GFA CONSULTING GROUP

NEWSLETTER 02 | 2020

IMPROVING CYBER RESILIENCE IN EASTERN PARTNERSHIP COUNTRIES

EDITORIAL

In recent months, the Covid-19 pandemic and its global implications have meant serious challenges for governments, businesses and individuals alike. GFA projects all across the world are not exempt from this unprecedented situation. Our project teams have to react fast and to acute needs. Many of our readers will have experienced similar challenges.

The project we recently started and showcase in this newsletter, CybersecurityEast, is affected as well. Its objectives remain relevant while the onslaught of the pandemic called for addressing pressing needs first, and subsequently for adjusting activities and strategies to the new context. Currently, we are approaching a phase in which our consultants – aside from technical needs – will be tasked with offering conceptual advice on addressing the implications and effects of the Corona crisis within their specific sector. Against this backdrop, we consider our work on cyber resilience as relevant to the current situation. There is a need to find reliable and safe digital solutions in many fields of daily life, from video conferences to the electronic exchange and sharing of increased amounts of data. This observation emphasizes the importance of a safe cyberspace. Cybercriminals, for example, are already trying to take advantage of society's increased reliance on the digital space by Corona-related cyberattacks and crimes such as phishing, malware attacks, malicious homepage registrations or fraudulent advertisements. In light of all the alarming pandemic news, we at GFA wish everyone to keep body and soul in good health and get through the Corona crisis unharmed.

Anja Desai
Managing Director
GFA Consulting Group GmbH

Anja Desai

The Corona lockdown caught the project CybersecurityEast in its inception phase. Related activities, started by GFA earlier this year, had to be adjusted. Two of the baseline assessments required for all six Eastern Partnership (EaP) countries as well as the project kick-off event and regional workshop planned for May have been postponed to September. Currently, GFA is developing innovative solutions to react to the situation and to support the efforts of beneficiary countries to address the pandemic.

In today's increasingly inter-connected world, cyberattacks are a common phenomenon and can threaten governments, business and citizens with wide-reaching and potentially devastating effects. Such incidents range from hacking social media accounts and the theft of social security information to attacks on financial systems and critical infrastructure.

Cyberattacks are not just increasing in number but are also becoming more and more sophisticated. Cybersecurity therefore refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

CYBERSECURITYEAST IN BRIEF

In 2013, the European Union (EU) adopted its first comprehensive strategy related to cyberspace. The EU explicitly recognized the need to foster capacity development initiatives in this field. Ever since, several cyber-related capacity development initiatives and projects have been launched.

In November 2019, GFA's Governance Department was awarded the service contract for CybersecurityEast, the first project with a focus on strengthening cyber resilience ever tendered in an open procedure. The project will run until November 2022 and aims at strengthening the EaP countries Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine in their efforts to develop their cybersecurity capacities at the national and regional level. GFA partners in this endeavor with the Estonian e-Governance Academy, Detecon International, Action Global and the German Federal Office for Information Security (BSI).

At the same time, the project intends to facilitate the legal and institutional harmonization and approximation of the Eastern Partnership countries with the European Union by focusing on the approximation to the EU's Network and Information Systems Directive (NIS). Two components include strengthening national cybersecurity governance and legal frameworks, and developing frameworks for the protection of operators of essential services (OES) and critical information infrastructure. Another component is to increase the operational capacities for cybersecurity incident management of national, respectively governmental computer emergency response teams (CERTs).

Another project component dealing with the prevention and prosecution of cybercrime is implemented in parallel by the Council of Europe (CoE). This allows GFA to seek synergies and look into the close links between cybersecurity and cybercrime. To achieve its objectives, the project addresses the specific needs of each of the EaP countries while fostering capacity development and cooperation at a regional level between the six EaP countries, and between them and EU members states and European institutions.

THE GFA APPROACH AND STRATEGY

The six EaP countries continue to make progress regarding different cybersecurity aspects highlighted, for example, in the Global Cybersecurity Index of the International Telecommunication Union for 2018/19. However, the countries show considerable differences and challenges regarding their level of cyber resilience. A project with such a wide regional scope and technical focus needs to take these differences carefully into account in order to provide meaningful and comprehensive capacity development measures. Another factor are varying levels of cooperation between individual EaP countries, and between them and the EU. For example, Georgia, Moldova and Ukraine have signed Association Agreements as well as Deep and Comprehensive Free Trade Agreements with the EU, while no such agreements are in place with Belarus, Azerbaijan and Armenia. These differences have direct implications in terms of the countries' specific needs for technical support as well as for opportunities to strengthen the approximation of their national to the EU's legal frameworks for cybersecurity and the NIS Directive. The GFA project strategy therefore focusses on differentiated and tailor-made activities based on sound and in-depth analysis of the status quo at the country and regional level.

CURRENT PROJECT ACTIVITIES

Collecting detailed baseline information for each of the six countries is a key step for the project in order to properly understand and assess their respective state-of-play with regard to cybersecurity. To this effect and in order to present the project to local cooperation partners and beneficiaries, the GFA expert team has begun to conduct missions to all EaP countries.

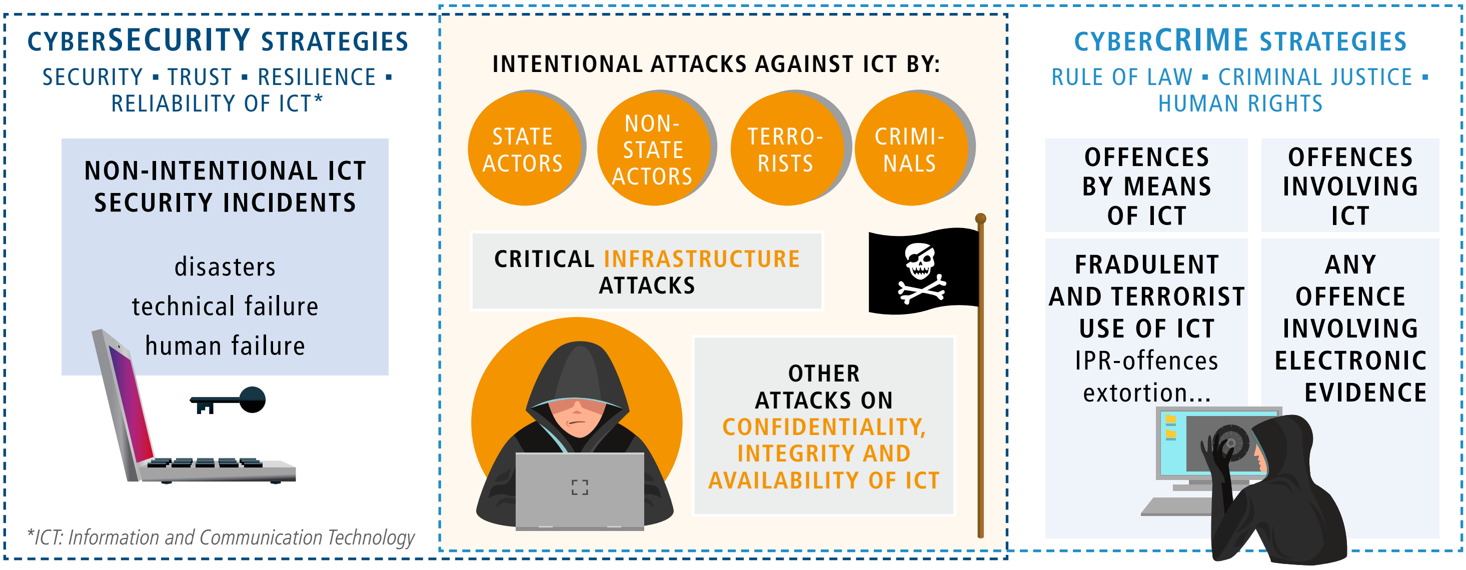
In February, the GFA team leader participated in the first steering committee meeting of the CoE-run CyberEast project in Kiev, Ukraine, which provided an opportunity to coordinate both projects' approaches, meet all relevant partner organizations, and begin with the collection of baseline data and information.

THE EUROPEAN NIS DIRECTIVE

The European Directive on Security of Network and Information Systems (NIS), adopted in 2016, is the legal centerpiece of the EU Cybersecurity Strategy and presents the first comprehensive EU-wide legislation on cybersecurity. It aims at achieving a minimum level of harmonization between member states by obliging them to adopt national NIS strategies and create single points of contact as well as CERTs. In addition, it sets out security and notification requirements for OES in critical sectors such as energy, banking, digital infrastructure, transportation, water, health, etc., and enables cross-border collaboration through a network of CERTs and the strategic NIS Cooperation Group. The reduction of cybercrime is another key objective of the NIS Directive.

The first mission to Ukraine was followed by inception missions to Moldova, Belarus and Armenia in February and March. In Moldova, the project plans to support the further qualification and organizational strengthening of government CERTs, the review of protection frameworks for critical infrastructure protection as well as increasing the awareness of citizens on cyber hygiene. The current situation in Armenia provides opportunities for the project to facilitate national efforts to draft a national cybersecurity strategy

CYBERSECURITY AND CYBERCRIME



CYBERSECURITY STRATEGIES

SECURITY ▪ TRUST ▪ RESILIENCE ▪ RELIABILITY OF ICT*

NON-INTENTIONAL ICT SECURITY INCIDENTS

disasters
technical failure
human failure

*ICT: Information and Communication Technology

INTENTIONAL ATTACKS AGAINST ICT BY:

STATE ACTORS

NON-STATE ACTORS

TERRORISTS

CRIMINALS

CRITICAL INFRASTRUCTURE ATTACKS

OTHER ATTACKS ON CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF ICT

CYBERCRIME STRATEGIES

RULE OF LAW ▪ CRIMINAL JUSTICE ▪ HUMAN RIGHTS

OFFENCES BY MEANS OF ICT

OFFENCES INVOLVING ICT

FRADULENT AND TERRORIST USE OF ICT
IPR-offences
extortion...

ANY OFFENCE INVOLVING ELECTRONIC EVIDENCE

First CyberEast steering committee, 13-14 February 2020 in Kiev, Ukraine

and to support the set-up of a new national CERT. In Belarus, assisting the development of a national cybersecurity strategy document may not be feasible due to the relatively narrow timeframe, and because the nature of the topic is politically charged. However, together with stakeholders in Minsk and the national CERT, a number of priorities in line with project objectives has been identified. The latter comprise, for example, a cyber hygiene campaign and support to the technical capacity of existing and sectoral CERTs yet to be established.

In Georgia, the project has been able to adjust to the Corona crisis quickly and to start a collaboration with its sister project implemented by the CoE. This project supports the government's ongoing reform efforts to review and improve the legal framework for cybercrime and cybersecurity. At the same time, the baseline study of the wider national context is being prepared as desk research, which will be complemented by a first mission to the country at a later stage.

All missions conducted and stakeholders engaged as well as the information and data collected show the high interest of GFA counterparts as well as the fact that the project kicks in at the right time. Cybersecurity is a topic of high relevance for the European Commission (EC) that has launched several initiatives in this field in recent years, including the EU CyberNet. The latter was launched by the Commission's Directorate-General for International Cooperation and Development in September 2019. It aims at strengthening the global delivery, coordination and coherence of the EU's cyber capacity development projects over the next four years and at reinforcing the EU's capacity to provide technical assistance to third countries in relation with cybersecurity and cybercrime. The Cyber Capacity Building Network is implemented under the auspices of the Estonian Information System Authority in partnership with the Cybersecurity Authority of Luxembourg, the Finish Transport and Communications Agency and the German Federal Foreign Office.

Due to Corona-induced restrictions, several ongoing EU4Digital projects have launched a virtual workshop series hosted by the EC, which provides a platform for all EU4Digital team leaders to present their respective projects, exchange experiences and present solutions to tackle common challenges related to Covid-19. In addition, main intermediaries of the projects from EaP countries participated in the workshops. This has enabled the project to highlight the importance of OES as one of its central features and to discuss best practices regarding security issues, including infrastructure and services of the health sector. The attempts of criminals to promote and sell counterfeit drugs and medical equipment online further prove the need and urgency to raise citizens' awareness on cyber hygiene as another important aim of the project.

In March 2020, the EC invited GFA to participate in a two-day workshop in Brussels, present its approach and exchange with colleagues and European stakeholders on the state-of-play in capacity development approaches related to cybersecurity. This presented a welcome opportunity for the GFA team to engage in networking and learning with and from others involved in this rapidly evolving field.

Contact: Tobias Tschappe,
tobias.tschappe@gfa-group.de &
Rune Rossius, rune.rossius@gfa-group.de

A VOICE FROM THE PROJECT ON THE IMPLICATIONS OF COVID-19 BY GFA TEAM LEADER BESNIK LIMAJ

Despite the circumstances, our project is still working on delivering its inception period results. While face-to-face events and meetings currently cannot take place, online work and meetings continue. The GFA project team is working around the clock to support our partners and the EC in addressing the Corona crisis. The six partner countries face severe difficulties since cyberattacks and fraudulent activities have increased since the Corona outbreak. Therefore, we raise the awareness of our beneficiaries and partners to be extra vigilant against online scams, including phishing and malware. We have developed recommendations for the CERTs of partner countries and their constituents' employees on how to stay safe online when using digital devices and systems. This includes advice on a variety of issues: The use of Virtual Private Network (VPN), automatic log-out policies when walking away from computers, limited access to devices when using them for work only, reminders on updating software including firewalls and antivirus programs, back-up of data, enabling two- or multi-factor authentication and having strong and lengthy passwords for online access.

In addition, our recommendations pay special attention to e-mail phishing since around 90 percent of all cyberattacks start with emails. Partner country beneficiaries should therefore consider e-mail protection a first line of defense and be able to do all it takes to block malicious e-mails from reaching their devices in the first place.

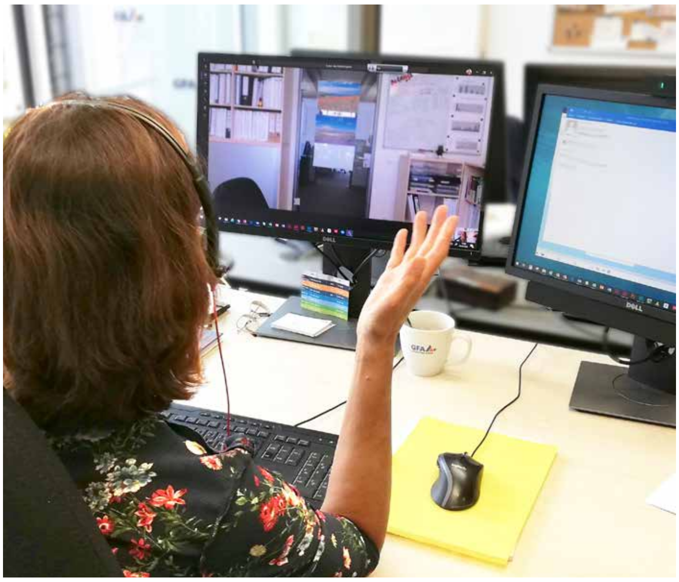
Overall, we have been able to learn from extreme events in recent weeks and we can address cybersecurity threats when criminal actors try to take advantage of the Covid-19 pandemic.

A SAMPLE OF GFA DIGITAL RESPONSES TO THE CORONA PANDEMIC

Tasked by the GIZ sector project Technical Vocational Education and Training (TVET), the Education, Skills and Employment Department of GFA is compiling a study on the application of digital learning formats within the TVET sector as a response to Covid-19. The study looks at partner countries of German development cooperation and showcases creative, digital approaches that compensate cancelled classes and it identifies the prevailing needs and gaps of digital applications. Based on these cases, GFA will develop approaches in the TVET systems of partner countries that systematically embed digital learning formats.

Due to the Corona pandemic, GFA experiences a digitalization push in its own organization. As MS Teams was piloted earlier this year, this allowed GFA to roll out the application throughout the company within a couple of days. To date, project coordinators are not only able to communicate and work together from home, but technical challenges, Corona responses and best practices are being posted, discussed and put to practice collectively across departments and job hierarchy. GFA is looking forward to exploit the possibilities for internal communication and knowledge management further during the coming months.

GFA has jump-started its onboarding procedures for new employees by going all digital. The company now conducts its first-workday Human Resources Introduction and the majority of all onboarding courses online via MS Teams. The onboarding courses are preceded by a short online training introduction to MS Teams. All new employees present themselves on GFA's internal website and are invited to relevant MS Teams channels.



Beyond that GFA has recently started a webinar series "GFA Learns Digital" for project coordinators and staff worldwide. More than 60 participants followed a short and intense one-hour input on when and how to use online tools for live voting and presentations. Further webinars and the production of quick guides for remote work have followed in accordance with the needs of 164 ongoing GFA projects gathered by means of a survey. In addition, individual support for project teams has been initiated as well as peer group assistance for quick knowledge transfer among projects.

GFA in cooperation with the European Digital SME Alliance recently offered a webinar Digital Solutions in Times of Covid-19 in the context of the project EU and Gulf Cooperation Council (GCC) Dialogue on Economic Diversification financed by the European Foreign Policy Instrument. The webinar was free of charge and introduced project stakeholders to Europe's first and largest SME association specializing in ICT and the support it offers to SMEs and startups. For example, the association has launched a campaign to share digital solutions offered by SMEs and startups with public and private clients in need of new tools and services to mitigate the effects of the Covid-19 crisis. The EU-GCC dialogue project in general contributes to stronger EU-GCC relations by supporting the GCC countries' ongoing process of economic diversification away from hydrocarbon-dependent sectors. In recent weeks, the project has become more relevant than ever because economic diversification models in the GCC are based on client-facing services such as tourism, transport, property development and financial services that are highly affected by the crisis. More information about the project as well as recent developments in the EU and GCC can be found at:
www.linkedin.com/company/eu-gcc-dialogue-on-economic-diversification
www.digitalsme.eu/solutions

Contact: Anja Desai, anja.desai@gfa-group.de

IMPRINT
GFA newsletter produced by GFA Consulting Group GmbH, Eulenkrugstraße 82, 22359 Hamburg, Germany, phone: +49 (0) 40 603 06-100,
fax: +49 (0) 40 603 06-199, e-mail: newsletter@gfa-group.de, www.gfa-group.de, all rights reserved © 2020, responsible for content: Anja Desai,
edited by Manfred Oepen, ACT Assist GmbH, layout: Natascha Pleß, printed by Zertani, photos: GFA, istockphoto

gfagroup GFA_CG in gfa-consulting-group-gmbh gfaconsultinggroup

GFA Consulting Group is a growing consulting organization active in international economic development. The main sectors of the company comprise agriculture & rural development, natural resources management & environment, climate change, energy, governance, public finance management, private sector development, education, skills & employment, financial systems development, health, monitoring & evaluation, water, sanitation & waste management, digital innovation and framework contracts. Every year, GFA carries out around 300 projects and studies around the world.

GFA vision – to be the partner of choice for clients in our core service areas.

GFA mission – to improve the livelihood of beneficiaries through our professional services.

GFA core values – to offer high performance in service delivery, technical excellence in our main sectors, innovative approaches and products, and credibility with our clients when putting projects into practice.