

RESEARCH PAPER

RP Nr. 2 | February 2024



**European
Repository of
Cyber Incidents**

RIGHT THOUGHTS, RIGHT WORDS, RIGHT ACTIONS?

The EU's application of the Cyber Diplomacy Toolbox

Annika Sachs

Imke Schmalfeldt

Kerstin Zettl-Schabath

contact@eurepoc.eu

www.eurepoc.eu

[@EuRepoC](https://twitter.com/EuRepoC)

The **European Repository of Cyber Incidents** is an independent research consortium dedicated to better understanding the cyber threat environment in the EU and beyond. It is led by the University of Heidelberg, in cooperation with the University of Innsbruck, the Stiftung Wissenschaft und Politik and the Cyber Policy Institute (Estonia), with funding from the German and Danish Foreign Ministries.

Table of Contents

1. EU cyber diplomacy in times of geopolitical turmoil – the story thus far	2
2, The Framework of the Cyber Diplomacy Toolbox (CDT)	4
3. Methodology	6
3.1. Data	6
3.2. Operationalisation	7
3.2.1. Preventive Measures	7
3.2.2. Cooperative Measures	8
3.2.3. Stabilising Measures	8
3.2.4. Restrictive Measures	8
4. Analysis	8
4.1. The CDT from 2017 to May 2023: patterns, trends, and anomalies	8
4.2. Spotlight Analysis	14
4.2.1. Helping states to become cooperation partners: preventative and cooperative measures	15
4.2.2. Sanctioning out of the comfort zone: stabilising and restrictive measures	17
5. Conclusion	21
6. References	23
7. Appendix	27

1. EU cyber diplomacy in times of geopolitical turmoil – the story thus far

On June 8 of this year, the Council of the European Union published the “Revised Implementing Guidelines of the Cyber Diplomacy Toolbox” (Cyber Diplomacy Toolbox = CDT). Despite six years passing since the adoption of the original CDT, the EU and its member states face a more diverse cyber-threat landscape than ever before. Thus, while acknowledging the changed geopolitical environment since Russia’s war against Ukraine in February 2022, as well as concurrent ransomware and wiper operations against critical infrastructure targets, the Council still aims for a strong(er) unified approach in the revised guidelines. In doing so, the revised guidelines closely align with the Strategic Compass (2022). In particular, the guidelines stress “guidance for the attribution of malicious cyber activities, strategic communications, as well as linkages to other EU toolboxes and crisis management mechanisms and activities, while preserving Member States competences on the matter” (EU Council 2023; 4).

The revised guidelines, as well as the CDT, reflect the inherent tension in most, if not all, Common Foreign and Security Policy (CFSP) activities: how can joint capacities and crisis mechanisms be strengthened while leaving Member States’ national security prerogatives untouched? In this context, this study seeks to empirically analyse the past application of the CDT (2017-2023) to evaluate the effectiveness of the original guidelines and present an evidence-based assessment of the prospects for the revised guidelines.

Setting the stage for the analysis of EU CDT activities, cyber conflict activities displayed both major continuities and changes. Whereas the most prominent cyberattacks originated in Russia, China, Iran and North Korea, operational patterns discernibly changed over the years, with a higher number of ransomware operations and disruptive wiper attacks (included in “disruption”; see Figure 1). However, especially when compared to recent kinetic warfare, most cyber operations still serve political purposes in order to manage escalation threats below a critical threshold by exploiting the advantages of this “grey zone” conflict behaviour.

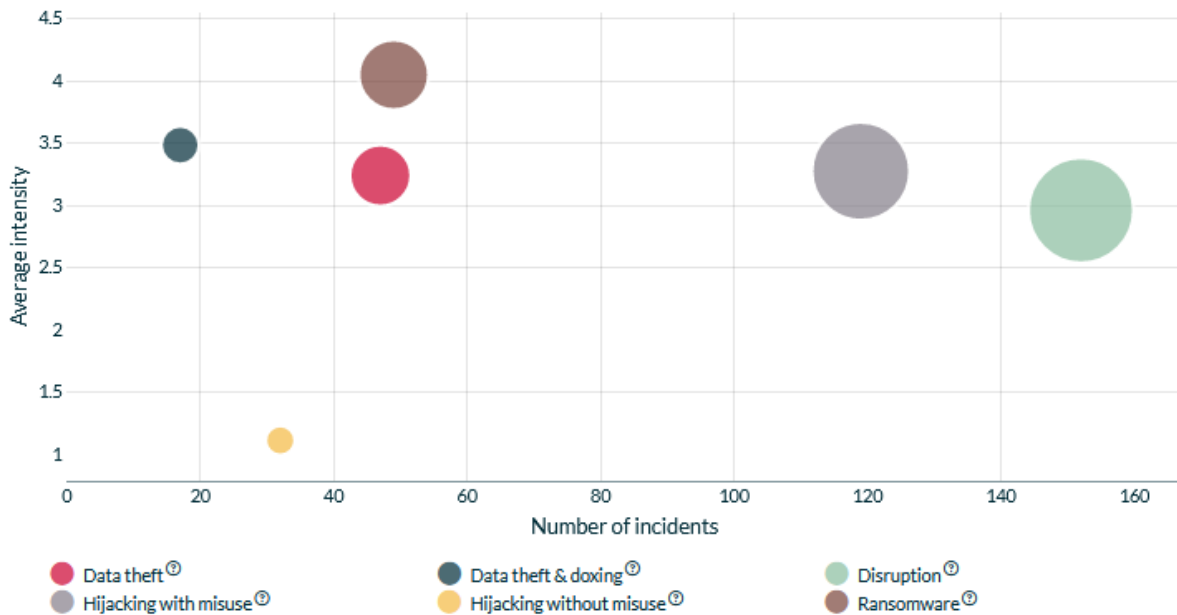


Figure 1. Incident types of cyber incidents affecting at least one EU Member State (1 January 2020 – 15 January 2024; EuRepoC dashboard).

Even though an overall pattern of state restraint regarding physically devastating cyberattacks exists, the observed attacks have brought significant financial, economic, reputational, and sometimes physical damage to companies and public infrastructure. The [WannaCry attack](#) in 2017 affected 150,000 computers worldwide, as well as companies and institutions such as Renault in France and the National Health Service in Great Britain (BBC 2017). In the same year, the wiper NotPetya caused massive business outages, with over \$10 billion USD in financial damages worldwide (Wolff 2021). Nevertheless, and in accordance with the early years of cyber conflict, political institutions were in the crosshairs of cyber attackers more than ever, not least since Russia’s war against Ukraine. At the same time, the invasion stimulated a “renaissance” of non-state, politically motivated hacking activities, further complicating the threat landscape and its political and legal regulation (Zettl-Schabath/Harnisch 2022). This is also reflected by recently published recommendations from the International Committee of the Red Cross, addressing states, belligerents, tech companies, and humanitarian organisations and how they can protect civilians against digital threats in armed conflicts (ICRC 2023).

Against this background, the EU implemented the CDT in 2017 in order to respond more coherently and systematically to this growing number and diversifying spectrum of malicious cyber activities. What stands out in the originally drafted implementing guidelines (Council of the European Union 2017b) is the frequent and strong emphasis on a “shared situational awareness of malicious cyber activities” (Council of the European Union 2017b; 10). This focus on an increasingly common perception stands in stark contrast to the existing state prerogatives for the attribution of cyber incidents, the planning and conduct of defensive and offensive cyber operations.

A closer look at the original CDT measures shows a focus on stabilising and cooperative actions, to supplement, not replace, existing EU initiatives in the field of cybersecurity. When establishing a joint mechanism for common EU sanctions in the

wake of malicious cyber activities, the original guidelines also go beyond proactive confidence-building measures (CBMs) and stress the need for restrictive deterrence measures.

This paper does not intend to assess the general effectiveness of such “cyber sanctions;” rather, it is the first to closely examine the actual application of the CDT’s measures by EU institutions/actors over the last six years, which culminated in the revised version of its implementing guidelines in June 2023. In doing so, we shed light on the question as to how far the EU has used the CDT as a vehicle to push for a strengthened Europeanisation of cybersecurity policies, or rather, if it presents a pragmatic approach to reach a stronger balance between internal and external coordination, as well as to reach the preservation of national prerogatives for security-sensitive actions.

To evaluate whether the EU’s words matched its deeds, we must first seek a clearer understanding of the underlying dynamics of the CDT’s actual application, considering internal and external factors on both institutional and policy levels. Too-unrealistic expectations regarding the CDT’s ability to be a potential all-purpose tool or even a “cyber-pacifier” could distract from its real added value. This is often the case with sanctions, where the focus often lies solely on their deterrent effects, which, if missing, can lead to an overall poor evaluation of the sanctions’ other effects (Peksen 2019). With this in mind, this analysis’ structure follows as such: first, we outline the CDT and its measures in detail before explaining our methodological approach to investigate its usage over the last six years. We then proceed to analyse the concrete application of the CDT by EU institutions/actors up to 31 May 2023, based on a dataset (“CDT dataset”) in conjunction with various other qualitative sources. We argue that - in line with the EU’s overall role as a “soft-power regulator” - the CDT’s history reflects the EU’s role as a preventive “civilian cyber power,” in contrast to a “coercive/restrictive cyber power.” Finally, we discuss our findings in light of the revised implementing guidelines and propose an outlook on the future of the CDT in the years to come.

2. The Framework of the Cyber Diplomacy Toolbox (CDT)

Adopting its Cybersecurity Strategy in 2013 (Commission of the European Union 2013), the EU extended its understanding of cybersecurity from the securitisation of the internal market to the political field of CSFP (Miadzvetskaya and Wessel 2022). This shift laid the foundation for a more substantial European cyber policy and the 2015 adoption of the Council’s conclusion on cyber diplomacy, which aimed at preventing conflicts and fostering stability in international relations in cyberspace. In 2017, the Council adopted the CDT as a legal framework for a joint response to malicious cyber activities in the EU (Council of the European Union 2017a). The CDT, in turn, seeks to support international cooperation with partners and to deter malicious individuals, organisations, or states (Council of the European Union 2017a). Soon after its adoption, the Political and Security Committee passed the corresponding implementing guidelines (Council of the European Union 2017b). These guidelines include five different instruments, ranging from preventive, cooperative, stabilising, and

restrictive measures to punitive measures for self-defence. This set of instruments shall make it possible to react proportionally to the scope and severity of malicious cyber activities on a political, diplomatic, or economic level. The range of instruments also illustrates the different functional levels on which responses to cyberattacks may be situated. In the conclusion of the CDT, the EU underlined that the attribution of malicious cyber activity remains a sovereign act on behalf of the Member States, but also that not all applications of measures rely on an underlying attribution (Council of the European Union 2017a).

Based on the implementing guidelines, these measures are described in the following way:

1. Preventive measures: Preventive are low-intensity measures designed to avert cyberspace conflicts. These consist of confidence-building measures, awareness-raising, and EU cyber capacity-building measures. The objective of awareness-raising is to make other countries aware of the EU's strategic stance on cybersecurity through the démarches of the High Representative of the EU and EU-led political and thematic dialogues. Cyber capacity-building measures, as per the definition provided by the European Commission, aim to establish functional and accountable institutions that can respond effectively to cybercrime. By enhancing a nation's cyber resilience, such measures are designed to receive financial or material support from the EU and help prevent cyber incidents that could impact EU Member States, thereby promoting global peace (Council of the European Union 2018). Capacity-building instruments may encompass short-term or long-term projects, with the latter being facilitated, for instance, by means of the European Neighborhood Instrument (Council of the European Union 2017b).

2. Cooperative measures: Cooperative measures are employed to indicate the severity of malevolent cyber activities for the EU and to solicit support, cooperation, or a joint response from third-party countries against such activities. These measures may also serve as a component of peaceful resolutions following an incident. In doing so, collaborative measures to enhance the EU and its member states' resilience against malicious cyber activities are introduced (Council of the European Union 2017b).

3. Stabilising measures: Stabilisation provisions comprise of statements made by the High Representative (HR) on behalf of the EU Council, Council conclusions, diplomatic démarches conducted by EU delegations, and diplomatic dialogues with states and international or multilateral bodies. The purpose of statements made by the HR is to signal the potential consequences of cyberattacks and to change aggressors' behaviour. The function of statements and Council conclusions is to communicate the EU's awareness of other entities' activities in cyberspace. Council conclusions are thus directed towards other EU institutions and the Member States to encourage political action. Diplomatic démarches are employed to both condemn actions in cyberspace and to request cooperation and assistance from third states to counteract malicious activities. They are therefore expected to be more often tied to concrete cyberattacks than preventive démarches. Besides, démarches and political or diplomatic dialogues can also signal, if known, the origin of the attack and openly condemn the rule/norm violation in cyberspace. Démarches do not need a firm attribution in order to address an attacker's activities (Council of the European Union 2017b).

4. Restrictive measures: Restrictive measures are currently the most robust and escalatory tool used to sanction malicious cyber activities. They can be levied

against third countries, entities, or individuals to modify the target's behaviour through negative economic ramifications. To enhance the Union's deterrence capacity, Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796 were introduced in 2019. These measures directly aim to restrict cyberattacks (Council of the European Union 2019a, Council of the European Union 2019b). Through this framework, the EU implemented a "horizontal sanctions regime" which enables it to enforce travel bans on or freeze assets of sanctioned individuals, organisations, or entities (Council of the European Union 2017b).

5. Possible EU support for Member States' lawful responses: In the event of a serious cyberattack on one of the EU's member states, the CDT also enables the provision of support to Member States in conformity with EU assistance (Art. 222 TFEU) and the Solidarity Clause (Art. 42 [7] TEU). This support can take the form of any lawful measure, from diplomatic measures to stronger responses. So far, it has not been used (Council of the European Union 2017b).

3. Methodology

The analysis starts with the observation that, while there are several qualitative studies on the CDT and its potential for improvement, covering legal, political, and technical aspects (e.g., Miadzvetskaya and Wessel 2022; Poli and Sommario 2023), there is no empirical analysis of the actual deployment of the CDT's instruments since its inception. We therefore created a dataset, compiling data on actions and speeches by EU institutions and actors, which we then categorised according to the different CDT measures to start an evidence-based discussion on CDT instrument deployment patterns and potential explanations for them. An expansion of this focus regarding CDT measures applied by individual Member States would have required an even more extensive research effort. Our timeframe extends from the day of the adoption of the implementing guidelines – 9 October 2017, the date from which the Toolbox is applicable – until 31 May 2023, shortly before the revised guidelines were published.

Our empirical analysis follows a mixed-methods design through compiling quantitative data on qualitative measures. In an unexplored area of research such as the use of the CDT, it is common and appropriate to use quantitative data as a starting point for qualitative analysis since mixed methods support explorative studies (Casula et al. 2021; 1713). In this way, puzzles and patterns can be identified that need to be explored in the subsequent analysis.

First, we provide a detailed description of the data collection process. Then, we operationalise the specific measures of the Toolbox.

3.1. Data

The CDT is an instrument of the CFSP, so we concentrated on the most relevant institutions within CFSP. This aligns with the implementing guidelines of the CDT, which identify the European Commission, the Council, the European Parliament, the European External Action Service (EEAS), and the High Representative of the EU as the most important European entities in this regard. Since we could only capture publicly

reported measures, we focussed our analysis on press releases, speeches, and declarations of the official websites of the aforementioned institutions. Only in individual cases, for specific measures such as cyber capacity-building, we accessed already-existing databases as secondary sources (e.g., [the EU CCB projects mapping by EU CyberNet](#) and the [Cybil Portal](#)). To analyse the website data, we scanned the specific archives throughout the observation period (October 2017 to May 2023) and employed a keyword analysis. Specifically, we further examined all sources that mentioned the keyword “cyber.”

3.2. Operationalisation

To ensure accuracy in our categorisation process, we implemented an additional criterion for the term “cyber,” which is often used in non-CDT related contexts. Measures that specifically target cybersecurity and are aimed at the general public or a third party outside the EU are categorised as “cyber diplomatic measures.” An action is considered a cyber diplomatic measure if its objective is to modify the conduct of actors within cyberspace in general, a specific actor in cyberspace in particular, or to assist a third actor in defensive issues in cyberspace. These measures may be specified further into the five different measures of the CDT (preventive, cooperative, stabilising, restrictive, and EU support for EU Member States’ lawful responses). As the EU’s backing of Member States’ lawful responses has yet to be implemented, we have refrained from their operationalisation. Coding examples and further information about the procedure, as well as our sources, can be found in the [Codebook](#).

3.2.1. Preventive Measures

According to the CDT implementing guidelines, the category of preventive measures includes confidence-building, awareness-raising, and capacity-building measures (Council of the European Union 2017b). For our analysis, we rely on the approach by the Centre for Strategic and International Studies, which defines confidence-building measures as measures that *address, prevent, or resolve uncertainties among states* (CSIS n.d.). Awareness-raising includes measures relating to the EU’s strategic direction in cyberspace and the communication regarding this (Council of the European Union 2017b). Therefore, we count any press statement or speech that references or discusses the risks and hazards of cyberspace or highlights the significance of enhancing cybersecurity as part of this measure. Capacity-building measures aim to enhance cybersecurity capabilities in third countries, specifically regarding responses to the growing number of cyber incidents and the carrying out of investigations into cyber criminals. These initiatives are predominantly documented in various databases, such as the EU CCB projects mapping by EU CyberNet or the Cybil Portal. The respective projects are only coded after the implementation of the CDT, provided that cyber capacities, security enhancements, or cyber resilience strengthening are specifically mentioned in the project descriptions or objectives. Capacity-building measures are also included, as announced in speeches. We count them as preventive measures if at least one of the aforementioned criteria is met.

3.2.2. Cooperative Measures

The CDT implementing guidelines for cooperative measures stipulates that the objectives of these measures are to signal the seriousness of a situation and to request assistance or cooperation in mitigating malicious cyber activities (Council of the European Union 2017b). However, our database adopts a wider interpretation of cooperation, whereby a measure is classified as cooperative if a speech, statement, or press release emphasises the importance or desire for cooperation in the field of cybersecurity with a third party. In addition, we consider pre-existing collaborations within our analysis.

We also differentiate between two types of cooperative measures, as a mere expression of willingness to cooperate does not equate to genuine cooperation. We thus make a distinction between less-committed forms of cooperation, specifically the mere expression of a desire or the importance to cooperate, and a more robust form of cooperation which involves initiating dialogues that can be considered as an initial attempt towards concrete cooperation.

3.2.3. Stabilising Measures

In line with the CDT implementing guidelines, stabilising measures reflect political stances, apprehensions over general cyber tendencies or actual cyber events, or even condemnations of them (Council of the European Union 2017b). Consequently, a measure is classified as a stabilising measure only if it highlights a political perspective on cyber activities or conveys a robust diplomatic message through condemnation or expression of concern. In this section, we differentiate between measures, as the strength of a measure is contingent upon the actor implementing it. For example, given the HR of the EU's prominent role in European security policy, their statements on cyber activities and threats are considered stronger measures than those from other institutions. In general, attributions are expected to mostly fall in this category.

3.2.4. Restrictive Measures

Restrictive measures fall under the umbrella of the EU's cyber sanctions regime (Council of the European Union 2017b). A measure is considered restrictive when it enforces sanctions against third countries, entities, or individuals for either attempting or successfully carrying out a cyberattack.

4. Analysis

We begin our analysis with an overview of our dataset to identify significant patterns, trends, or anomalies that merit further attention in the second part of the analysis.

4.1. EU's CDT application from 2017 to May 2023: patterns, trends, and anomalies

A total of 243 measures linked to the CDT were identified during the examined period for the aforementioned EU institutions as investigated actors. Of these 243 CDT measures, 105 were preventive, 63 were cooperative, and 73 were stabilising. Two instances of restrictive measures, both in the form of sanctions, were applied. The most consequential measure, the EU's potential support of a lawful response by a Member State, was not implemented (see Figure 2).

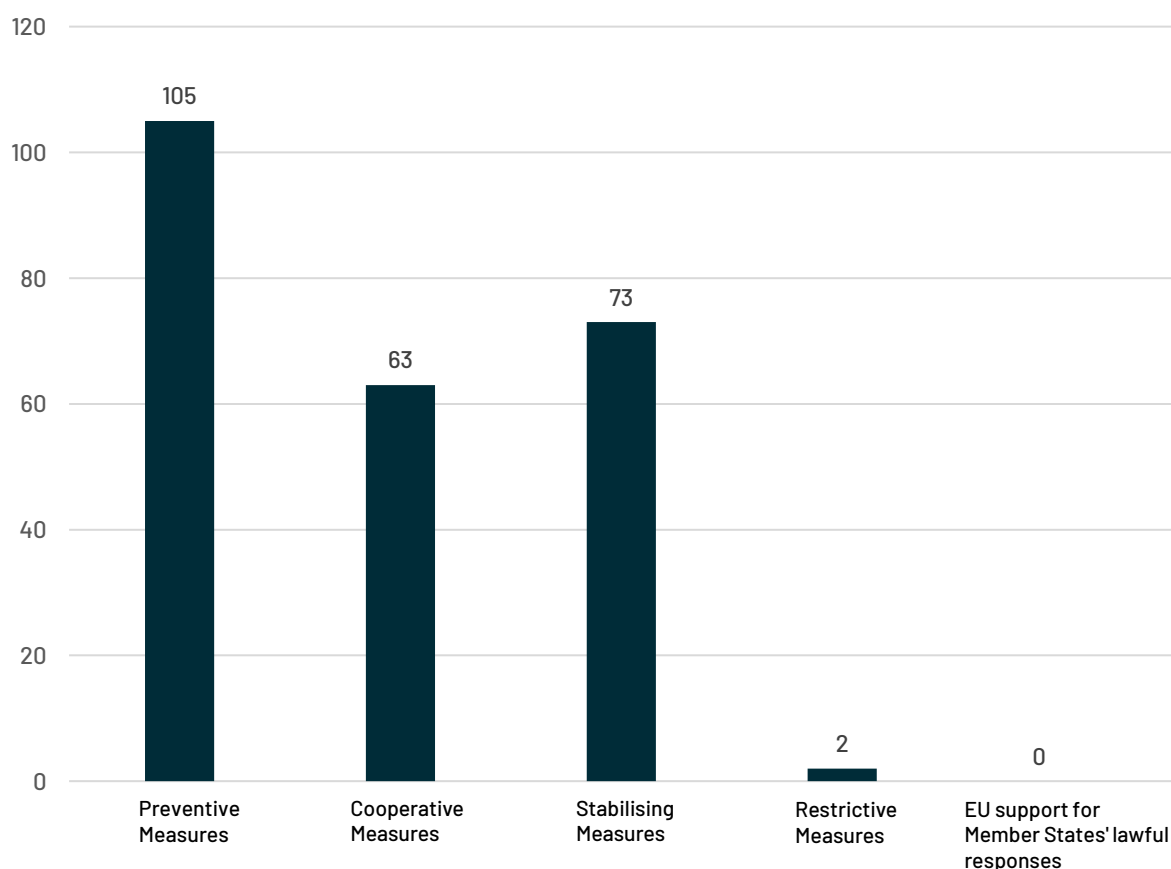


Figure 2. Distribution of applied CDT measure types from October 2017 to May 2023 (source: CDT dataset).

Since 2017, there has been a gradual increase in the usage of the Toolbox's measures. Its application grew from 29 uses in 2018 to 34 in 2020 and 37 in 2021. In 2022, 80 measures were applied, reaching a peak of CDT utilisation thus far (cf. Figure 3).

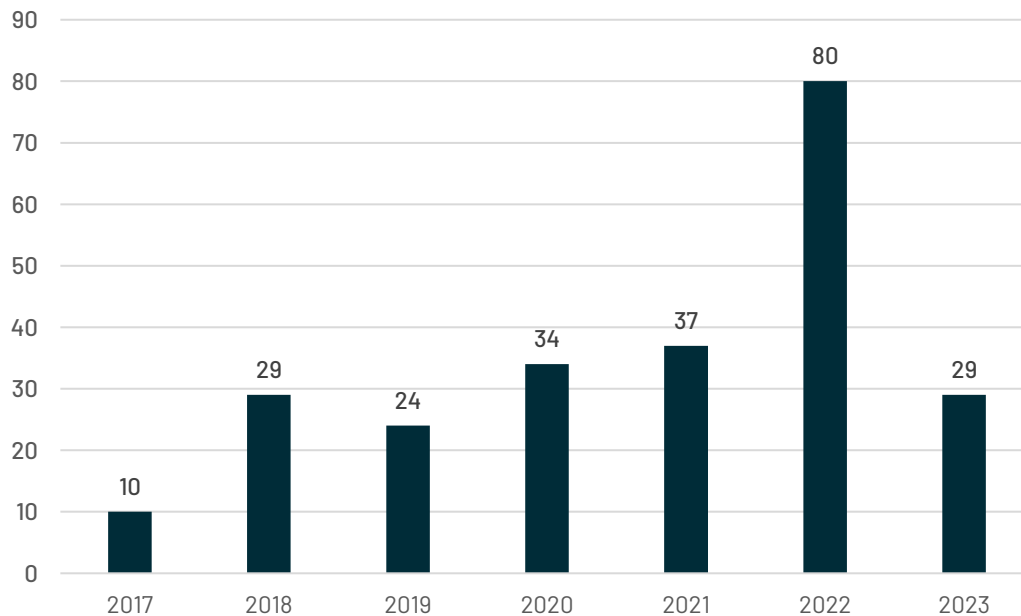


Figure 3. The application of CDT measures over time (source: CDT dataset).

The CDT database indicates a clear impact of the Russian war against Ukraine on EU cyber diplomacy. Out of the 243 measures recorded, 58 were related to Ukraine, which falls just short of 25% of the total number of measures recorded. 54 out of 58 measures were implemented after January 2022. Among the 80 CDT measures taken in 2022, the EU employed 27 between 23 February and 31 March 2022, coinciding with the onset of the Russian war against Ukraine. The employment of stabilising measures, such as statements condemning the Russian cyber-threats in Ukraine, experienced a peak shortly after the onset of hostilities. In March 2022, twelve stabilising measures were executed, followed by four measures each in May and June 2023.

Out of the 105 measures for preventive action, 16 could be categorised as capacity-building measures. Most of these measures were carried out in regions geographically close to the EU. Specifically, six capacity-building projects were implemented in Balkan or western Balkan countries, two were implemented in member states of the European Eastern Partnership, one was implemented in Georgia, and another was in Moldova. Concerning Ukraine, four projects were initiated, with two taking place after the onset of hostilities. Only two capacity-building projects were initiated further abroad: one in the Horn of Africa and one in partnership with ECOWAS member states (Economic Community of West African States). Both projects aimed to support the region’s overall digitalisation efforts, including defence against cyberattacks (cf. Figure 4).

The CDT also provides for dialogues with other countries as part of cooperative or stabilising measures to share information about cyber-threats, combat malicious cyber activities, or express condemnation of recent attacks. These CDT dialogues are frequently held with G20 member states, such as the US (four times) and China (twice) (cf. Figure 5).

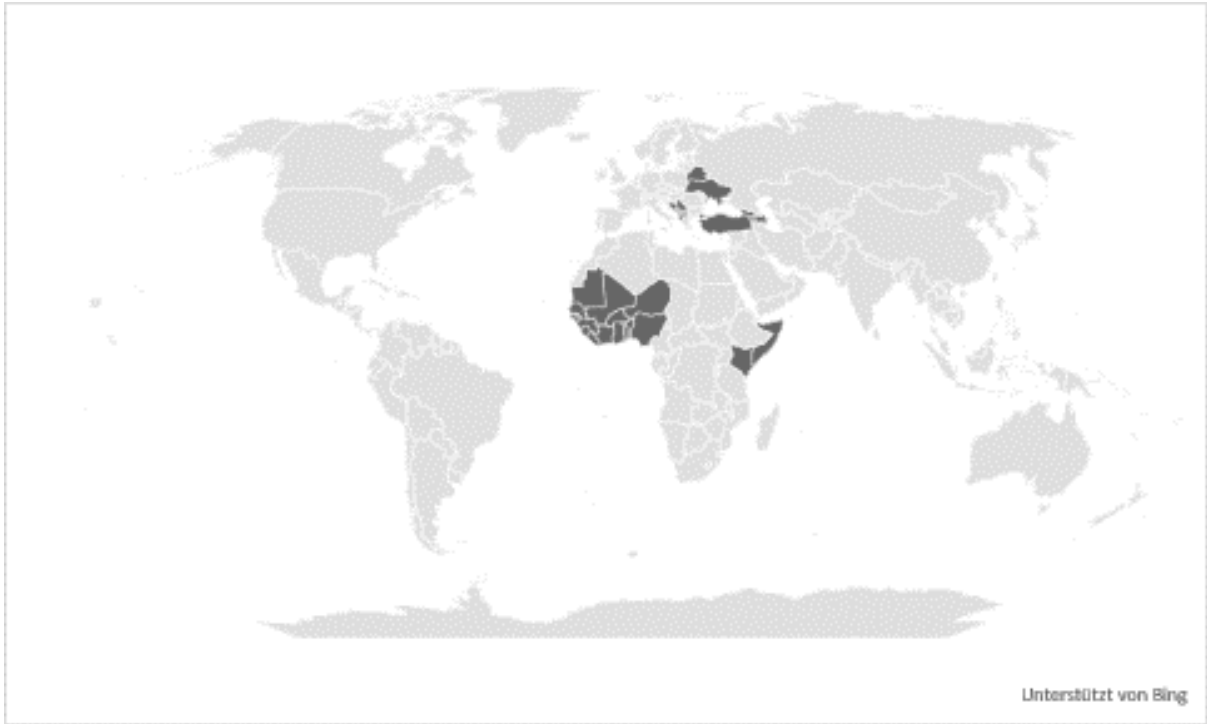


Figure 4. Countries benefitting from the CDT's capacity-building measures (source: CDT dataset).



Figure 5. Dialogue partners of the EU within the framework of cooperative measures (source: CDT dataset).

The findings show that dialogues were not constrained to countries in close proximity to the EU, but rather, the dialogues extended globally. In total, the CDT expressed “support,” “cooperation,” or a “wish for cooperation” with another state, region, or organisation 44 times, although measures taken were not always explicitly classified as dialogue-related or within capacity-building. Following the outbreak of the Russian war against Ukraine, 17 of these measures came into effect. The EU aimed to create various measures through the CDT to respond to malicious cyber activities. Consequently, stabilising measures were established to counter such activities more severely, with a total of 73 measures, which were invoked more frequently than cooperative measures. The actual impact of a statement, speech, or declaration can vary within a single measure. The most impactful stabilising measures are likely the démarches of the EU HR, given that their function is to coherently coordinate the CFSP of the EU with Member States. Excluding these démarches, more impactful stabilising measures were only utilised eight times.

Apart from those action-endorsing measures, the CDT also foresees the option to sanction other actors/entities, in line with its restrictive measures. These sanctions were implemented for the first time in July 2020 against two Chinese and two Russian individuals, as well as three entities: the Centre for Special Technologies of the Russian Armed Forces, Chosen Expo in North Korea, and an entity in China. In October 2020, the sanctions regime was implemented for the second time, targeting two Russian individuals and the Main Directorate of the Chief Staff of the Russian Armed Forces (GRU). The sanctions were imposed due to past cyber incidents. The previous sanctions, issued in July 2020, were a response to the [WannaCry](#) and [NotPetya](#) attacks of 2017, the 2017 [Operation Cloud Hopper](#), and the attempted attack against the Organisation for the Prohibition of Chemical Weapons (OPCW) in 2018. The sanctions imposed in October 2020 were related to the hack against the [German Bundestag](#) in 2015. Unlike many actions carried out under other categories of measures, sanctions respond to specific cyber incidents, potentially involving attributions. However, the EU decided to circumvent the sensitive issue of potentially assigning direct responsibility for a cyber operation to another state with its Council decision from May 2019, as it underlines the targeted nature of the restrictive measures and excludes any attribution of responsibility for cyberattacks to a third country, in contrast to the original Council guidelines from 2017 (Miadzvetskaya and Wessel 2022; 434). When considering only measures implemented within a year of a specifically referenced cyber incident, or measures explicitly linked to an incident, such as sanctions, the count is only 45. Out of those, 24 are connected to the Russian war against Ukraine. [NotPetya](#) (8) and [WannaCry](#) (10) were the most frequently mentioned incidents, followed by the attempted attack on the [OPCW](#) (6) and the attack on [ViaSat/KA-SAT](#) (7). Specifically, the KA-SAT attack on 24 February 2022 is noteworthy for being the only incident that has been officially attributed to a state by the governments of the US, United Kingdom, Canada, and Australia, as well as through a statement by the High Representative of the EU (Kerttunen, et al. 2023; 5). Also notable is the relatively high number of measures (8) meant to respond to incidents affecting critical infrastructure targets, such as health services and political institutions, thus reflecting the strong emphasis the EU puts on threats to critical infrastructure targets since its adoption of the NIS2 Directive.

The various CDT measures do not have an equal association with incidents. The impact of a measure appears to be correlated to the number of connected incidents:

as previously mentioned, both restrictive measures are connected to cyber incidents. Out of the 73 stabilising measures, 27 were linked to an incident, whereas merely two of 63 cooperative measures and 14 of 105 preventive measures were associated with specific cyber incidents. Notably, out of the eight statements released by the High Representative regarding cyberspace, seven were associated with specific cyberattacks. It seems plausible that incidents that are generally perceived as more intense or impactful are more likely to be the subject of public statements. In turn, it also highlights a more strategic and long-term aspiration of many preventive and cooperative measures in contrast to more consequential, *ad hoc* statements as part of stabilisation efforts in the wake of cyberattacks.

In sum, the findings indicate that the EU directed its preventive measures (capacity-building) mostly towards its “friends,” namely those within Europe. In contrast, more strategic and less operative dialogues used as cooperative measures concentrated on G20 states, but also on “rivals” such as China. With regards to sanctions, it stands to reason that cyber incidents with a wider spectrum of negative consequences and greater “public attention,” as well as their respective perpetrators, were targeted more frequently compared to actors in “smaller,” less attention-seeking incidents for which there is usually a less-consolidated technical evidence base. The case of the attempted hack of the OPCW stresses that the actual technical impact of an attack is obviously only one qualifier for CDT inclusion. Rather, if attempted hacks violated the EU’s position on responsible behaviour in cyberspace, they could also be addressed through sanctions or other measures. And yet, even if this politically-driven decision-making seems politically intuitive, it does not strengthen the transparent and coherent application of the CDT in accordance with its core criteria. It also stands out that the EU has found a way to avoid politically-sensitive allocation of responsibilities to a state by imposing sanctions on individuals or entities instead. This highlights the challenges faced by Europe in establishing a common standard for attribution, as well as effectively applying international law to cyber conflicts; it also indicates a lack of shared interest in promoting those two objectives (Poli and Sommario 2023). Finally, the strong uptick in measures related to Russia’s war against Ukraine demonstrates the relevance of the full spectrum of CDT instruments, particularly during conventional armed conflicts.

The European Repository of Cyber Incidents (EuRepoC) also provides some first insights into the Member States’ employments of actions that can be categorised under the measures within the CDT framework. The EuRepoC dataset covers direct political responses to specific cyber incidents since September 2022. The data for this time frame, which covers through May 2023, encompasses cyber incidents that affected at least one EU Member States (see Figure 6) and indicates a slightly different distribution of applied CDT-like measures on the Member State level compared to the supranational level. For 17 of 237 incidents that have been added to the EuRepoC database from September 2022 until 15 January 2024 and affected at least one EU Member State, political responses by one (or more) have been recorded. In contrast to the official CDT measures, Member States most frequently used actions that can be categorised as “stabilising” measures, such as statements made by ministers, heads of states, or subnational officials. Preventive measures, such as awareness-raising technical alerts or capacity-building measures, come in second place. The EuRepoC database only records state-initiated measures that are *direct* responses to specific cyber incidents, which is even more reasonable for statements and speeches in the

sense of stabilising measures than for capacity-building measures. This could partially explain the different ranking of those types of measures in comparison to the official CDT measures applied by EU actors, which were most often implemented independent of particular cyber incidents.

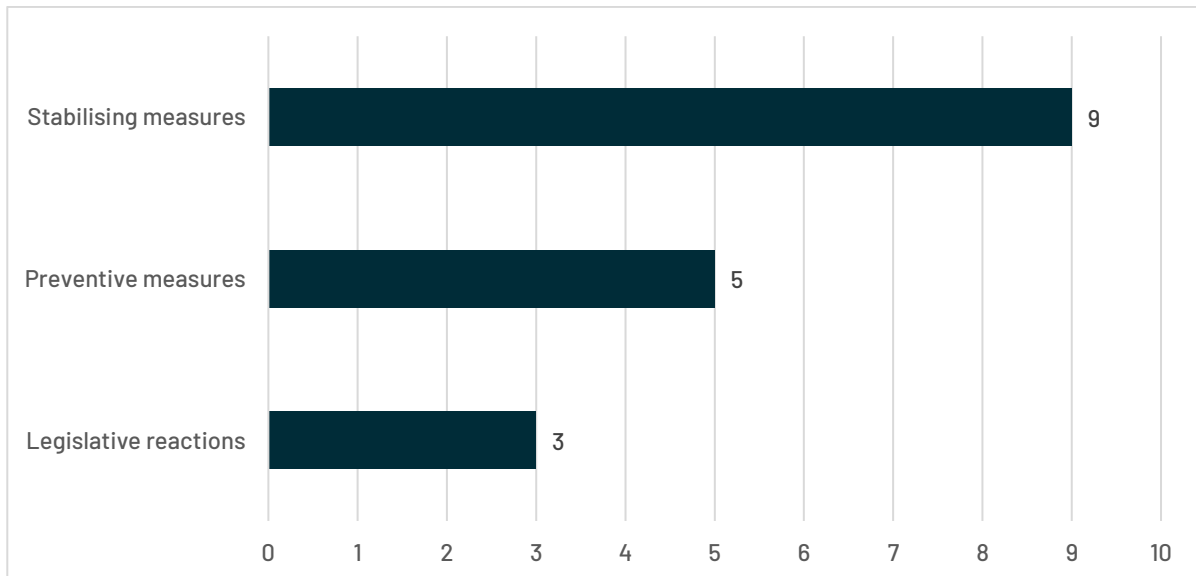


Figure 6. EU Member States’ political responses for cyber incidents affecting at least one EU Member State, added to the EuRepoC database from September 2022 to January 15, 2024 (source: EuRepoC dataset). *Legislative reactions* are not included in the CDT framework and comprise legislative initiatives, parliamentary investigative committees, and dissenting or stabilising statements by Members of Parliament.

4.2. Spotlight Analysis

Having set the stage by analysing general trends in the application of CDT instruments, we now turn to a more in-depth analysis of specific CDT measures. According to the descriptive analysis presented, a discernible pattern can be observed in the utilisation of capacity-building measures and dialogues. Given the existing literature’s emphasis on the sanctions regime (see Moret and Pawlak 2017; Tomas Colatin 2020; Calleri 2020; Kapsokoli 2021; Miadzvetskaya and Wessel 2022; Poli and Sommario 2023), we focus on preventive and cooperative measures, with a particular emphasis on cyber capacity-building and the occurrence of dialogues. Following this, we aim to identify patterns of usage for more consequential measures, including stabilising and restrictive measures. Considering the pertinence of current affairs and standout discoveries relating to the Russian war against Ukraine, we will examine how this conflict has influenced the utilisation of the Toolbox’s prescriptions.

We also highlight preventive and cooperative measures because of their different “targeting logic.” While most preventive measures, in the form of capacity-building, were aimed at assisting friendly third states with lower cyber capabilities, cooperative measures mostly involved high-level strategic dialogues with better-equipped (and not necessarily “friendly”) states.

4.2.1. Helping states to become cooperation partners: preventive and cooperative measures

Starting with the EU's CDT capacity-building measures, a clear geographical pattern emerges: there are four capacity-building projects in the Balkans, with three of them being in the western Balkan states, as well as two in the Eastern Partnership states. Moreover, there are additional separate projects for individual states such as Moldova, Turkey, or Georgia. Four additional projects are implemented in Ukraine. Furthermore, there is one separate joint project for the states of Albania, Montenegro, and North Macedonia. These states are all close to EU-Europe and they are all candidates for an EU membership, or they are at the very least part of the European Partnership Program (except for Belarus) (European Union n.d.; Council of the European Union & European Parliament 2014). Additionally, all the aforementioned states are also either bordering or geographically close to Russia. Plus, according to various EU institutions' speeches and press releases, some of these states are also themselves common targets of cyber threats (#137, #177, #183).¹ Upon closer inspection of the implemented programmes themselves, it is noteworthy that the majority of these projects strive to strengthen cybersecurity measures in adherence to EU standards, evaluate legal frameworks in alignment with the NIS2 Directive, or to adopt legislative and policy frameworks of the Budapest Cybercrime Convention. Notably, only two of the Ukrainian projects implemented during wartime fail to mention such standards.

The two additional projects further abroad, one in the Horn of Africa and one in cooperation with ECOWAS as mentioned in Section 4.1, notably do not refer to norms, with their sole purpose being improving cybersecurity. Given the smaller degree of shared normative values with Africa in contrast to southeastern European states, this does not come as a surprise. Furthermore, the projects were sponsored through development funds and implemented by Expertise France, the agency for French international technical cooperation projects, which may indicate a higher degree of trust between the respective African states and French authorities due to their closer historical ties.

The French involvement in cybersecurity capacity-building is not limited to Africa; it also covers the Balkan region. In 2022, France and Slovenia began the "Western Balkans Cyber Capacity Centre (WB3C)," located in Montenegro and serving as a training center in the fields of cyber-crime, cybersecurity, and cyber diplomacy (La France au Monténégro 2023). France shows a great interest in bilateral/trilateral cyber capacity-building measures with multiple different conceivable motives (e.g., lower-threshold implementation and/or greater influence on the implementation than under the EU CDT auspices).

Smaller African states that are increasingly becoming digitised, but which have inadequate national cybersecurity programmes, are eligible for support through EU capacity-building measures. This is due to the continent increasingly becoming a hub for cyber-crime, which not only threatens companies within Africa, but also those back in Europe, as cyber-crime tools, tactics, and techniques continue to proliferate. The "cyber-crime strategy" by AFRIPOL (African Union Mechanism for Police Cooperation) for 2020 to 2024 underlines the existing mutual interest in cyber

¹ If a statement refers to a specific case from our database, we quote the ID of the respective observation with "#".

capacity-building cooperation, and it calls for closer coordination with EUROPOL (Diplo 2023).

However, having a poorer cybersecurity record seems to play a more important role for conducting capacity-building projects in African states than for those located in Europe. Turkey, North Macedonia, or Armenia, for example, score better in the International Telecommunication Union's Cyber Security Index (2020) than, for example, EU Member States such as the Czech Republic or more-developed states such as Switzerland.² It is reasonable for the EU to prioritise investing in operational-level relationships with states prior to any potential accession in order to mitigate cybersecurity risks for the Union as a whole.

We conclude that the EU executes cyber capacity-building initiatives via three approaches. First, it deploys cybersecurity capacities in states that are geographically close by, and which are relatively frequent targets of cyberattacks. This is intended to enhance security via operational augmentation of security capacities and through deterrence. Enhanced cybersecurity in neighboring states benefits the EU by preventing cyberattacks from spilling over into its borders. Second, the EU spreads its norms in the geographical neighborhood by linking capacity-building to the alignment and implementation of EU norms. Therefore, the capacity-building measures are not solely a defensive measure, but rather, they are able to create a normative space. Third, the EU provides support to states (far) beyond its geographic boundaries, albeit to a lesser extent. Since the cybersecurity status holds significance in this context, capacity-building efforts primarily strive towards development objectives. A closer look at the cooperative measures reveals three different "groups" within the EU's previous employment of cooperative measures: 1) the states benefitting from preventive measures, 2) Western-allied states, and 3) internationally powerful non-Western states.

For the first group, comprising the aforementioned states/regions (Balkans, West Balkans, Georgia, Moldova, and Ukraine), the recorded CDT documents reveal a dominance of "perseverance slogans" which call for a continuation and expansion of the established cooperation (#111).

The second group brings together powerful Western states such as the US, Canada, and Australia. Here, the wording of the speeches and statements is cooperative and welcoming. For example, the documents discuss "deepening our cooperation" (#216) or emphasise cooperation so far: "The cooperation on this, between the EU and Canada, has been excellent" (#85) and "There is also strong transatlantic cooperation on this issue. It is discussed in the EU/US security and cyber dialogues" (#26). Even where no cooperation existed prior, the press releases still emphasised togetherness: "In this regard, they recognized the contribution of the Sydney Dialogue and welcomed the EU's possible future participation" (#204). Additionally, not only the wording of speeches is remarkable, but also the amount of dialogues with those states is noteworthy. There have been four dialogues with the US, and US-EU cooperation was additionally mentioned in four other speeches. There have also been five dialogues with Canada and two with Australia. In sum, these cooperative dialogues appear to function as signals to other parties, such as rivaling autocratic states, that the EU and its' partners share a deep mutual understanding of

² We are aware that cyber capacity-building measures are also one of the evaluation criteria used for the index. This could serve as a potential explanation as to why some of those states are ranking surprisingly higher than expected. Additionally, some data, for example for Switzerland, is missing, which could also be the reason for the lower ranking.

core cybersecurity norms, values, and priorities. At the same time, it also empowers the EU through cooperation with technically advanced states, especially members of the Five Eyes intelligence alliance.

Rivaling autocratic states were also part of EU cooperative measures, albeit less frequently and often accompanied by a different rhetorical framework. Against the backdrop of the high number of cyber operations against targets from the EU that were attributed to Russia (90 incidents) and China (45 incidents) and recorded in the EuRepoC database until mid-January 2024, the general aspiration to maintain some kind of communication channel seems plausible. However, the tone of the EU's accompanying statements is much stricter, less consensual, and more instructive than those directed towards allied states. For example, the press release of the EU-China summit states: "The EU recalled the importance of the application of international law and cooperation against malicious cyber activities, including on ICT-enabled theft of intellectual property, for an open, stable and secure cyber-space" (#38). Another instructive example is the press release following a telephone dialogue between European Council President Charles Michel and Russian President Vladimir Putin: "From the EU perspective, the relationship with Russia can only take a different direction if there is sustained progress on issues like the implementation of the Minsk agreements, stopping hybrid and cyberattacks on Member States and respect for human rights" (#105). Consequently, framing those measures as "cooperative" is itself diplomatic since they appear to serve the main purpose of communicating the EU's norms and values in an international context and signaling its position towards notorious norm-violators. In summary, the EU's use of cooperative measures distinctly reflects the varying relationships the Union maintains with the addressed states, leading to adjustments in the related objectives accordingly.

4.2.2. Sanctioning out of the comfort zone: stabilising and restrictive measures

Although our dataset indicates that the stabilising measures have been used frequently, the significantly potent measures – the declarations of the High Representative of the EU – have been used considerably sparingly. From 2017 to 2023, the HR issued only eight declarations. Moreover, restrictive measures have also seldom been utilised – only on two occasions. We will therefore take a closer look at the applications of the stabilising and restrictive measures.

We analysed speeches and statements implemented by the European Council, European Commission, and HR as stabilising measures. Nevertheless, as the HR's declarations are the most potent within this category, we will focus our attention on them. Upon closer inspection of HR declarations over time, it is worth noting the absence of any mention of "cyber" before 2020. Another notable discovery is that the language used has evolved, with formulations becoming more stringent and direct. In response to an October 2019 cyberattack in Georgia, the first HR statement was released in February 2020. It is noteworthy that four months passed before a statement was issued regarding cybersecurity, and that the first statement pertained to a non-EU Member State. Furthermore, the statement came one day after the UK attributed the cyberattack to the primary intelligence service of the Russian military, the GRU (National Cyber Security Centre 2020). However, the EU statement merely

condemns the attack and expresses its concerns without addressing the attribution. The initial statement lacked clarity as it did not provide specifics on any particularities of the attack, it did not clarify the origin or actors involved, and it expressed a subjective evaluation.

Notably, the EU changed its cyber threat communications approach after the [SolarWinds campaign](#), which primarily targeted the US. The SolarWinds campaign marks the first instance in which the HR solely expressed concerns without explicitly condemning the attack, instead reiterating the US attribution towards the Russian regime, but without indicating consent on this. In response to the cyberattack on Microsoft Exchange servers by China's APT40 and APT31 three months later, both the attackers and the country of origin were mentioned for the first time without qualifying phrases such as "suggested" or "adjusted." However, the attribution only points to China as the suspected country of origin, without indicating a state responsibility for the operations. In these cases, EU Member States were also directly impacted. The High Representative vehemently condemned the attack, urging China to conform to the accepted norms of responsible state behaviour in cyberspace, namely not allowing its territory to be used for malicious cyber activities, once again reflecting the missing attribution of direct state responsibility and instead indicating a violation of the principle of due diligence. The declarations regarding both the SolarWinds and Microsoft Exchange hacks reflect the EU's desire to avoid assigning direct state responsibility for cyber operations to third states. This is achieved through two different rhetorical techniques.

Another significant statement was that concerning the [Ghostwriter campaign](#), which (thus far) is only "associated with Russia" (#109) broadly, even though the Polish and German governments had previously attributed it specifically to the threat actor UNC1151. It is noteworthy that, although Poland requested to apply the Toolbox in this case, the sole public response, initially, was the denunciation of malicious cyber activities against Poland and Ireland, as stated in the EU Council Conclusions of June 2021 (#109). However, when Germany advocated for the Toolbox's implementation, a declaration by the High Representative emerged only a few days later (Soesanto 2021). Interestingly, the European Union appears to implement more robust measures only if a cyber incident affects another EU Member State that is particularly actively engaged in cyber diplomacy. In this specific case, though, it remains unclear whether the statement disseminated by the HR reacted to German insistence or if it reacted because of the involvement of another EU state.

The HR's two latest declarations pertain to Ukraine. The first one was released in January 2022, on the same day the [WhisperGate](#) wiper attack occurred. In it, the High Representative condemned the attack on the Ukrainian government websites, but the perpetrator was not mentioned. The second declaration was issued in July 2022, recalling the condemnation of cyberattacks in January and the attribution of the [KA-SAT attack](#) to the Russian Federation on 10 May 2022. Notably, the effects of the KA-SAT incident also impacted the EU, but the HR failed to mention that EU members were affected, while also condemning other recent DDoS attacks on EU Member States. Nevertheless, it is the first HR declaration on behalf of the EU to communicate an attribution statement that can be interpreted as the assignment of direct state responsibility for a cyber operation. The declaration also employed tougher language, specifically mentioning the "unacceptable risks of spillover effects, misinterpretation, and possible escalation" and stating that the EU "strongly condemns this unacceptable

behavior in cyber-space” (#189). Noticeably, every statement made by the HR draws a different group of states to align with it, revealing a missing level of coherence and unity when it comes to the attribution and verbal condemnation of malicious cyber behaviour.

Strong condemnations by the High Representative of the EU may occur when cyber incidents affect either EU Member States or (closely aligned) non-members. Thus far, only one direct attribution to another state has been made by the HR regarding the KA-SAT attack. It stands to reason that enduring conflicts lower the level of restraint for the HR to issue “genuine” political attributions against the offender. If this is the case, this pattern is also in line with the existing national prerogatives for political attributions of cyberattacks as part of the CFSP. Therefore, the High Representative was able to attribute a cyber operation in Russia’s war against Ukraine at a relatively low political cost because there was a close and coordinated action to support Ukraine against Russia. A similar effect may be observed for attacks that have been attributed internationally by allied states but without a direct involvement of the EU itself or its member states. Regarding internal EU politics, the example of Ghostwriter suggests that more powerful or more engaged states may find it easier to convince other Member States to commit to a united response under the CDT than other states, but also that the scope and quality of shared attribution evidence may also play an important role.

The patterns identified for stabilizing measures are supported by the findings for restrictive measures: here, there were two applications, in which eight individuals and four entities were sanctioned. The sanctions were all imposed because of major cyber incidents: [WannaCry](#), [NotPetya](#), [Cloud Hopper](#), and the [Bundestag-Hack](#); the exception being the attempted OPCW attack, which was stopped even before it started. All of them (except for the OPCW case, as it is not coded due to the missing violation of the CIA Triad) were rated with 4 out of 15 possible points in the intensity scale in the EuRepoC dataset (EuRepoC 2023). While still moderate, these operations are significant when compared to the overall intensity average of 2.23 for all incidents (2556 in total) covered by the EuRepoC dashboard (as of 15 January 2024). Most of the operations aimed to affect critical infrastructure or political targets in EU Member States. WannaCry affected the NHS in the UK, Deutsche Bahn in Germany, a financial service in Spain, and the telecommunications companies Telefonica and O2 both within Spain and Europe more broadly. NotPetya hit, among others, the Danish container shipping company Maersk. The Bundestag-Hack primarily impacted the German Federal Parliament. Interestingly, each sanctioned operation targeted at least one more powerful (current or former) EU Member States: the UK, Germany, or France, further supporting engagement or power hypothesis (Bendiek/Schulze 2021).

The case of the hack against [TV5 Le Monde](#) from 2015 can be considered an outlier here, as it affected a French target but was not addressed through a joint EU response. Given France’s focus on strategic autonomy, it can be argued that the French government had a specific interest in acting independently from the EU’s institutional frameworks regarding cyberattacks that exclusively impacted French entities (Soesanto 2020).

The rare application of EU sanctions may also be partially explained by the missing EU attribution mechanism. Given that state governments, such as the French and German governments, emphasise the necessity for state prerogatives in attributing cyber operations, more frequent EU attributions as in the case for the KA-

SAT hack and aligned sanctions should not be expected to occur very frequently in the future. The entry threshold appears low enough for a unified EU approach only when there is a high-impact event pertaining to cyber-adversaries already targeted by sanctions within the conventional sphere. It appears that diverging attribution capacities and the need for intelligence provisions by allied third countries further hamper a joint response (Soesanto 2020; Bendiek and Schulze 2021), as does a lack of political will among Member States to allow the EU to assign state responsibility for cyber incidents. Interestingly, Poli and Sommario observe that, in cases of restrictive measures addressing non-digital threats, the Union has never openly indicated that legal attribution should be left only to Member States (2023; 535).

Potential obstacles for common action are also partially highlighted by the revised CDT implementing guidelines. But these guidelines focus much more on the potential benefits of joint EU attributions, as to *“expose the specific malicious cyber activity or specific actor, enable mitigating initiatives, promote the UN framework for responsible state behavior, demonstrate capability to identify its origin, discourage future malicious cyber activities, as well as to enable other response options to be used sequentially or in combination with the attribution and raise awareness about the cyber threat landscape”* (Council 2023, 18).

Focussing on Ukraine, we observed a significant increase in preventive and stabilising measures since the onset of hostilities. Preventive measures were focussed on operational improvements, also in neighbouring countries such as Moldova or Transnistria. The number, and also the language, of the stabilising measures changed; the European External Action Service (EEAS), for example, issued statements such as *“Russia also must stop its disinformation campaign and cyberattacks”* (e.g., #168, #179, #182). Moreover, two declarations by the HR were published against the background of cyberattacks in Ukraine, one of them during the war. If political circumstances require it, EU Member States seem to be capable to reach a consensus, even for a joint attribution of an attacker residing in Russia. But why, then, did the EU not implement additional sanctions against Russia because of cyberattacks such as the KA-SAT incident? The following reasons may be considered: first, there were already extensive EU (and other international) sanctions in place; more sanctions would likely not have had much, if any, additional effect. Second, sanctions may have increased escalation risks vis-à-vis the EU, but the EU’s condemnation of Russian war atrocities may be interpreted as an even more escalatory step. Thus, the least the EU could do was to regularly condemn Russian cyber operations in statements, speeches, and declarations as part of its stabilising measures.

5. Conclusion


The European Union, its member states, and its institutions have considerably broadened and deepened their activities and instruments to detect, resist, and repel nefarious cyber operations by state and non-state actors. These tools, and the Cyber Diplomacy Toolbox in particular, are bound to grow, to broaden, and to sharpen themselves as the EU's threat environment continuously evolves (ENISA 2023). The preceding analysis has foregrounded the evolution of the Cyber Diplomacy Toolbox and its various instruments, thereby presenting the first evidence-based assessment of the CDT since its inception in 2017.

The analysis focusses on identifying trends and patterns in the application of the CDT's primary functional tools by EU institutions/actors. In assessing their use, as well as the change in application and the respective politics within and among the EU and its member states and institutions, we identify several non-intuitive and henceforth undetected patterns.

First, preventive measures by far dominated other tool applications quantitatively, with stabilising and cooperative measures following suit. In turn, the EU uses restrictive measures, such as sanctions, rarely. Overall, the use of CDT measures over time has clearly increased, with measures taken in the context of Russia's aggression against Ukraine being a strong driving factor.

Second, capacity-building initiatives were most frequently applied as preventive measures. These capacity-building measures mostly addressed states that were candidates for EU accession, thus the entry barriers for such measures were rather low.

Cooperative measures, such as strategic dialogues, were directed towards powerful cyber-allies and powerful cyber-adversaries alike. Consequently, the tone of the employed measures, mostly statements, varied significantly, reflecting the diverse aims pursued, such as signaling alliance-coherence/unity compared to signaling and defending the union's normative values vis-à-vis strategic rivals, such as China. Third, focusing on the discursive dimension of the CDT's instruments, we find substantial evidence that the EU's stabilising measures still use open and often vague diplomatic language, thus allowing for ambiguous interpretations by various actors (Byers 2020). In our dataset, we identified only one joint attribution, the one towards Russia for the KA-SAT operation, which used clear and unambiguous language. While political attributions of cyberattacks remain national prerogatives, a pragmatic interpretation follows that the diverging cyber incident detection and attribution capabilities among the 27 Member States will probably persist for some time, necessitating an ever-closer coordination of attribution policy among Member States and EU institutions. Fourth, given that Member States have different priorities and capacities when it comes to cybersecurity, it is no surprise that some state governments are more prone to influence collective EU actions than others. It follows that the application of CDT measures becomes more likely if and when engaged states, such as France and Germany, are affected or interested in a diplomatic EU response, even if this does not automatically result into a restrictive measure being employed, such as sanctions. However, make no mistake; fifth, if engaged Member States, particularly France, prefer exclusive control over national responses, they may prefer to retain the full spectrum of strategic autonomy vis-à-vis the suspected adversary.



Lastly, most of the observed CDT measures were not directly linked to specific cyberattacks. Five years into the application of the CDT, the question remains as to why some cyber operations trigger a response while others do not, and if they do, why not all available tools are used. While no clear-cut behavioural pattern by the EU was to be expected, avoiding haphazard or ambiguous signalling towards friends and foes in cyberspace clearly should be a policy priority for the European Union as it reviews and adapts its Cyber Diplomatic Toolbox.

More specifically, the CDT does not yet meet the criteria of providing a toolbox for a punishment-based deterrence policy, among other reasons because it lacks attribution capabilities. At this stage of its evolution as a cybersecurity policy actor, the Union is capable of implementing preventive measures and thus of pursuing a denial-based deterrence strategy. It follows that the CDT primarily assists neighbouring countries in boosting their own cyber resilience, and by proxy the EU's. By regularly organising dialogues and other cooperation initiatives with so-called "political swing states," i.e., those who switch between the Western stakeholder approach and the state-sovereignty based approach, as well as leaders from the latter camp, such as China, the EU also positions itself as a norm entrepreneur in cyberspace.

We also found considerable evidence that the EU united behind Ukraine in its fight against Russian (cyber-) aggression. Given that the pertinent literature suggests that cyber operations are generally less escalation-prone (e.g., Kostyuk and Zhukov 2019), one might argue that the EU could adopt much more restrictive measures in the event of severe cyber operations, even if those occur against the backdrop of enduring conventional conflicts. It follows that we anticipate more frequent application of the CDT's restrictive measures during conventional conflict. This could also be the case for the recent conflict between Hamas and Israel that began in October 2023, even if no HR statement pertaining to the cyber dimension of the conflict has been published so far. The expected potential (moderate) increase of restrictive CDT measures in particular pertains to joint attributions, as encouraged by the revised implementing guidelines.

In the future, intra-European dynamics may not be the only driving forces that determine whether Member States can agree on joint measures within the CDT framework, such as sanctions. Instead, geopolitical conflicts and the course of the USA in the years following 2024 may also impact their implementation, and attention should be given to how these factors influence the application of CDT measures in the future.

6. References

- [1] BBC (2017). *Massive ransomware infection hits computers in 99 countries*. Available at <https://web.archive.org/web/20240111070218/https://www.bbc.com/news/technology-39901382> [Archived on: 13.01.2024].
- [2] Josephine Wolff (2021). *How the NotPetya attack is reshaping cyber insurance*. Brookings. Available at <https://web.archive.org/web/20240112153942/https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/> [Archived on: 12.01.2024].
- [3] Kerstin Zettl-Schabath and Sebastian Harnisch (2022). *One Year of Hostilities in Ukraine: Nine Notes on Cyber Operations*. European Repository of Cyber Incidents. Available at https://web.archive.org/web/20240116075311/https://strapi.eurepoc.eu/uploads/One_Year_of_Hostilities_in_Ukraine_59f3e36897.pdf?updated_at=2023-04-20T12%3A19%3A26.189Z [Archived on: 16.01.2024].
- [4] ICRC (2023). *Protecting Civilians Against Digital Threats During Armed Conflict: Recommendations to states, belligerents, tech companies, and humanitarian organizations*. From the International Committee of the Red Cross. Available at <https://web.archive.org/web/20240114101300/https://shop.icrc.org/download/ebook?sku=4735/002-ebook> [Archived on: 14.01.2024].
- [5] Dursun Peksen (2019). *When Do Imposed Economic Sanctions Work? A Critical Review of the Sanctions Effectiveness Literature*. In *Defence and Peace Economics* 30 (6). 635–647. DOI: 10.1080/10242694.2019.1625250.
- [6] Commission of the European Union (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber-space*. EU Commission. Available at <https://web.archive.org/web/20240114102834/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001> [Archived on: 14.01.2024].
- [7] Yuliya Miadzvetskaya and Ramses A. Wessel (2022a). *The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox*. In *European Papers*, 7(1), 413–438. Available at <https://web.archive.org/web/20230518092055/https://www.europeanpapers.eu/en/e-journal/externalisation-eu-cybersecurity-regime-cyber-diplomacy-toolbox> [Archived on: 18.05.2023].
- [8] Sara Poli and Emanuele Sommaro (2023). *The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions*. In the *German Law Journal*, 24. Available at <https://web.archive.org/web/20240119112933/https://www.cambridge.org/core/services/aop-cambridge-core/content/view/OCD9A70721FB48EDEC1BDC521F358536/S2071832223000251a.pdf>

f/rationale_and_the_perils_of_failing_to_invoke_state_responsibility_for_cyberattacks_the_case_of_the_eu_cyber_sanctions.pdf [Archived on: 19.01.2024].

[9] Council of the European Union (2017a). *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*. Available at <https://web.archive.org/web/20240114103227/https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf> [Archived on: 14.01.2024].

[10] Council of the European Union (2017b). *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*. Available at <https://web.archive.org/web/20240114103702/https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf> [Archived on: 14.01.2024].

[11] Council of the European Union (2018). *EU External Cyber Capacity Building Guidelines*. Available at <https://web.archive.org/web/20240114103501/https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf> [Archived on: 14.01.2024].

[12] Council of the European Union (2019a). *Council Decision (CFSP) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. Available at <https://web.archive.org/web/20240114103817/https://ccdcoe.org/uploads/2019/10/EU-190517-Council-Regulation-concerning-restrictive-measures-against-cyber-attacks-threatening-the-Union-or-its-Member-States.pdf> [Archived on: 14.01.2024].

[13] Council of the European Union (2019b). *Council Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*. Available at <https://web.archive.org/web/20240114104019/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0797> [Archived on: 14.01.2024].

[14] Mattia Casula, Nandhini Rangarajan, and Patricia Shields (2021). *The potential of working hypotheses for deductive exploratory research*. In *Quality & quantity* 55 (5). 1703–1725. DOI: 10.1007/s11135-020-01072-9.

[15] Center for Strategic and International Studies (n.d.). *Confidence-Building Measures*. Available at <https://web.archive.org/web/20240113151931/https://www.csis.org/programs/international-security-program/isp-archives/asia-division/confidence-building-measures> [Archived on: 13.01.2024].

[16] Mika Kerttunen, Kim Schuck, and Jonas Hemmelskamp (2023). *Major Cyber Incidents*. KA-SAT 9A. European Repository of Cyber Incidents (EuRepoC). Available at <https://web.archive.org/web/20240114101843/https://eurepoc.eu/wp-content/uploads/2023/10/KA-SAT-Viasat-MaCI.pdf> [Archived on: 14.01.2024].

[17] Erica Moret and Patryk Pawlak (2017). *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?* European Union Institute for Security Studies (EUISS).

Available at

<https://web.archive.org/web/20240114102146/https://www.jstor.org/stable/pdf/resrep06815.pdf> [Archived on: 14.01.2024].

[18] Samuele de Tomas Colatin (2020). *Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action*. CCDCOE. Available at <https://web.archive.org/web/20240114102538/https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/> [Archived on: 14.01.2024].

[19] Martina Calleri (2020). *The European Union as a Global Actor in Cyberspace: Can the Cyber Sanctions Regime Effectively Deter Cyber-Threats?* In the *Romanian Cyber Security Journal* 2 (2). 3–9. Available at https://rocys.ici.ro/documents/42/2020_fall_article_1.pdf.

[20] Eleni Kapsokoli (2021). *Sanctions and Cyberspace: The Case of the EU's Cyber Sanctions Regime*. In *Proceedings of the European Conference on Information Warfare and Security: Academic Conferences International Ltd*. Available at <http://tinyurl.com/24cxc7xh> [Archived on: 14.01.2024].

[21] European Union (n.d.). *Joining the EU*. Available at https://web.archive.org/web/20231128164151/https://european-union.europa.eu/principles-countries-history/joining-eu_en [Archived on: 28.11.2023].

[22] Council of the European Union & European Parliament (2014). *Regulation (EU) No 232/2014 of the European Parliament and of the Council of 11 March 2014 establishing a European Neighbourhood Instrument*. Available at <https://web.archive.org/web/20240114102934/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0232> [Archived on: 14.01.2024].

[23] La France au Monténégro (2023). *Western Balkans Cyber Capacity Center (WB3C)*. Ambassade de France a Podgorica. Available at <https://web.archive.org/web/20231229080955/https://me.ambafrance.org/Western-Balkans-Cyber-Capacity-Center-WB3C> [Archived on: 14.01.2024].

[24] Diplo (2023). *Regional cybersecurity and cybercrime policies in Africa*. Diplo. Available at <https://web.archive.org/web/20230928001506/https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/cybersecurity-cybercrime-africa-continental-regional-policies> [Archived on: 28.09.2023].

[25] International Telecommunication Union (2023). *Global Cybersecurity Index 2020*. Available at <https://web.archive.org/web/20231229185429/https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E> [Archived on 29.12.2023].

[26] National Cyber Security Centre (2020). *Foreign Secretary condemns Russia's GRU after NCSC assessment of Georgian cyber-attacks*. Available at

<https://web.archive.org/web/20231004163741/https://www.ncsc.gov.uk/news/foreign-secretary-condemns-russia-s-gru-after-ncsc-assessment-of-georgian-cyber-attacks> [Archived on: 04.10.2023].

[27] Stefan Soesanto (2021). *The limits of like-mindedness in cyber-space*. Real Instituto Elcano. Available at <https://web.archive.org/web/20230928122038/https://www.realinstitutoelcano.org/en/analyses/the-limits-of-like-mindedness-in-cyberspace/> [Archived on: 28.09.2023].

[28] European Repository of Cyber Incidents (2023). *EU dataset* (April 2023) [Dataset]. Available at <https://web.archive.org/web/20240113152658/https://eurepoc.eu/database/> [Archived on 13.01.2024; last access on 30.08.2023].

[29] Annegret Bendiek and Matthias Schulze (2021). *Attribution: A Major Challenge for EU Cyber Sanctions - An Analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the Attack on the OPCW*. SWP Comment, *Stiftung Wissenschaft und Politik*. Available at <https://web.archive.org/web/20230603010526/https://www.swp-berlin.org/publikation/attribution-a-major-challenge-for-eu-cyber-sanctions> [Archived on: 11.01.2022].

[30] Stefan Soesanto (2020). *Europe Has No Strategy on Cyber Sanctions*. Lawfare Media. Available at <https://web.archive.org/web/20240113161048/https://www.lawfaremedia.org/article/europe-has-no-strategy-cyber-sanctions> [Archived on: 13.01.2024].

[31] ENISA (2023). *ENISA Threat Landscape 2023*. Available at <https://web.archive.org/web/20240102182520/https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> [Archived on: 02.01.2024].

[32] Michael Byers (2021). *Still agreeing to disagree: international security and constructive ambiguity*. In the *Journal on the use of force and international law* 8.1 (2021). 91-114.

[33] Nadiya Kostyuk and Yuri M. Zhukov (2019). *Invisible digital front: can cyber attacks shape battlefield events?* In the *Journal of Conflict Resolution* 63.2. 317-347.

7. Appendix

[EU Cyber Diplomacy Toolbox Dataset Codebook – Version 1.0](#)

[EU Cyber Diplomacy Toolbox Dataset – Version 1.0](#)



**European
Repository of
Cyber Incidents**

contact@eurepoc.eu

www.eurepoc.eu

[@EuRepoC](#)

About the authors:

Annika Sachs is a Student Assistant at the Institute of Political Science at Heidelberg University.

Imke Schmalfeldt is a Student Assistant at the Institute of Political Science at Heidelberg University.

Kerstin Zettl-Schabath is a researcher at the Institute of Political Science (IPW) at Heidelberg University.

This analysis is based on a term paper by Annika Sachs and Imke Schmalfeldt.