Cyber Capacity Building Measures trough Cyber Education, Training, Exercise and Evaluation (ETEE) Platform under the ESDC Raised Awareness of the EU's Contribution to Global Cyber Stability

Dirk DUBOIS, Horațius-Nicolae GÂRBAN, Marios THOMA
Security and Defence College, European External Action Service
dirk.dubois@eeas.europa.eu; horatius.garban@eeas.europa.eu; marios.thoma@eeas.europa.eu

Abstract: This article deal with the EU Cyber Ecosystem as it related to the external dimensions, in particular cybersecurity capacity-building efforts in the EU's neighbourhood and confidence building measures. It presents key EU cyber diplomacy activities and pays particular attention to a valuable instrument in the EU's toolbox, which is the Cyber Education, Training, Exercise and Evaluation (ETEE) Platform of the European Security and Defence College. This initiative continuously identifies training gaps, and develops activities to address them, together with its network partners and main EU actors, contributing mainly to the cybersecurity education, professional training and expertise development pillar of the EU external cyber capacity building initiatives. It also contributes to cyber hygiene and awareness as well as a culture of cyber security. The article places the activities of this platform in the wider context of EU and global efforts at ensuring cyber governance in an increasingly threatening security environment.

Keywords: Cybersecurity, Global governance, Neighbourhood policy, Confidence building measures, Education and training, Cyber Education, Training, Exercise and Evaluation (ETEE) Platform, Capacity Building, Foreign policy, Cyberdiplomacy

INTRODUCTION

THE CYBER EDUCATION, TRAINING, EXERCISE AND EVALUATION (ETEE) PLATFORM AT A GLANCE

On 13 November 2017, the EDA Steering Board, bringing together the 27 participating Ministers of Defence, agreed with this collegiate view and decided to request the ESDC to establish such a Centre (hereinafter the 'Platform').

On 6 February 2018, the EU Member States, represented in the ESDC's Steering Committee, decided that a **Cyber Education, Training, Exercise and Evaluation (ETEE) Platform** should be created within the ESDC, following an updated study undertaken by RAND Europe.

As it was set out, the main aim of the Cyber ETEE Platform would be to educate and train together civilian and military personnel of the Member States and EU institutions. The main target audience of the ESDC's dedicated Cyber Courses would be mid-ranking to senior officials, dealing with technical, operational to strategic aspects in the field of cybersecurity and cyber defence, and for decision-makers, the activities should be from awareness to strategic level.

On 14 May 2018, the Council adopted Decision (CFSP) 2018/712 amending Decision (CFSP) 2016/2382 establishing a European Security and Defence College, and broadening its activities in the cyber domain. On 29 June 2018, the ESDC Steering Committee followed the advice of the Executive Academic Board to refocus the mission of the eLCIP EAB configuration and to rename the configuration into EAB.Cyber.

EAB.Cyber meets regularly every three months during each academic year of the ESDC. Its discussion items comprise activities under the Cyber ETEE Platform (including curriculum development and activity evaluations), as well as developments in the overall cyber context. It is also the focal point to foster collaboration and to establish synergies between its network members in the academic and operational domains.

The main mission of the Cyber ETEE Platform is to address cybersecurity and defence training among the civilian and military personnel, including for the CSDP requirements for all CSDP training levels as identified by the EU Military and Civilian Training Groups (EUMTG and EUCTG), and to upscale the training opportunities for the Member States.

At a later stage, and depending on the further development of such a concept, the Cyber ETEE Platform could advance ETEE opportunities for a wider cyber defence workforce (the so-called Cyber Reserve) (Dubois et al, 2020).

THE KEY CONCEPTS AS DEPICTED IN THE EU CYBER SECURITY STRATEGY

- **Capacity building in the EU cyber domain**

In broad terms, **capacity building in the cyber domain** is aimed at responding effectively to cybercrime and enhancing the countries' cyber resilience. By fostering a common view and purpose, securing a free, open, interoperable cyberspace for everyone and ensuring compliance with human rights and the rules of law, this concept can foster international stability and solidarity.

The EU has been leading international cybersecurity capacity building since the adoption of the Cybersecurity Strategy in 2013, systematically linking efforts with development cooperation funds. Such actions are based on promoting a rights-based and whole-of-government approach that integrates lessons learned from the EU's internal experience. Moreover, in 2018, the Council drew the conclusions on the EU External Cyber Capacity Building Guidelines (10496/2018), clearly stating, at EU level, that lessons from development cooperation should be taken into account in external cyber capacity building efforts, enhancing effectiveness and sustainability. These conclusions stress the need for promoting partnerships and the participation of all stakeholders, focusing on sustainable results and solutions, promoting a broader policy, reforming and updating legal and technical processes, ensuring that trust, transparency, accountability and shared responsibility are the driving forces behind any assistance (Council Secretariat, 2018c).

In light of this, a concerted effort is necessary, consolidating the lessons learned from the EU's experience to date - particularly in bridging the development and technical communities, as well as to translate the several dimensions of cyber policy into a systematic methodology that will serve as operational guidance when designing and implementing the EU's external cybersecurity capacity-building efforts in the neighbourhood.

In this regard, the Cyber ETEE platform, as an active part of the EU Cyber Ecosystem, continuously identifies training gaps, and develops activities to address them, together with its network partners and main EU actors (Dubois et al, 2020).

The external cyber capacity building initiatives of the EU and its Member States are focused on reforms across the main pillars of cyber resilience, increasing incident management capabilities, and **developing education, professional training and expertise** in cyber domains. Promoting cyber hygiene and awareness as well as a culture of cyber security, assessment of digital products, processes and services in compliance with European and international standards and best practices should be the compass of the next activities (Council Secretariat, 2018c, Council Secretariat, 2018d).

Another aspect is the holistic and consistent rights-based approach on relevant external capacity building activities, due to the crosscutting aspects of electronic evidence and cyber-enabled systems, infrastructure and services, especially on justice and security, in particular in programmes dedicated to counter-terrorism and countering organised crime.

The same guidelines call on the EU and its Member States to adapt their capacity building actions in partner countries and regions, according to local specificities.

This approach should encourage inter-regional cooperation according to the cyber maturity of individual countries, engaging key international and regional partners, organisations and stakeholders, civil society, academia and research, as well as private sector. Taking into consideration the highly sensitive aspects of cybersecurity and potential risks running contrary to key EU values and policies, great vigilance is necessary to ensure coherence between EU policy and programmes (Ziolkowski, 2013).

- **Confidence-building measures**

The continuously growing importance of internet-enabled platforms delivering e-government, e-democracy, financial, private and public services makes them one of the key priorities for national and regional security. State, state-sponsored or non-state actors have developed highly sophisticated intrusive techniques at the same pace to gain the economic, political, security or information advantage over the EU or Member States who are adversaries. The widening and evolution of that landscape of threats, challenges, slow reaction and lack of diplomatic consensus linked to attribution of cyber-attacks have further increased the risks of misunderstandings and the misperception of operations in cyberspace (or cyber-ops) against EU and its Member States (Fontelles, 2021, Healey et al, 2014).

In the course of the effort of countering these malicious activities, and with the lack of engagement of affected states, an important number of international and regional organisations across the world have started the process of developing confidence-building measures in cyberspace (European Commission, 2017, ECDP 2019a), with a focus on:

- improving and securing communication and information exchange/ sharing,
- increasing transparency and verification,

- increasing cooperation and implementing better restraint measures against potential adversaries, to deter aggressive action.

While these initiatives are welcome, there is always a side effect, in growing concerns that the global 'cyber stability regime' may be undermined by diverging concepts, methods and measures elaborated within different national frameworks and within the view and specific strategy of each Member State.

The European Union is considering the development of cyberspace as one of its key priorities. In this regard, the EU Cybersecurity Strategy contributes actively to the ongoing debates about norms, provides support to regional confidence-building processes, and pursues the objective of a stable, safe and secure cyberspace by providing funding for capacity building in partner countries (European Commission, 2020).

What are confidence-building measures (CBMs) in fact?

As primarily stated in the 1975 Helsinki Final Act, the 1986 Stockholm Document on Confidence and Security Building Measures and Disarmament in Europe, and in the 1990 Vienna Document, the aim of CBMs is to reduce and / or prevent the risk of conflict by reducing or eliminating causes of mistrust, misunderstanding and miscalculation between states. However, the primary focus was on the military field, with the aim of increasing transparency, improving information exchange and restraining the use of violence by armed forces. The main assumption is that information exchange about military doctrines and capabilities contributes to regional and global stability by enhancing situational awareness and building common understanding between partners and neighbours (Pawlak, 2015).

In cyberspace, CBMs are the key mechanisms in the international community, aimed at preventing or reducing the risk of a conflict (any type) by eliminating the causes of mistrust and miscalculation between states, organisations and partners. These CBMs are in fact cooperation tools for ensuring the same understanding of the norms and commitments. Consequently, in cyberspace, implementing effective CBMs is the main goal in the debates at the global and regional levels (GFCE, 2020, Pawlak, 2015).

In this respect, the main international organisations, such as the UN, OSCE, OAS and ASEAN, established, since the early 1990s, different sets of CBMs, with a focus on the regional level, but tackling the same aspects in different views. In those years, the first Cyber-Security Strategies were established, according to the understandings and the development level of partners in each organisation, and the need of a common understanding raised in all these forums.

In the effort to create a common understanding a use of efforts, the UN GGE was established in 2005 – United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – which became the main channel for the discussion about cyber norms and confidence-building measures. The UN GGE group stressed that “international law (UN Charter in particular), is applicable, and is essential to maintaining peace and stability, promoting an open, secure, peaceful and accessible ICT environment”, recognising the importance of confidence-building measures as means to “strengthening international peace and security” and “increasing cooperation, transparency, predictability and stability” (GFCE, 2020).

The European Union’s approach to confidence-building measures is highlighted in some important documents such as the EU Cybersecurity Strategy adopted in 2020, or the Council Conclusions on Cyber Diplomacy adopted on 10 February 2015.

Furthermore, the EU is pursuing the objective of strengthening confidence-building processes through:

- support for the initiatives focused on confidence-building measures launched by other regional organisations,
- the development of structured and overarching EU strategic cyber consultations, sectoral dialogues, and operational cooperation with the US, China, Japan, India, South Korea and Brazil;
- active participation in global and regional debates on cyber norms;
- capacity-building initiatives implemented by the European Commission alone or in cooperation with other regional or international organisations (Council of Europe, OAS, NATO). The focus of these projects is primarily on developing legal and technological capabilities (Pawlak, 2015, OAS, 2009, Pupillo et al, 2018, Ziolkowski, 2013).

EUROPEAN UNION’S CYBER DIPLOMACY INITIATIVES

In 2018, regionally, Europe fares best in terms of cyber public awareness campaigns, research and development, educational programmes, as well as cyber industry and capacity building. Europe recorded more bilateral, multilateral and international agreements than any other region in the world, while also enjoying the highest score for participation in international forums, according to the Global Cybersecurity Index (2018) (GCSI, 2018).

Although the EU's cybersecurity strategy dates back to 2013, revised in 2017 and 2020, the EU Global Strategy in 2016 and the Cyber Defence Policy Framework in 2018 have also been issued. These strategic documents address several key points and create an overarching framework:

- pledging EU support for critical infrastructure protection and cyber crisis management;
- stimulating cooperation between Member States on political, operational and technical cyber issues;
- calling for technological capabilities for cyber resilience to be bolstered across the spectrum;
- proposing the mainstreaming of cyber issues across all EU policy areas;
- enhancing cyber cooperation with core partners, international organisations and through public-private partnerships (Council Secretariat, 2018e, Council Secretariat, 2014, Council Secretariat, 2016, Council Secretariat, 2018b, Council Secretariat, 2021).

In October 2017, EU Member States adopted the **cyber diplomacy toolbox**, addressing the joint EU diplomatic response to malicious cyber behaviour, highlighting the deterrent effect upon potential aggressors, and conditioning the effectiveness upon a "shared situational awareness agreed among Member States" and proportionality of response (Council Secretariat, 2017). This document sets the guidelines for malicious cyber activities at all levels of the conflict spectrum:

- preventive measures – cyber confidence and capacity building abroad, awareness raising activities of EU cyber policies;
- cooperative measures – political and thematic dialogues or EU diplomatic démarches;
- stability measures – official statements by EU leadership, Council conclusions, diplomatic engagements in international forums;
- restrictive measures (sanctions) – travel bans, arms embargos, freezing of assets; EU support for Member States' lawful responses should they fall victim to a cyber act: including in the case of invoking the EU's mutual assistance clause, Article 42 (7) TEU and the solidarity clause, Article 222 TFEU. NATO Allies can also invoke Article 5.

Directly contributing to the EU's cyber diplomacy goals is the EU Cyber Direct project, financed through the EU's Partnership Instrument, which aims to develop dialogues with the EU's strategic partners and to become a platform where governmental and non-governmental actors discuss cyber norms, responsible cyber behaviours and confidence-building measures (ECDP 2019a, ECDP, 2019b).

The European Parliament has consistently advocated robust EU-level cyber measures. An important set of actions and regulations were adopted strengthening the cooperation and forcing EU Member states to implement common specific measures and increase cooperation and information sharing. In June 2018, with a resolution focused on cyber defence, Parliament confirmed its commitment to an open, free and secure cyberspace, upholding EU values, while calling upon EU Member States to implement the EU's approach to cyber diplomacy and cooperate with NATO in formulating criteria and definitions for cyber operations. It consequently welcomed the EU's cyber diplomacy toolbox and called for a proactive, cross-sectional foreign policy approach to strengthen it (Pawlak, 2015, Latici, 2020, Council Secretariat, 2019).

BURNING ISSUES IN THE CONTEXT OF THE GLOBAL CYBER ECOSYSTEM

Recent analyses brim with talk of a new digital/cyber/technological arms race. Another relevant aspect is that many countries see cyberspace as 'an extension of the military domain', or 'a new battle-space', triggering this race. In the effort to stop this new race, the United Nations (UN) and the OSCE elaborated new recommendations, which should include the development of an internationally-agreed prohibition on attacking certain targets (e.g. civilian facilities), cyber-arms control security-building measures, and collaborative approaches to fill the cyber regulatory governance gaps.

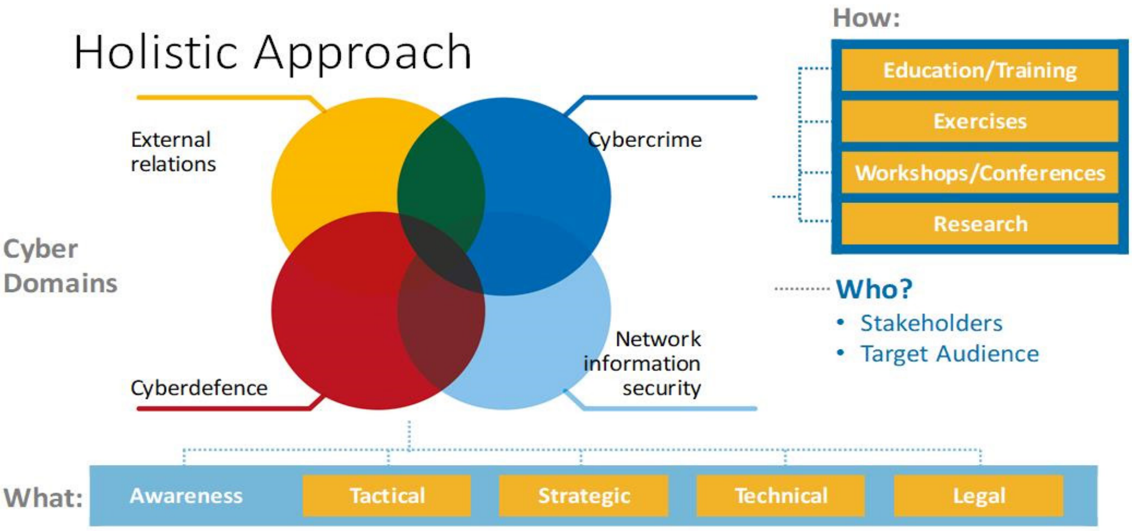
Although UN initiatives such as the Group of Governmental Experts and the Open-Ended Working Group are essential for 'advancing responsible state behaviour in cyberspace', for now, there are no globally agreed international treaties or binding guidelines on rules of engagement in a cyber-war (GFCE, 2020).

The 'grey zone' of a cyber war also results from the fact that cyber tools can be used for both civilian and military purposes – they are dual-use devices. Just a line of code could make the difference between a weaponised cyber-tool and one that is not. Equally, most of the commercially available cyber-tools can be used for both legitimate goals or as intrusion weapons, depending on the user's intention. This dual-use makes the export of cyber tools particularly difficult to regulate. In the effort to tackle this aspect, the EU is considering to include cyber-surveillance technologies in the dual-use export control regime (Healey et al, 2014, Council Secretariat, 2016, Council Secretariat, 2018a, Council Secretariat, 2018b).

THE CYBER ETEE IN THE CONTEXT OF THE EU CYBER ECOSYSTEM

ANALYSIS

Based on the state of play regarding cyber within the EU and the decisions in place, in 2018, the ESDC secretariat analysed the EU cyber ecosystem, Member States' training requirements and actual offers in the cyber field. As a result, in the first EAB.Cyber meeting on 27th of September 2018, a new holistic approach was proposed and adopted as the strategic compass regarding the development of the Cyber ETEE Platform:



Source: ESDC internal documents

Furthermore, a concrete plan for the way ahead was proposed and adopted, specific topics and fields of expertise (such as the 'tactical', 'strategic', 'technical' and 'legal' fields) are targeted, starting with awareness courses as the basis for organising in-depth activities (Dubois et al, 2020).

In the same forum, it was decided that the ESDC's Cyber ETEE Platform should achieve its main goals through:

- Education/training - curricula development for the different training activities;
- Exercises - support for scenario development (covering the functional and operational level);
- Workshops/conferences - identification of topics, lecturers and institutions to be involved;
- Research - identification of relevant actors, best practices and new approaches.

The Cyber ETEE platform attributed great importance to collaboration with all cyber related EU agencies, and created, contributed or hosted several specific projects in cooperation with ENISA, EDA, but also extending this cooperation with other EU operational agencies and entities: eu-LISA, EUROPOL, CEPOL, CERT-EU, etc.

While the Platform is still in its early stages, it is already becoming an active, visible and successful actor in the EU cyber ecosystem. Several successful pilot activities organised in 2019 and 2020, targeting different levels and cyber-domains, were approved by all 27 Member States, in the ESDC Steering Committee, to become regular training activities, which are to be organised every year:

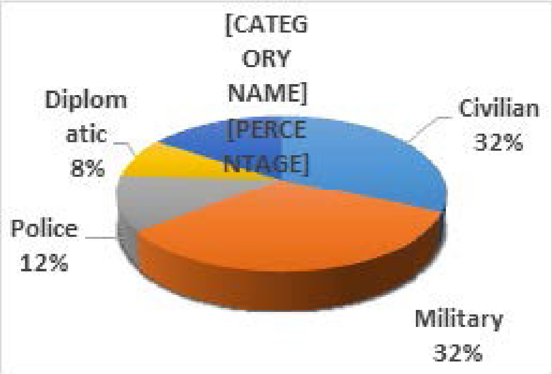
- External Relations: The role of the EU Cyber Ecosystem in the Global Cyber Security Stability, which will be organised in 2021 in 3 iterations with a focus on different regions – MENA Countries, Western Balkans and Eastern Partnership,
- NIS: Critical Infrastructures in the Context of Digitization, Information Security Management and ICT Security (2 iterations in 2020 and 3 iterations in 2021)
- CyberDefence: Cybersecurity Organisational Defensive Capabilities, Cyber Security Basics for Non-Technical Experts
- Other cyber activities have been planned and are on-going, in all cyber domains and at all levels, during the academic year 2020 – 2021, including tactical/technical activities requiring a high level of expertise:
- Critical Infrastructures Modular Course (2 modules, awareness and strategic / policy level, including 2 table top exercises),
- Cyber Diplomacy Modular Course (2 modules, awareness and strategic/ policy level, including 2 table-top exercises),
- Cyber Defence Policy on National and International Level,
- Practical Cyber Threat Intelligence and Information Sharing using MISP CTI,

More and updated information, regarding Cyber ETEE activities, is available on the ESDC's website or through the Goalkeeper application.

Regarding the main aim of the Cyber ETEE Platform, the following objective was achieved: educating and training together civilian and military personnel of the Member States, EU Institutions and Third States in different fields of cyber. By now, the statistics, which cover finalized activities, show that we addressed the trainings to all categories of personnel, from all working domains and covering all working fields:

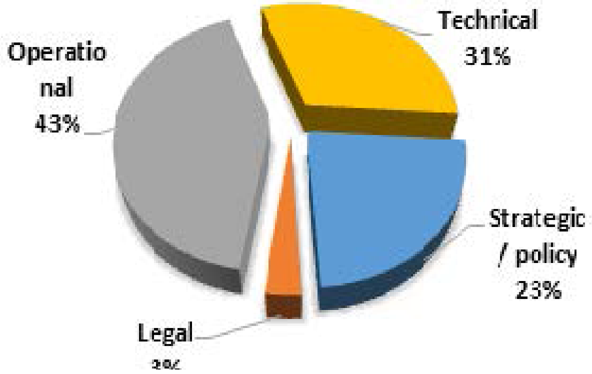
1. https://esdc.europa.eu

2. https://goalkeeper.eeas.europa.eu/



Source: ESDC internal documents

Working Domain



Working level/field

As regards exercises, the Cyber ETEE Platform was involved in supporting both the European External Action Service during the Cyber DIPLO 2019 exercise and the European Military Staff during the MILEX 2019 exercise, and this support will continue in the following years. A new opportunity is Cyber ETEE's participation, as observer, in the Cyber Phalanx 2021 Exercise organised by European Defence Agency.

This involvement in supporting Cyber Exercises at EU strategic level aims to identify the gaps in the level of knowledge, create lessons learned, develop new activities and, together with the network partners, address and fill these gaps.

CURRENT DEVELOPMENTS

Moreover, following the EU Cyber Strategy lines, the ESDC continues its engagement in the EU-NATO collaboration process by establishing working relations with the NATO Maritime Interdiction Operational Training Center, welcoming it among its Associated Network Partners, and by participating as keynote speaker and moderator in NATO Cyber conferences.

In an effort to increase cohesion within the cyber domain and to improve the exchange between academic research and the operational world, the ESDC is currently exploring the establishment of a research cooperation program under the Cyber ETEE Platform. The idea is to leverage the knowledge and innovative power of academia for the problems existing in the operational field.

VISION – WAY FORWARD

Given that the ESDC is a network college (capabilities and resources are within the network of the College), its Cyber ETEE Platform aims to facilitate training coordination within the EU cyber ecosystem in order to:

- transfer cyber knowledge between domains;
- focus, deepen and strengthen cyber expertise;
- thereby improve the quality of education/training/exercises;
- develop cooperation and synergies (saving resources and time), and
- reduce overlaps and achieve the necessary complementarity between actors.

The goal is to deliver directed, sophisticated, and target-oriented activities by harmonising and standardising Cyber ETEE activities, thereby establishing a common European cybersecurity culture at EU level and at the same time contributing to global cyber stability.

Most important is that Cyber ETEE platform's way forward and activities organised are in line with the recommendations of EU Parliament, Commission, Council, closing the gaps in all cyber domains, especially in Cyber Diplomacy, highlighting and promoting the EU values and approaches in cyber, acting as a capacity building and confidence-building tool for the EU values.

https://esdc.europa.eu

Email: ESDC-CYBER-ETEE@eeas.europa.eu

REFERENCE LIST

Dirk DUBOIS, Dr. Marios THOMA, Dr. Gregor SCHAFFRATH - CSDP Cyber Education, Training, Exercise and Evaluation (ETEE) Platform under the ESDC - European Security & Defence College, SECURITATEA CIBERNETICĂ - PROVOCĂRI ȘI PERSPECTIVE ÎN EDUCAȚIE, Craiova, Romania, 2020, https://www.arasec.ro/documente/CybersecurityEDU2020-RO.pdf

EU Cyber Direct Project, EU Cyber Diplomacy in Action – Factsheet, sept 2019, as ECDP (2019a), https://eucyberdirect.eu/content_knowledge_hu/eu-cyber-diplomacy-in-action-factcheet/

EU Cyber Direct Project, Peace and Stability in Cyberspace – Factsheet, sept 2019, as ECDP (2019b) https://eucyberdirect.eu/content_knowledge_hu/peace-and-stability-in-cyberspace-factsheet/

European Commission, European External Action Service, Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13/09/2017, Doc: Join 450/2017, Belgium, Brussels, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

European Commission, Service for Foreign Policy Instruments (FPI), Partnership Instrument Annual Action Programme 2020, COMMISSION IMPLEMENTING DECISION of 5.5.2020 on the financing of the 2020 Partnership Instrument Annual Action Programme for cooperation with third countries to be financed from the general budget of the European Union, Brussels, 5.5.2020, C(2020) 2779 final, https://ec.europa.eu/fpi/content/partnership-instrument-annual-action-programme-2020_en

General Secretariat of the Council, 07/06/2017, Council Conclusions on a Framework for a Joint EU Diplomatic

Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")-Adoption, Doc: 9916/17, Belgium, Brussels, https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

General Secretariat of the Council, 09/03/2021, Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade, Doc: 6722/21, Belgium, Brussels, https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf

General Secretariat of the Council, 14/05/2019, Council Decision Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its MemberStates, Doc: 7299/19, Belgium, Brussels, https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf

General Secretariat of the Council, 16/04/2018, Council conclusions on malicious cyber activities (approval), Doc: 7925/18, Belgium, Brussels, as Council Secretariat (2018a), https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf

General Secretariat of the Council, 17–18/11/2014, EU Cyber Defence Policy Framework, Doc: 15585/14, Belgium, Brussels, https://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/en/pdf

General Secretariat of the Council, 18/10/2018, Council Conclusions on Measures to build strong cybersecurity in the EU, Doc: EUCO 13/18, Belgium, Brussels, as Council Secretariat (2018d), https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/

General Secretariat of the Council, 26/06/2018, EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises - Council conclusions, Doc. 10086/18, Belgium, Brussels, as Council Secretariat (2018b), https://data.consilium.europa.eu/doc/document/ST-10086-2018-INIT/en/pdf

General Secretariat of the Council, 26/06/2018, EU External Cyber Capacity Building Guidelines-Council conclusions, Doc. 10496/18, Belgium, Brussels, as Council Secretariat (2018c), https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

General Secretariat of the Council, 28/11/2016, Council Conclusions on the Mainstreaming digital solutions and technologies in EU development policy, Doc: 14682/16, Belgium, Brussels, https://www.consilium.europa.eu/media/24221/st14682en16-dsat.pdf

General Secretariat, of the Council, 19/11/2018, EU Cyber Defence Policy Framework (2018 update), Doc: 14413/18, Belgium, Brussels, as Council Secretariat (2018e), https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

Global Cyber Security Index (2018), accessible at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Global Forum for Cyber Expertise's (GFCE) Task Force on CBM, Overview Of Existing Confidence Building Measures As Applied To Cyberspace, 03/06/2020, https://cybilportal.org/wp-content/uploads/2020/05/GFCE-CBMs-final.pdf

Jason HEALEY, John C. MALLERY, Klara TOTHOVA JORDAN, and Nathaniel V. YOUD (2014), Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security, Brent Scowcroft Center on International Security, Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/report/confidence-building-measures-in-cyberspace-a-multistakeholder-approach-for-stability-and-security/

Josep Borrell FONTELLES, European Foreign Policy in Times Of COVID-19, Publications Office of the European Union, Luxembourg, 2021

Katharina ZIOLKOWSKI, Confidence Building Measures for Cyberspace – Legal Implications, NATO Cooperative Cyber Defence Centre of Excellence – CCD CoE Estonia, Tallin, 2013, https://www.ccdcoe.org/uploads/2018/10/CBMs.pdf

Lorenzo PUPILLO / Melissa K. GRIFFITH / Steven BLOCKMANS / Andrea RENDA, Strengthening the EU's Cyber Defence Capabilities, Centre for European Policy Studies, Belgium, Brussels, 2018, https://www.ceps.eu/ceps-publications/strengthening-eus-cyber-defence-capabilities/

Patryk PAWLAK, Cyber diplomacy - Confidence-building measures, European Parliamentary Research Service, Oct 2015, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)571302

Permanent Council of the Organization of American States, Consolidated List of Confidence and Security Building Measures for Reporting According to OAS Resolutions (Approved at the meeting of January 15, 2009, and amended at the meeting of March 3, 2016), as OAS (2009), https://www.oas.org/csh/english/csbmlist.asp

Tania LAȚICI, Understanding the EU's approach to cyber diplomacy and cyber defence, European Parliamentary Research Service, 2020, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651937

Dirk DUBOIS

He graduated the Belgian Military Academy with a master degree in social and military science. In the first part of his career, he occupies several operational posts and positions as a staff officer. From 2007 to 2012, he was a training manager at the European Security and Defence College, before joining the Directorate-general for education of the Belgian MoD. Since 2015, he has been appointed as Head of European Security & Defence College (ESDC).

Horațius-Nicolae GÂRBAN

He is a military engineer with both Mechanical and ICT degrees, and an MSc in Cyber Security and ICT. He was seconded in 2019 as Cyber Defence Training Manager in European Security and Defence College. With more than 20 years in the cyber domain, he has the role of growing the Cyber Education, Training Exercise and Evaluation Platform and utilize its expertise in Cyber Defence and Cyber Diplomacy / External Relations in Cyber.

Marios THOMA

He holds a PhD degree in Cyberspace Defense and specifically in the modelling and early detection of cyber-attacks. He is a military officer currently seconded as training manager in the European Security and Defence College (ESDC) leading since 2018 the Cyber Team of the College. Previously he served in the military of Cyprus at various posts in the domain of communications, security and cyber.