in certain cases that involve processing of certain types of data (such as health or banking sector), the data controller may decide to perform the auditing of the sub-processor itself.

From a contractual point of view, addressing the above obligations of the data processor through liability and warranty clauses may prove insufficient in terms of recovering the prejudice incurred. For this reason, it may be useful to use standardisation of approaches in a specific sector.

The above organisational points on establishing processes for compliance with data protection requirements when involving third party data processors, together with proper auditing of the privacy management plan are applicable also for the internal organisation of a company. The data flows between departments in a company and the life cycle of data in a company and through the IT systems within a company should also reflect the data protection principles mentioned above.

In addition, the internal processes for changes in data flows within the IT systems in a company should cover, aside from the technical changes needed, the analysis of IT security and data protection implications.

In view of ensuring implementation of such internal processes, training of employees is essential. From an organisational perspective the findings mentioned recently by ENISA in a study about the cyber security culture within a company [21] are relevant also for data protection compliance, as the human factor is essential in this respect.

4. Conclusions and recommendations for future research into handling data protection challenges

As detailed above, for data protection concerning IT systems, there are certain implementation challenges, especially given the various levels of maturity in terms of privacy management between the companies in the market and between various sectors of the economy (while correlating these with other relevant requirements, such as the NIS Directive or other sector security requirements and including incident identification, management and remedies implementation as well). For these challenges, some suggested approaches are listed below.

These approaches may be useful also for SMEs, especially when these are vendors or service providers for other companies, as they can hold a large amount of personal data.

In certain sectors (such as banking, energy, health), professional associations have discussed the adoption of codes of conduct for their members in relation to protection of personal data. This type of standardisation may be useful in terms of raising awareness and maturity among the companies from that sector. In practice, it has been complemented by specific regulatory requirements (for security and, in some cases data protection) in certain specific areas, such as internet banking services, open banking or insurance sector.

Another mechanism for ensuring a common level of data protection compliance could be the setting-up of certification schemes (similar to the recent approach adopted

at the EU level for cyber security). Nevertheless, it may be useful to have more specific certifications, for a particular types of service or a particular types of sector of the economy rather than a general data protection legislation certification.

As in other sectors, auditing may also be useful in view of standardisation and may be a prerequisite of the certification schemes. Auditing methodologies may be considered only for data protection matters or may be correlated with IT security audits.

Until this moment, there have been some standardisation and auditing methodologies designed. For example, GAPP [22] has been created as methodology to evaluate the maturity level of a company in terms of data processing. NIST has embedded the privacy aspects in its security documentation (for example NIST 800-53 on controls in IT systems for security and data protection) and has begun discussions for a privacy framework [23].

The above suggestions in relation to standardisation in implementation of data protection requirements also have an impact on IT systems or are related to IT security principles, in relation to certain aspects, including those detailed in the above sections.

References

- [1] OASIS, "Privacy Management Reference Model and Methodology (PMRM) Version 1.0," [Online]. Available: <http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html>. [Accessed 30 May 2019].
- [2] ENISA, "Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default," 2019.
- [3] ENISA, "Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics," 2015.
- [4] OASIS, "Privacy by Design Documentation for Software Engineers Version 1.0," [Online]. Available: <http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/pbd-se-v1.0.html>. [Accessed 30 May 2019].

- [5] PRIPARE, "A New Vision on Engineering Privacy and Security by Design," [Online]. Available: <http://pripareproject.eu/research/>. [Accessed 30 May 2019].
- [6] "LINDDUN - Privacy threat modelling," [Online]. Available: <https://linddun.org/>. [Accessed 30 May 2019].
- [7] European Data Protection Board, "Guidelines on Data Protection Impact Assessment," [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. [Accessed 31 May 2019].
- [8] CNIL, "DPIA guidance," 2018. [Online]. Available: <https://www.cnil.fr/en/privacy-impact-assessment-pia>. [Accessed 31 May 2019].
- [9] Norwegian Data Protection Authority, "Big Data - privacy principles under pressure," 2013. [Online]. Available: <https://www.datatilsynet.no/en/about-privacy/reports-on-specific-subjects/big-data--privacy-principles-under-pressure/>. [Accessed 31 May 2019].
- [10] Danish Data Protection Authority, "Sanctions for lack of data minimisation," 2019. [Online]. Available: <https://dataprivacy.foxrothschild.com/2019/03/articles/european-union/danish-data-protection-authority-dings-cab-company-for-data-minimization-violations/>. [Accessed 31 May 2019].
- [11] Working Party Article 29, "Opinion 3/2013 on purpose limitation," 2013. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. [Accessed 31 May 2019].
- [12] Working Party Article 29, "Opinion 05/2014 on Anonymisation Techniques," 2014. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. [Accessed 31 May 2019].
- [13] Working Party Article 29, "Opinion 4/2007 on the concept of personal data," 2007. [Online]. Available: <https://ec.europa.eu/justice/article->

29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

[Accessed 31 May 2019].

- [14] ENISA, "Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation," 2019.
- [15] W. Winkler, "Re-identification Methods for Masked Microdata," *Privacy in Statistical Databases*, pp. 216- 230, 2004.
- [16] G. Nelson, "Practical Implications of Sharing Data: A Primer on Data Privacy, Anonymization, and De-Identification," [Online]. Available: https://www.researchgate.net/publication/318866074_Practical_Implications_of_Sharing_Data_A_Primer_on_Data_Privacy_Anonymization_and_De-Identification. [Accessed 31 May 2019].
- [17] Infosecurity Magazine, "Polish Data Protection Authority GDPR fine," [Online]. Available: <https://www.infosecurity-magazine.com/news/polish-regulator-issues-first-gdpr/>. [Accessed 31 May 2019].
- [18] ENISA, "Handbook on Security of Personal Data Processing," 2018.
- [19] ENISA, "Guidelines for SMEs on the security of personal data processing," 2017.
- [20] IT Security Association Germany (TeleTrust), "Guideline State of the Art - Technical and organisational measures," [Online]. Available: <https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/>. [Accessed 30 May 2019].
- [21] ENISA, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity," 2019.
- [22] American Institute of CPAs (AICPA) and Canadian Institute of Chartered Accountants (CICA), "Generally Accepted Privacy Principles (GAPP)," [Online]. Available: https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf. [Accessed 31 May 2019].
- [23] NIST, "NIST Privacy Framework," [Online]. Available: <https://www.nist.gov/privacy-framework/working-drafts>. [Accessed 31 May 2019].



ABOUT THE AUTHORS



ABOUT THE AUTHORS

About the Authors

List of authors (in alphabetical order by last name):

Iulian ALECU is the Deputy General Director of the Romanian National Computer Security Incident Response Team (CERT-RO), with an experience of more than eight years in cybersecurity and related international cooperation. He was the Chair of the Cooperation Group during the Romanian Presidency at the Council of the European Union.

Sabina-Daniela AXINTE received BSc in Electronics and MSc in Quality and Reliability Engineering, both from UPB. Advocating for an enhanced and modern learning approach, her areas of expertise are software quality assurance, education and information security. Now she is PhD candidate at the ETTI-B Doctoral School, her researches being focused on verification and validation techniques for LMS systems.

Ana BADEA-MIHALCEA is an expert at the National Cyberint Center, which is the national cyber-intelligence authority with the role of identifying, preventing and countering vulnerabilities, risks and threats to Romania's cyber security. The Center provides legal beneficiaries with the necessary information to prevent and manage the consequences of cyber attacks against IT&C systems in Romania.

Răzvan BĂRBIERU is a police officer engineer at the "Al. I. Cuza" Police Academy in Bucharest. In 2006 he graduated from the Polytechnic University of Bucharest. Between 1999 and 2017, he served as network administrator and security administrator in various central structures of the Romanian Ministry of Defense. Since 2017 he has been working as a network administrator at "Al. I. Cuza" Police Academy.

Mircea BORCAN is an expert of the General Directorate for Communications and Information Technology. The author graduated the Military Technical Academy in Bucharest as head of promotion. He contributes to the elaboration and implementation of the security mechanisms for the communications network of the Ministry of Internal Affairs. He owns many certifications in the field of networking and security.

Jon BROWNING is the Deputy Director for Digital Government at the UK National Cyber Security Centre. His team provide support to Central Government, Local Government, the Health Sector, Emergency Services, Devolved Administrations and the Crown Dependencies and Overseas Territories, making it easier for the public sector to secure its digital services.

Daria CĂTĂLUI is a cyber security training and awareness professional starting back in 2010 as trainer for national organisations then for EU's cyber security agency ENISA, the European Commission or the Romanian Presidency of the Council of the EU. She had the chance to kick-off and help scale up for impact the following projects: EC Cyber Aware and CyberReadyGame, European Cyber Security Month, NIS quiz.

Claudiu CHIRIAC is a R&D officer working for the Center for Scientific Research Coordination. With a master's degree in economics and international affairs, the main responsibility is the management of the projects funded under R&D programmes and sectorial plan of the MoI. As a PhD student is author/co-author of various articles indexed in international databases and published in conference proceedings.

Costel CIUCHI, PhD, is a Senior Expert in the Information Technology Directorate, General Secretariat of the Government with responsibilities in developing government apps and infrastructure, security of IT services (INFOSEC) and coordinating Gov.ro Domain Registry. Associate Professor at University Politehnica of Bucharest, he conducts research activities in decision making, cybersecurity and security risk area.

Carmen-Elena CÎRNU, PhD, Senior Researcher II, is the Head of the Cybersecurity and Critical Infrastructure Department at ICI Bucharest and Vice-President of the Scientific Council at ICI Bucharest. She is an Aspen Institute Fellow, former Guest Researcher at Global Security Research Institute Japan, former Parliamentary Advisor and former Advisor to the Minister of Communication and Information Society.

Ioan CONSTANTIN got his BSc degree from “University of Craiova” with a thesis on cyber criminology and since then his main focus was to build a career in the field. He has in-depth knowledge on all-around IT Security Technologies and management systems having received numerous professional certifications such as the UKAS ISO27001 Architecture & Implementation.

Alexandru-Cătălin COSOI is the Bitdefender's Chief Security Strategist. He wears many hats, from energizing and publicizing the company's technological progress from within the CTO Office to leading the cyber-intelligence team tasked with helping international law enforcement agencies fight cybercrime. Alex is also a member of the Internet Security Advisory Group at Europol and Bitdefender’s liaison with Interpol.

Arthur DE LIEDEKERKE joined CERT-EU in 2018. He is currently working on External Affairs, Policy and Administrative matters. He previously worked in the European Parliament as an accredited assistant, on foreign affairs and security issues. He holds two masters’ degrees - in geopolitics and international relations - from King’s College London and the University of Maastricht.

Mihai-Ștefan DINU, PhD, is a senior researcher at the Information Systems and Cyber Actions from the Security and Defence Faculty in Carol I National Defence University, Bucharest. With two won scholarships in national security domain, he is also an expert of Strategikon Think Tank and Associate Member of Military Sciences Section of Academy of Romanian Scientists.

Viorel GAFTEA is a Scientific Secretary within the Romanian Academy - Science and Information Technology Section. With an extensive experience in IT&C management, administrator for national wide networks and systems, he was member in EC working groups and in various national working groups for elaboration of “Digital Agenda 2020”, “National Plan NGN” and “Romanian Academy” Strategies.

Larisa GĂBUDEANU is a data protection professional and a PhD candidate with the Babeş-Bolyai University. With a vast experience as a lawyer in an international law firm, counselling international clients and coordinating projects related to IT law and data protection matters, she also has good knowledge of information security gathered in a regional banking group and from her academic background in information security.

Andrei IANCU is the head of the Networks Department within the General Directorate for Communications and Information Technology from 2017. Under his coordination, the department manages the security of the Ministry of Internal Affairs wide area network and perimeter network. The author also participated in many international missions providing technical expertise in the networking and security field.

Angela IONIȚĂ is a Senior Researcher I and Deputy Director at the Institute for Artificial Intelligence of the Romanian Academy and has over 40 years of experience in the field of Research and Development in Computer Science. She has coordinated many national and European research projects and participated in various groups for development of strategies.

Andrei-Sorin JERCA is a cyber security expert, with a good proficiency in project management along with a goal-oriented work focused capacity, deep understanding and strong technical knowledge in penetration testing, cyber security incident handling, design and implementation of cyber security policies and best practices, software programming and privacy of web applications, computer systems and networks.

Matt LAVIGNA is President and CEO for the NCFTA (National Cyber-Forensics and Training Alliance), a U.S. based public-private consortium committed to identifying, mitigating, and disrupting significant cyber and cyber enabled threats. Prior to the NCFTA, Matt spent 26 years investigating and overseeing financial and cybercrimes as an agent with the United States Secret Service.

Ioan-Cosmin MIHAI is a cybersecurity and cybercrime researcher, professor, trainer and conference speaker. He is Associate Professor at “Al. I. Cuza” Police Academy, “Carol I” National Defence University, the University Politehnica of Bucharest, Romania, and Honorary Professor at the CT University, India, where he is teaching disciplines related to information technology, cybersecurity and cybercrime.

Liviu MORON works as IT service manager in the Security Assurance team for the European Commission. In the past he worked for companies like Unibail Rodamco, Palais des Congres de Paris, Certsign, BCR. He is a GIAC certified professional (GPEN, GXPN, GMON). He is involved in many projects (Cybershare, GovSec) that want to help public and private entities to share good practices in cybersecurity.

Alexandru OZARCHEVICI is a cyber security expert with major focus on SIEM security design review and recommendations, technical data gathering and cyber security incident handling, with deep understanding and strong technical knowledge in penetration testing and in design and implementation of cyber security policies and best practices.

Robert PĂTRĂNCUȘ is a criminal intelligence analyst and an investigator, a police officer specialized in countering trans-border organized crime, with a professional background in law enforcement and a valuable work experience spreading over 16 years, of which 7 years at international level. His scope of work covers mainly multi-layered cases of drug trafficking, terrorism and cybercrime.

Gabriel PETRICĂ has an extensive experience acquired in over 25 years of work in ICT field. With a PhD in Electronics, his area of interest includes the dependability of systems, Web programming, and information security. Currently, the author performs teaching and research activities within the Faculty of Electronics, Telecommunications and Information Technology - University Politehnica of Bucharest.

Cătălina PISARGIAC is an expert at the National Cyberint Center, which is the national cyber-intelligence authority with the role of identifying, preventing and countering vulnerabilities, risks and threats to Romania's cyber security. The Center provides legal beneficiaries with the necessary information to prevent and manage the consequences of cyber attacks against IT&C systems in Romania.

Georgios PSYKAKOS joined the European Institutions in 2015 as leader of the CERT-EU CSOC and is currently working in Strategy and Cyber Security Operations sector. Since 2009, he has been providing his country's National Authorities with cyber-security. He has extensive experience in security intelligence and counter-intelligence. He holds an MSc in Computer Security.

Călin M. RANGU, PhD, MBA, Ec, Eng, is acting as Director in Romanian Financial Supervision Authority (FSA), President of Institute of Financial Studies, Vice-president of EIOPA InsurTech Task Force, President of Shareholder Group in Consumer Protection, Board Member of EFICERT, Coordinator Fintech HUB. He has a broad experience in management, financial & banking, operational risks, IT security.

Mihai SEBE is currently an expert in European Affairs and Romanian Politics, European Institute of Romania. He is an editor of the Romanian Journal of European Affairs and member in the scientific committees of several international publications and think-tanks (Institute of European Democrats). He has obtained a PhD in Political Sciences at the University of Bucharest.

Viorel SÎNPETRU is an expert at the National Cyberint Center, which is the national cyber-intelligence authority with the role of identifying, preventing and countering vulnerabilities, risks and threats to Romania's cyber security. The Center provides legal beneficiaries with the necessary information to prevent and manage the consequences of cyber attacks against IT&C systems in Romania.

Virgil SPIRIDON serves as Head of Operations of the Cybercrime Programme Office based in Bucharest, responsible for managing the cybercrime projects on capacity building of the Council of Europe. He was the head of the Romanian National Cyber Crime Unit from 2003 to 2012, where he created and developed the Cybercrime Unit in Romania and established the cybercrime strategy for the Romanian National Police.

Virgilius STĂNCIULESCU is the Director of the IT and Data Protection Division, ANCOM. With an experience of 20 years in ICT looking forward to strategical and technical challenges imposed by digital evolution, Virgilius is trying to lead ANCOM on the way of digital transformation. His vision is a digital ANCOM, with safe, interoperable IT distributed systems.

Mircea-Constantin ȘCHEAU is PhD in Public Order and National Security with a theme of interest for the economic and security domains - *Cybercrime regarding Financial Transfers*. Author and coauthor of three books, more than twenty scientific articles in the field of management, economy, law enforcement, defense, critical infrastructures, information technology and lector to many international conferences.

Tara TRICKETT is a policy specialist with the NCFTA (National Cyber Forensics and Training Alliance). She works with independent colleges to meet their cyber security needs through the development of a collaborative group that works together to develop policies and practices to protect their networks. Tara holds degrees in Network Administration and Cyber Security.

Mădălin VASILE is a network and security specialist with more than 15 years of relevant experience. He joined Fortinet in 2011 as a Presales Systems Engineer and he is supporting Romania, Balkans and Adriatic region. As part of the Fortinet team, Mădălin designed and influenced security solutions for Datacenter, Internet Service Providers, Webhosting and complex networks covering different technologies.

Adrian-Victor VEVERA, PhD, Senior Researcher II, is the Technical Director and member of the Scientific Council of the National Institute for Research and Development in Informatics ICI Bucharest. He has extensive experience in the field of national security, fulfilling various managerial and advising positions in different state organisms.

Cătălin ZETU is leading the Cyber Attacks Office, part of the Romanian Central Cybercrime Unit, with wide responsibilities from investigations, to intelligence and strategy. Cătălin is developing strong partnership with private partners in order to bust the overall capacity of the unit. He is a very experienced cyber crime investigator that worked or supervised high profile cases with multiple international ramifications.



Romanian Association
for Information Security Assurance

Romania, 2019